

# Diploma in Infocomm Security Management (DISM)



## DIGITAL FORENSICS ASSIGNMENT

Module Name:	Digital Forensics and Investigation
Module Code:	ST2514
Class:	DISM/FT/ <u>2B/23</u>
Student Name and ID:	<u>Adeeb (p2107035)</u> <u>Toh Yi Da (p2123488)</u> <u>Chua Mun Ling (p2123516)</u>

# Table of Contents

Executive Summary .....	3
1.0 Introduction .....	3
2.0 Detail Analysis.....	3
2.1 Forensic Tools and Methodology .....	4
2.1.1 Magnet AXIOM Examine .....	4
2.1.2 SMALL SEO TOOLS .....	4
2.2 Evidence Extraction .....	4
2.2.1 Details of Jim Cloudy's Laptop.....	4
2.2.2 Details of Jim Cloudy's Account.....	5
2.2.3 Web Searches/URLs .....	5
2.2.4 Media .....	6
2.2.5 Documents.....	8
2.2.6 Others .....	15
2.3 Evidence Analysis .....	15
2.3.1 Web Searches/URLs .....	15
2.3.2 Media .....	17
2.3.3 Documents.....	20
2.3.4 Others .....	23
2.4 Findings .....	24
3.0 Conclusion .....	25
4.0 References .....	25
5.0 Reflection and Task Allocation .....	26
5.1 Reflection .....	26
5.2 Task Allocation.....	27

# Executive Summary

As the era of the internet is rising, so are the crimes that are committed against the use of computers. As a response to the expansion of computer crime, the field that relates to the usage of forensics has appeared. It involves collecting and examining electronic evidence that not only assesses damage to the pc but because of an electronic attack. Its primary goal is to collect all relevant information from a system like this that would be required to identify and arrest a criminal.

With the prevalence of cybercrime today, it is important for everyone to understand the most recent technologies utilized in the forensics industry and how it may be used lawfully. This concept shows how beneficial it is to use this field and promote such regulations. The computer gradually became into an extremely potent tool as new technological era compromised.

Unfortunately, as computers have improved, so too have the crimes that involve them. Distributed denial of service attacks and other viruses, zone call hijacking, Trojan horses, and website shutdowns are just a few of the large number of documented attack types generated using computers against other computers. The process of using scientific knowledge to collect, analyse, and present forensic evidence to the court. Forensics mostly refers to the gathering and examination of potential evidence. Potential evidence can come in many different shapes and sizes, including bloodstain DNA evidence, fingerprints left on windows, and data on hard drives.

## 1.0 Introduction

The purpose of this report is to provide corroborative evidence of the motivation and intent of Jim Cloudy with regards to a suspected mass shooting.

Jim's brother, having noticed that Jim's behaviour was increasingly concerning, alerted the police to the situation. As a result, Jim's laptop was seized by the police.

Therefore, digital forensics experts were engaged to find, to the best of their ability, corroborative evidence regarding Jim's intentions and motivations concerning the mass shooting.

## 2.0 Detail Analysis

After downloading the required files provided, we allocated one of our team members, Yi Da, to create a case and process the evidence files in the case with Axiom Process. After Yi Da processed the case, he zipped up the case and sent it to all our members. From there, with the same case file we all have access to, we used Axiom Examine to

look at the Artifacts and analyse them. Following this are Artifacts we found and analysed.

## 2.1 Forensic Tools and Methodology

Below are some tools and methodology that we have used.

### 2.1.1 Magnet AXIOM Examine

With Magnet AXIOM, investigators can recover forensic data from multiple sources; computers, smartphones, clouds, and other IoT devices, all within one case file. The primary goal of Magnet AXIOM is to allow examiners to capture and analyse forensics data, as well as share data discoveries seamlessly.

### 2.1.2 SMALL SEO TOOLS

Small SEO Tools is a website to reverse image to know where the image originated from.

## 2.2 Evidence Extraction

We managed to extract some evidence from Jim's laptop and placed them below.

### 2.2.1 Details of Jim Cloudy's Laptop

Laptop Details	
Operating System	Windows 10 Education
Version Number	6.3
Installed/Updated Date/Time	27/3/2018 12:13:27 PM
Product Key	FNQKC-MJ3BJ-Q34DQ-837KC-RVVYY
Owner	Windows User
Computer Name	DESKTOP-PM6C56D
DHCP DNS Server(s)	68.105.28.11, 68.105.29.11, 68.105.28.12
Operating System Version	Education
Build Number	16299
Product ID	00328-00089-23637-AA141
Last Shutdown Date/Time	27/3/2018 9:45:28 PM
System Root	C:\Windows
Path	C:\Windows
Last Access Time Enabled	Last Access Updates Disabled

Figure 2.1: Details of Jim's laptop

### 2.2.2 Details of Jim Cloudy's Account

Account	Email used
Dropbox	jimcloudy1@gmail.com
Twitter	jimcloudy1@gmail.com
Microsoft	jimcloudy@outlook.com
Box	jimcloudy1@gmail.com
AWS Amazon	jimcloudy1@gmail.com
Skype	jimcloudy@outlook.com
Google Drive	jimcloudy1@gmail.com

Figure 2.2: Relevant Jim accounts

### 2.2.3 Web Searches/URLs

Jim's laptop had many Google searches, some of which uncovered his motive. A table of the search terms we found interesting is shown in Figure 2.3 below.

Search Terms
where the dollar goes farthest vietnam or indonesia
bali airport
iad airport
jfk airport code
gunbroker
upcoming anti-gun rally near me
democratic national headquarters
hotels in bali
how to smuggle cash through airport
gun control in indonesia
things to do in bali
uk wants to ban knives
gun control great britain
just how easy is it to buy an illegal gun
airports near dc
police response times by zip code
which state has the worst police response times
which dc airport has fewest delays
concealable tactical rifles
submachine guns
gunstore near me
Northern Virginia Gun Works
most beautiful contries with non extradition
transferring money to an overseas account
keltec 2000 site:gunbroker.com
flights to bali, indonesia
430 south capitol street, DC
reston virginia democratic party building
public buildins in reston va
fairfax democate building
cascades library sterling va meeting room

how to use google docs as chat
--------------------------------

Figure 2.3: Non-exhaustive list of Google Searches found on Jim's laptop

Additionally, we found a list of URLs that Jim's laptop had accessed. A table of the URLs we found that could be used as evidence is shown in Figure 2.4 below.

URLs
<a href="https://www.theblaze.com/video/preach-gun-owner-slams-leftists-over-gun-violence-in-impassioned-speech-at-city-council">https://www.theblaze.com/video/preach-gun-owner-slams-leftists-over-gun-violence-in-impassioned-speech-at-city-council</a>
<a href="https://www.theblaze.com/news/2018/04/05/commentary-how-the-left-bullies-everyone-who-disagrees-with-them-and-what-you-should-do-about-it">https://www.theblaze.com/news/2018/04/05/commentary-how-the-left-bullies-everyone-who-disagrees-with-them-and-what-you-should-do-about-it</a>
<a href="https://www.theblaze.com/video/you-cant-fight-the-government-its-time-to-debunk-this-popular-anti-gun-talking-point">https://www.theblaze.com/video/you-cant-fight-the-government-its-time-to-debunk-this-popular-anti-gun-talking-point</a>
<a href="https://pocketsense.com/can-americans-foreign-bank-accounts-7995.html">https://pocketsense.com/can-americans-foreign-bank-accounts-7995.html</a>
<a href="https://www.quora.com/Can-the-scanner-machines-in-airports-detect-the-currency-notes-in-the-checked-in-luggage-hand-luggage">https://www.quora.com/Can-the-scanner-machines-in-airports-detect-the-currency-notes-in-the-checked-in-luggage-hand-luggage</a>
<a href="https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/Desktop/?region=us-east-2&amp;tab=overview">https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/Desktop/?region=us-east-2&amp;tab=overview</a>
<a href="https://app.box.com/folder/48430849690">https://app.box.com/folder/48430849690</a>
<a href="https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&amp;field-keywords=velcro+tear+away+clothes">https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&amp;field-keywords=velcro+tear+away+clothes</a>
<a href="https://www.wikihow.com/Make-Rip-Away-Pants">https://www.wikihow.com/Make-Rip-Away-Pants</a>
<a href="https://weather.com/weather/alerts/localalerts/l/IAD:9:US?phenomena=Wl&amp;significance=Y&amp;areaid=VAZ506&amp;office=KLWX&amp;etn=0005">https://weather.com/weather/alerts/localalerts/l/IAD:9:US?phenomena=Wl&amp;significance=Y&amp;areaid=VAZ506&amp;office=KLWX&amp;etn=0005</a>
<a href="https://www.tripadvisor.com/Hotels-g294226-Bali-Hotels-BackUrl.html">https://www.tripadvisor.com/Hotels-g294226-Bali-Hotels-BackUrl.html</a>
<a href="https://www.resistandprotest.com/event-list">https://www.resistandprotest.com/event-list</a>
<a href="http://fairfaxdemocrats.org/calendar/">http://fairfaxdemocrats.org/calendar/</a>
<a href="http://fairfaxdemocrats.org/blog/event/presentation-how-to-improve-your-gun-argument/?instance_id=36213">http://fairfaxdemocrats.org/blog/event/presentation-how-to-improve-your-gun-argument/?instance_id=36213</a>
<a href="https://www.resistancecalendar.org/">https://www.resistancecalendar.org/</a>
<a href="https://marchforourlives.com/">https://marchforourlives.com/</a>
<a href="https://docs.google.com/document/d/1GOv7MwOXM-7Vkoy4kJE3Q5bMDB5IWA0tB57a3u2hqEA/edit?usp=docslist_api">https://docs.google.com/document/d/1GOv7MwOXM-7Vkoy4kJE3Q5bMDB5IWA0tB57a3u2hqEA/edit?usp=docslist_api</a>
<a href="https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/Desktop/?region=us-east-2&amp;tab=overview">https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/Desktop/?region=us-east-2&amp;tab=overview</a>

Figure 2.4: Non-exhaustive list of URLs accessed by Jim's laptop

## 2.2.4 Media

A table of the image files we used as evidence is shown in Figure 2.5 below.

Filename (if any)	Image
RedGuns.jpg	

f_0018cd	
f_0017c5	
	
f_0018ce	
f_0018ce	


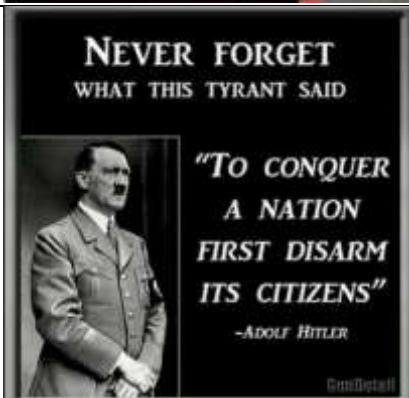
f_0017ee		
f_0018ca		

Figure 2.5: Table of images used as evidence

## 2.2.5 Documents

We found several documents on Jim's laptop that uncovered his intent and motive. Firstly, the file 'The Cloudy Manifesto.docx' contains a manifesto. The first and last few paragraphs of the manifesto are shown in Figures 2.6 and 2.7 below.

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

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

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

Figure 2.6: The first few paragraphs of the manifesto in 'The Cloudy Manifesto.docx'



Something must be done to show that gun-free zones do not work and will never work. So I intend to break the law. Because that's what the criminals will do. No matter your laws, when they decide to act, they will. Drugs have always been illegal, but that doesn't stop people from getting drugs. Speeding is illegal, but people still drive fast. Fraud is illegal, but greed is a strong motivator. So I will be the lone wolf that helps demonstrate to the American Public that laws and signs won't work. Only the ability to protect yourself will work. The Second Amendment was not "poorly written" it was drafted by the same men who drafted the rest of the Constitution. And no one is complaining about the protections and freedom it gives you. Especially the 1<sup>st</sup> amendment which allows you to spew your crazy gun-control thoughts.

You will soon see when the blood has been shed and the defenseless bodies stacked high. I will do what I must. No matter who is hurt, the collateral damage will be worth it.

I will be the change. I will be the revolutionary. I will be the history maker. I will fight. I will be the Lone Wolf.

Figure 2.7: The last few paragraphs of the manifesto in 'The Cloudy Manifesto.docx'

The metadata of the document is shown in Figure 2.8 below.

<b>Creator:</b>	jcloudy
<b>LastModifiedBy:</b>	jcloudy
<b>Revision:</b>	1
<b>Created:</b>	2018-04-02T01:00:00Z
<b>Modified:</b>	2018-04-02T01:35:00Z
<b>Template:</b>	Normal
<b>Application:</b>	Microsoft Office Word
<b>AppVersion:</b>	16.0000

Figure 2.8: Metadata of 'The Cloudy Manifesto.docx'

Secondly, the file 'Cloudy thoughts (4apr).docx' contains some thoughts of Jim. The file's contents and metadata are shown in Figures 2.9 and 2.10 respectively.

I don't know if this plan will work. Plans never survive first contact. I don't expect to fail, but there are so many possibilities. But now the weather. Its going to snow, and the winds will be strong. No problem for the attack, but if my flight is delayed or cancelled, that might prove to be a problem.

I'm stressed and writing used to help me calm down. It seems to be working. Im leaving a lot behind, and the weight of this responsibility is almost too much to handle. I wont stop now, though. Even if I'm killed at the site, I know that what im doing is just and right. Freedom requires sacrifice. If I must be that lamb, then I walk to my slaughter freely of my own accord.

I am saving everything to the cloud on several accounts. I don't want my words mixed up, and I don't want my thoughts deleted. I want my family to understand why I did this. I think they will keep my secret if I am successful and leave the country without problems. The only record will remain in the cloud and Paul will have the only other keys.

My fate will be in God's hands. I pray I have the strength and the luck necessary to persevere. Please let the weather clear!

Figure 2.9: Contents of 'Cloudy thoughts (4apr).docx'

<b>Creator:</b>	jcloudy
<b>LastModifiedBy:</b>	jcloudy
<b>Revision:</b>	1
<b>Created:</b>	2018-04-05T02:32:00Z
<b>Modified:</b>	2018-04-05T02:39:00Z
<b>Template:</b>	Normal
<b>Application:</b>	Microsoft Office Word
<b>AppVersion:</b>	16.0000

Figure 2.10: Metadata of 'Cloudy thoughts (4apr).docx'

Thirdly, the file 'AIRPORT INFORMATION.docx' contains some information of a flight. The file's contents and metadata are shown in Figures 2.11 and 2.12 respectively.

## 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.

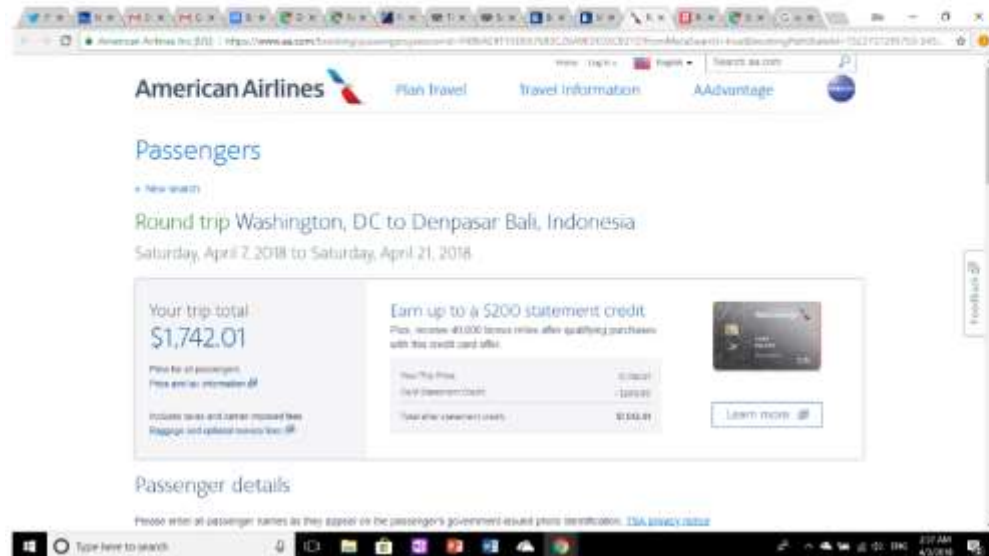


Figure 2.11: Contents of 'AIRPORT INFORMATION.docx'

<b>Creator:</b>	jcloudy
<b>LastModifiedBy:</b>	jcloudy
<b>Revision:</b>	9
<b>Created:</b>	2018-03-30T02:29:00Z
<b>Modified:</b>	2018-04-04T04:59:00Z
<b>Template:</b>	Normal
<b>Application:</b>	Microsoft Office Word
<b>AppVersion:</b>	16.0000

Figure 2.12: Metadata of 'AIRPORT INFORMATION.docx'

Fourthly, the file 'Planning.docx' contains some plans. The file's contents and metadata are shown in Figures 2.13, 2.14 and 2.15 below.

## Planning

### 1. Target

- a. Must have good escape route
- b. Preferably near Airport
- c. Must be Gun Free zone.

### 2. Supplies

- a. Gun (black market)
  - i. Norther VA Gun Works 7518 Fullerton Rd # K, Springfield, VA 22153
  - ii. NOVA 412 W Broad Street Falls Church, VA 22046
- iii. b. Ammo.
  - i. 9mm is 1000 for \$360
  - ii. Kel-Tec Sub 2000 9mm \$400.
- c. Latex gloves
- d. Velcro tear away clothing?
- e. Cash

### 3. Escape

- a. No Extradition countries
  - i. Indonesia (Nicer, but more expensive)
  - ii. Vietnam
  - iii. Can live very well on 100 a day, for 9 years.
- b. Buy tickets for same day
- c. Preferable direct flight
- d. Have suitcase in car.

### 4. Release

- a. Start writing ideas and thoughts
- b. Save to separate locations for redundancy
- c. Place it in the cloud for remote access
- d. "Press Release" once home free.

Figures 2.13 and 2.14: Contents of 'Planning.docx'

<b>Creator:</b>	jcloudy
<b>LastModifiedBy:</b>	jcloudy
<b>Revision:</b>	9
<b>Created:</b>	2018-03-30T02:16:00Z
<b>Modified:</b>	2018-04-04T05:30:00Z
<b>Template:</b>	Normal
<b>Application:</b>	Microsoft Office Word
<b>AppVersion:</b>	16.0000

Figure 2.15: Metadata of 'Planning.docx'

Lastly, we have "Operation 2nd Hand Smoke.pptx" which contain the plan. This could be seen from figure 2.23 below.



Figure 2.16: Anti-Gun Rally

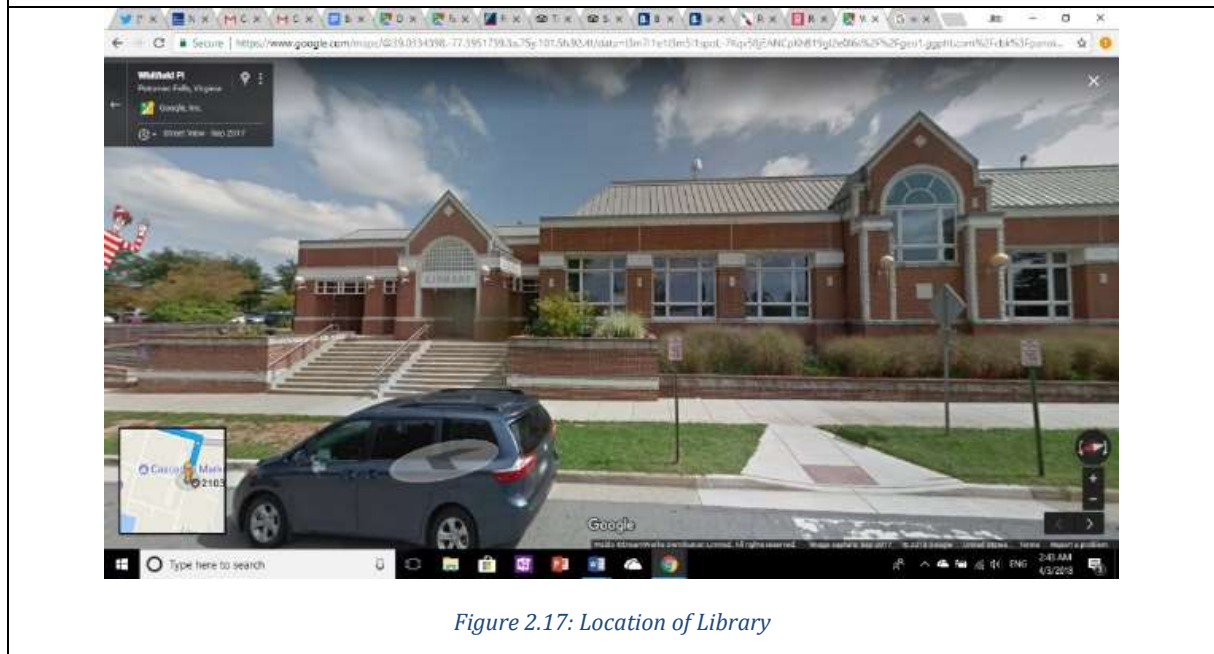


Figure 2.17: Location of Library

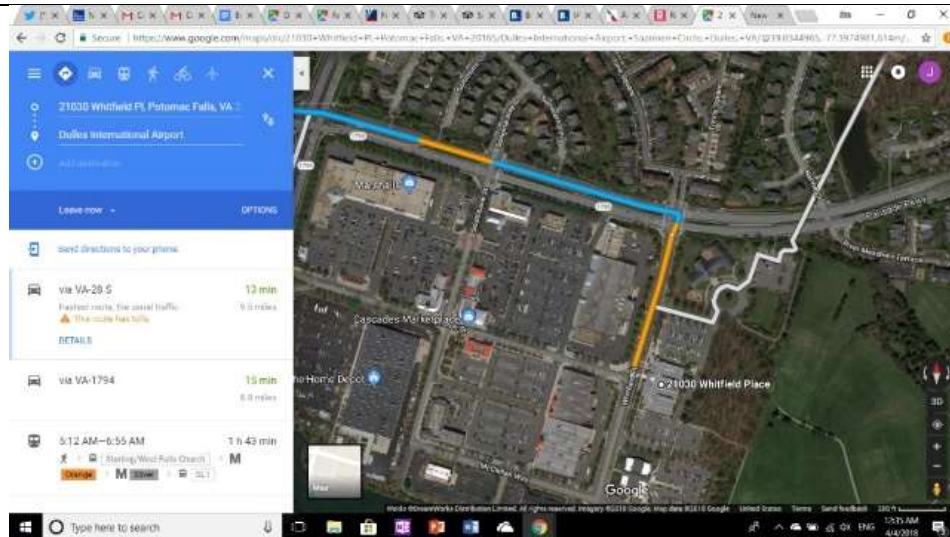


Figure 2.18: Google Map GPS

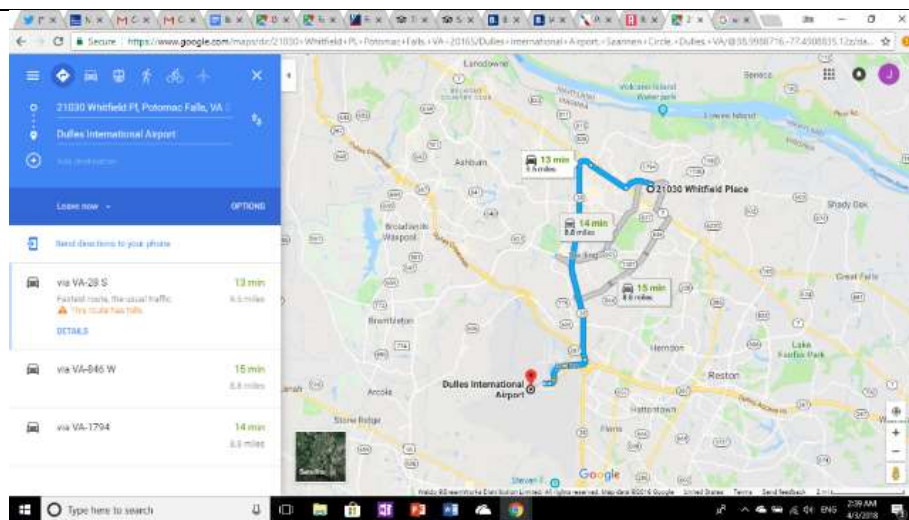


Figure 2.19: Google Map GPS

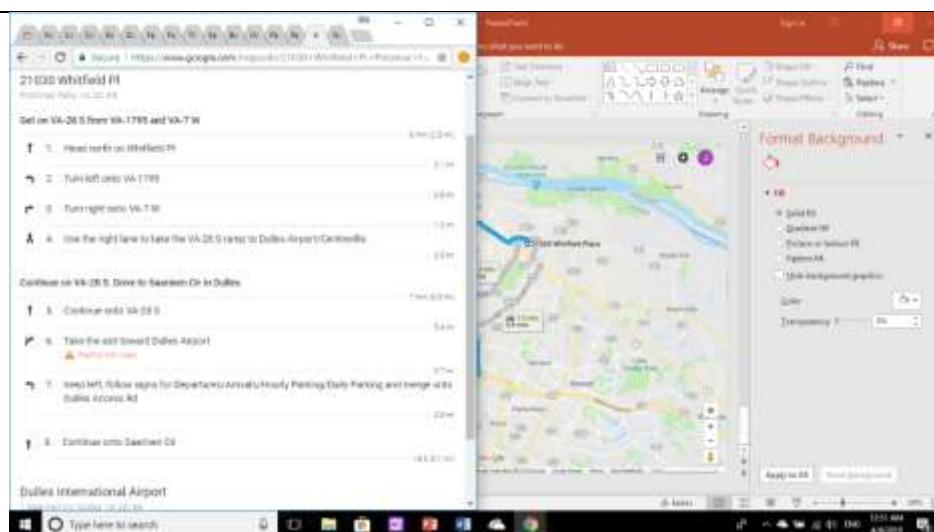


Figure 1.20: Directions from Google Map



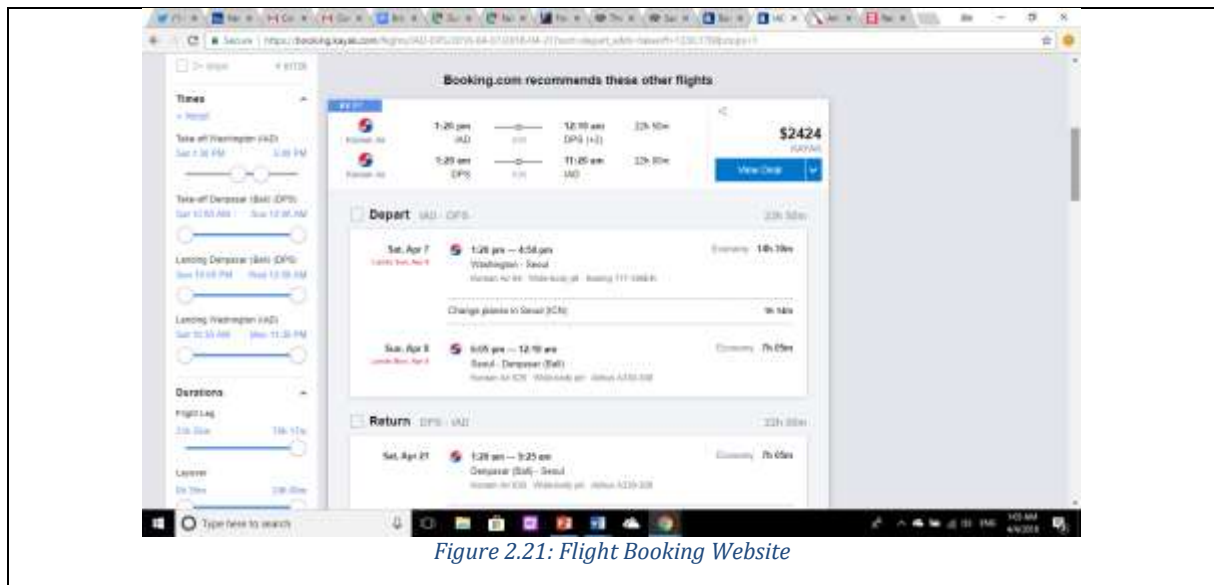


Figure 2.21: Flight Booking Website

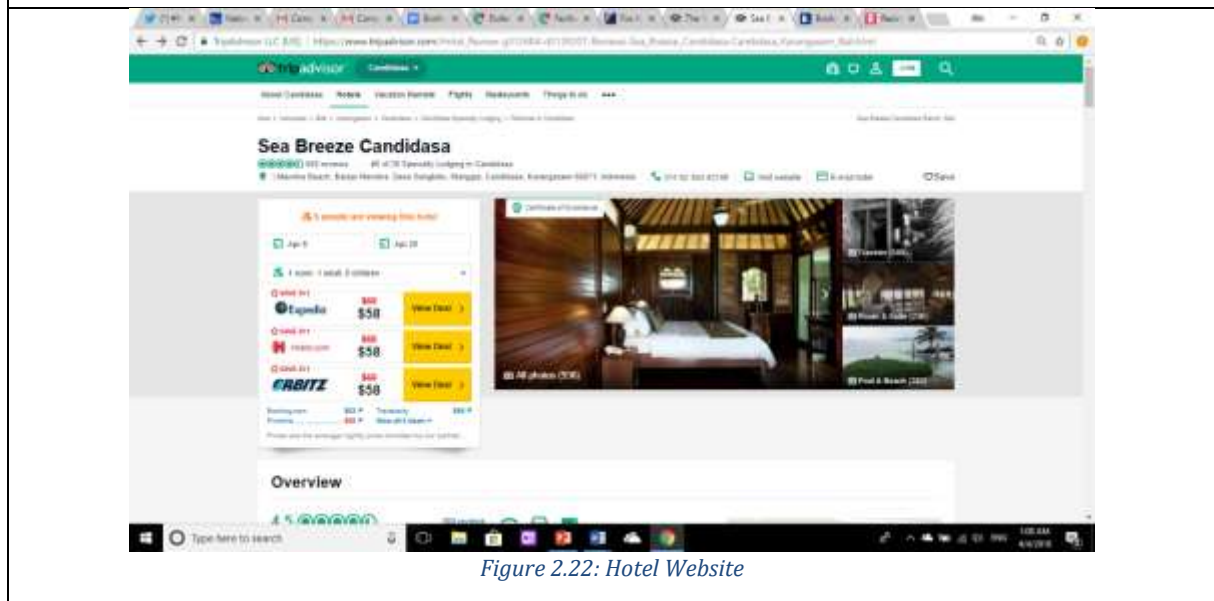


Figure 2.22: Hotel Website

<b>Title:</b>	PowerPoint Presentation
<b>Creator:</b>	jcloudy
<b>LastModifiedBy:</b>	jcloudy
<b>Revision:</b>	7
<b>Created:</b>	2018-04-04T04:32:32Z
<b>Modified:</b>	2018-04-04T05:11:27Z
<b>Application:</b>	Microsoft Office PowerPoint
<b>PresentationFormat:</b>	Widescreen
<b>Slides:</b>	7
<b>Notes:</b>	0
<b>HiddenSlides:</b>	0
<b>MMClips:</b>	0
<b>AppVersion:</b>	16.0000

Figure 2.23: Contents of Operation 2nd Hand Smoke.pptx

The CSV File:

File Name	Content
rootkey.csv	AWSAccessKeyId=AKIAJQCL74OG6U6JRXKQ  AWSSecretKey=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

Figure 2.24: Content of rootkey.csv file

## 2.2.6 Others

Other than the above evidence, there were also evidence related to the location and travel made by Jim on Google Maps.

Below are some location and travel searches Jim has made on Google Maps.

Location and Travel Searches
National Rifle Association of America
430 S Capitol St SW, Washington, DC 20003
Indonesia
Source Address: Fairfax County Democratic Committee, 8500 Executive Park Ave, Fairfax, VA 22031 Destination Address: Dulles International Airport, Saarinen Circle, Dulles, VA
Source Address: 21030 Whitfield Pl, Potomac Falls, VA 20165 Destination Address: Dulles International Airport, Saarinen Circle, Dulles, VA
Northern Virginia Gun Works
Hamad International Airport
Dulles International Airport
Sterling VA

Figure 2.25: Jim's location and Travel searches

## 2.3 Evidence Analysis

After extracting the evidence, we first analysed it piece by piece.

### 2.3.1 Web Searches/URLs

From the Google searches performed and URLs accessed on Jim's laptop, we uncovered a lot of detail about Jim's intents and motives.

Two tables showing the searches and URLs and explaining what their implications on Jim's likely intent and motives are shown in Figures 2.26 and Figures 2.27 below.

Search	Implication(s)
where the dollar goes farthest vietnam or indonesia	Jim wants to go to either Vietnam or Indonesia and chose which country to travel to by where the dollar goes further.
upcoming anti-gun rally near me	Jim wants to go to an anti-gun rally.

how to smuggle cash through an airport transferring money to an overseas account	Jim wants to transfer cash to another country.
just how easy is it to buy an illegal gun  concealable tactical rifles  submachine guns  gunstore near me	Jim wants to purchase a firearm.
police response times by zip code  which state has the worst police response times	Jim did research into the responsiveness of police by state.
airports near dc  which dc airport has fewest delays	Jim wants to go on a flight from an airport in Washington DC but does not want to deal with delays.
most beautiful countries with non-extradition	Jim wants to travel to a country without extradition, possibly to commit a crime or escape the consequences of committing a crime.

Figure 2.26: Google searches on Jim's laptop and their implications

URL	Implication(s)
<a href="https://www.theblaze.com/video/preach-gun-owner-slams-leftists-over-gun-violence-in-impassioned-speech-at-city-council">https://www.theblaze.com/video/preach-gun-owner-slams-leftists-over-gun-violence-in-impassioned-speech-at-city-council</a>  <a href="https://www.theblaze.com/news/2018/04/05/commentary-how-the-left-bullies-everyone-who-disagrees-with-them-and-what-you-should-do-about-it">https://www.theblaze.com/news/2018/04/05/commentary-how-the-left-bullies-everyone-who-disagrees-with-them-and-what-you-should-do-about-it</a>  <a href="https://www.theblaze.com/video/you-cant-fight-the-government-its-time-to-debunk-this-popular-anti-gun-talking-point">https://www.theblaze.com/video/you-cant-fight-the-government-its-time-to-debunk-this-popular-anti-gun-talking-point</a>	Jim does not like that his right to bear firearms is being taken away.
<a href="https://www.quora.com/Can-the-scanner-machines-in-airports-detect-the-currency-notes-in-the-checked-in-luggage-hand-luggage">https://www.quora.com/Can-the-scanner-machines-in-airports-detect-the-currency-notes-in-the-checked-in-luggage-hand-luggage</a>	Jim wants to transfer money overseas though his luggage.
<a href="https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&amp;field-keywords=velcro+tear+away+clothes">https://www.amazon.com/s/ref=nb_sb_noss?url=search-alias%3Daps&amp;field-keywords=velcro+tear+away+clothes</a>	Jim wants some clothing he can quickly tear away, possibly to change his appearance.




<a href="https://www.wikihow.com/Make-Rip-Away-Pants">https://www.wikihow.com/Make-Rip-Away-Pants</a>	
<a href="https://www.tripadvisor.com/Hotels-g294226-Bali-Hotels-BackUrl.html">https://www.tripadvisor.com/Hotels-g294226-Bali-Hotels-BackUrl.html</a>	Jim wants to visit Bali.
<a href="https://www.resistandprotest.com/event-list">https://www.resistandprotest.com/event-list</a>  <a href="http://fairfaxdemocrats.org/calendar/">http://fairfaxdemocrats.org/calendar/</a>  <a href="http://fairfaxdemocrats.org/blog/event/presentation-how-to-improve-your-gun-argument/?instance_id=36213">http://fairfaxdemocrats.org/blog/event/presentation-how-to-improve-your-gun-argument/?instance_id=36213</a>  <a href="https://www.resistancecalendar.org/">https://www.resistancecalendar.org/</a>  <a href="https://marchforourlives.com/">https://marchforourlives.com/</a>	Jim wants to visit an anti-gun rally.
<a href="https://docs.google.com/document/d/1GOv7MwOXM-7Vkoy4kjE3Q5bMDB5lWA0tB57a3u2hqeA/edit?usp=docslist_api">https://docs.google.com/document/d/1GOv7MwOXM-7Vkoy4kjE3Q5bMDB5lWA0tB57a3u2hqeA/edit?usp=docslist_api</a>	<p>Jim use Google Docs to chat with his brother Paul as seen from “how to use google docs as chat” in his Google Search.</p> <p>The file title is ‘Brother Chat’</p>
<a href="https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/Desktop/?region=us-east-2&amp;tab=overview">https://s3.console.aws.amazon.com/s3/buckets/cloudy-thoughts/Desktop/?region=us-east-2&amp;tab=overview</a>	<p>This is Jim’s amazon website to store his files via cloud.</p> <p>Only people who has the key can access the website. Which contains some of Jim’s Private documents such as “Cloudy thoughts (4apr)” as seen in this URL.</p> <p>The access key is stored in rootkey.csv</p>

Figure 2.27: URLs accessed by Jim’s laptop and their implications

### 2.3.2 Media

Media files found in Jim’s laptop shows some possible thoughts that Jim has about guns and shootings.

The table below shows the media images we have extracted and the possible implications on Jim’s thoughts about guns and shooting.

Image	Implication(s)
	<p>Picture shows and states that majority of the map owns a gun overpowering those that wants a revolution.</p> <p>Jim may think that having a gun in possession would be very powerful.</p>

	<p>Picture shows and states that at an exhibition with 78,865 “Gun Nuts” carrying all kinds of guns around, no shooting accident happened. While in NYC where one of the most restrictive gun control laws is, a shooting incident happened. It also stated that this is what happens when only bad guys have guns.</p> <p>Jim may think that having a gun in possession will not do any harm unless he intends to do so and inflict harm on people.</p>
	<p>Picture includes a link and after searching for it online, it turns out to be a shop which sells a wide range of firearms, ammunition, and accessories. The shop is in United States, Grand Rapids.</p> <p>Jim would be considering purchasing his own firearms from this shop.</p>
	<p>Picture shows a woman with a girl holding on to a gun. The picture states to teach girls to shoot as restraining order is just a piece of paper and women should be able to protect themselves.</p> <p>Jim maybe trying to promote that more people such as females should know how to use guns and have guns in their possession.</p>
	<p>Picture has a background full of magazines which makes up a part of a rifle and states “Shop Magazines”.</p> <p>Jim may want to purchase rifles and plan to use both rifles and guns for the mass shooting.</p>

	<p>Picture states that a student who was bullied in school snapped one day shot the school. "I bullied but let's blame the guns!" states that although the shooting happened because of the bullying but the tragedy happened, and harm was caused because of the guns.</p> <p>Jim would think that guns can cause the greatest destruction and all blames would be on the guns if any harm was done.</p>
	<p>Picture shows some quotations of words said by two people. After searching, David Hogg is a gun control activist and Laura Ingraham is an American conservative television host. In the quotations, Laura Ingraham says that David Hogg could not get into college while in David Hogg's quotation, there were vulgarities and he stated to boycott Laura Ingraham's sponsors. After searching, it was known that Laura Ingraham tweeted and mocked David Hogg about getting rejection letters from four colleges and called him a Gun Rights Provocateur which referred to him as one who behaves controversially to provoke arguments or strong reactions.</p> <p>As the picture states that "the first amendment only applies to the left", which may mean that freedom of speech only applies to the left-wing politics. Jim may think that gun control activists like David Hogg do not have a say and that left-wing politics that support and seek to achieve social equality would also be against such activists.</p>
	<p>Picture shows Hitler and a quote said by him: "To conquer a nation first disarm its citizens"</p> <p>Jim may think that being armed brings more power and the effects of having or even using firearms can cause a big change.</p>

Figure 2.28: Images in Jim's laptop and their implications

### 2.3.3 Documents

The documents we used as evidence says a lot about Jim's intents and motives. A table showing some of the contents of these documents, as well as their implications is shown in Figure 2.29.

Document	Content	Implications
The Cloudy Manifesto.doc x	Look at Clive Bundy and the now the Snake River Ranchers. Without the means to protect themselves, they would have been victims of the government. Without the means to protect yourself, you may be a victim of the same, or of your fellow man.	Jim believes that people need to and should have the right to protect themselves from the government.
	when a shooter wants to do something...he does. The laws won't stop him, and neither will disarming yourself.	Jim believes that anti-gun laws and disarmament are ineffective.
	So are we really concerned about what is killing us? Why not outlaw unhealthy food? Oh, its our right to eat what we want? You don't say?!	Jim believes that anti-gun laws do not have a significant impact on deaths in his country compared to unhealthy food.
	Our military is full of people who grew up around guns and are comfortable shooting them. Get rid of that and it erodes a portion of our readiness.	Jim believes that the right to bear firearms can noticeably strengthen a nation's military.
	This will never stop. Once they outlaw guns, criminals will turn to knives. Then they will try to outlaw those as well. This is happening in the UK now. They already outlawed guns, and now they want to outlaw pocket knives.	Jim believes that anti-gun laws will lead to more problems in the future.
	Drugs have always been illegal, but that doesn't stop people from getting drugs. Speeding is illegal, but people still drive fast. Fraud is illegal, but greed is a strong motivator. So I will be the lone wolf that helps demonstrate to the American Public that laws and signs won't work.	Jim wants to express, to the public, his opinion that laws are ineffective.
	You will soon see when the blood has been shed and the defenseless bodies stacked high. I will do what I must. No matter who is hurt, the collateral damage will be worth it.	Jim wants to fight for what he believes in by taking the lives of several people.

	I will be the change. I will be the revolutionary. I will be the history maker. I will fight. I will be the Lone Wolf.	
Cloudy thoughts (4apr).docx	Its going to snow, and the winds will be strong. No problem for the attack, but if my flight is delayed or cancelled, that might prove to be a problem.	Jim is worried that his plan will fail if his flight is delayed or cancelled.
	Even if I'm killed at the site, I know that what im doing is just and right. Freedom requires sacrifice. If I must be that lamb, then I walk to my slaughter freely of my own accord.	Jim believes that he must risk his life to fight for what he believes is right.
	I want my family to understand why I did this. I think they will keep my secret if I am successful and leave the country without problems.	Jim wants his family to understand that he believes that he is fighting for what he thinks is right and is sure that they will not disclose his location to the police.
AIRPORT INFORMATION.docx	Ronald Reagan has best record of on-time departures. Dulles has flights to Indonesia. With Layover in Qatar.	Jim wants to fly from the United States of America to Indonesia.
	22 min from Fairfax County Democratic Committee, 8500 Executive Park Ave, Fairfax, VA 22031 to Dulles Airport.	Jim wanted an airport that was close to the Fairfax County Democratic Committee building.
Planning.docx	1. Target a. Must have good escape route b. Preferably near Airport c. Must be Gun Free zone.	Jim wants to go to a gun-free zone, possibly to show that anti-gun laws do not work.
	b. Ammo. i. 9mm is 1000 for \$360 ii. Kel-Tec Sub 2000 9mm \$400.	Jim wants to purchase a gun and some ammunition.
	c. Latex gloves d. Velcro tear away clothing?	Jim wants to conceal his identity to ensure he does not get caught.
	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.	Jim wants to escape to a country without extradition, so that he cannot get sent back to the United States of America for trial and stay there for nine years.

<p>Operation 2nd Hand Smoke.pptx</p>	<p>Refer to 2.2.5 figures 2.16 to 2.22</p>	<p>This PowerPoint contains details of Operation 2<sup>nd</sup> Hand Smoke which is presumably Jim's plan for the attack.</p> <p>In figure 2.16, a screenshot regarding a Town Hall For Our Lives campaign where issues about gun violence will be talked about in Sterling VA on 7<sup>th</sup> April 2018 from 12pm to 2pm. Jim may have wanted to attend the talk.</p> <p>In figure 2.17, it is a google maps search to Whitfield Pl, Potomac Falls, VA. The place shown on the map is Cascades Loudoun County Public Library which is highly likely the place that Jim wants to attack.</p> <p>In figure 2.18, 2.19 and 2.20, it is the google maps search result for the route from Whitfield Pl, Potomac Falls to Dulles International Airport. Jim may have planned for this to be his escape route from Cascades Loudoun County Public Library to Dulles International Airport.</p> <p>In figure 2.21, it shows recommended flight bookings for Jim from Washington to Seoul and from Seoul to Bali. This is most likely Jim's plan for getting out of the country after his attack. From this, we can also assume that Jim is planning his attack on 7<sup>th</sup> April 2018, the day he booked his flight on.</p>
--------------------------------------	--	---

		In figure 2.22, it shows a hotel booking page for Sea Breeze Candidasa located in Bali. The booking duration stated is from 8 April to 20 April. Jim may have planned to stay in this hotel from 8 April to 20 April after he has fled to Bali.
--	--	---

Figure 2.29: Documents in Jim's laptop and their implications

### 2.3.4 Others

Other location and travel evidence found shows possible routes and actions Jim has taken and places he has visited.

Below are the locations Jim has searched for and the possible implications for each of it.

<b>Location and Travel Searches</b>	<b>Implication(s)</b>
National Rifle Association of America	The National Rifle Association of America (NRA) is a gun rights advocacy group and the largest gun-owners' organisation in the United States. It is one of the oldest civil rights organisations and they would provide firearms training and gun safety programs to gun owners. Jim may have wanted to go the NRA to receive training regarding firearms to better know how to use his guns and rifles.
430 S Capitol St SW, Washington, DC 20003	This is the address of the Democratic National Committee. This could have been one of the target places that Jim wanted to attack.
Indonesia	Indonesia may be one of the countries in Jim's plan to escape to.
Source Address: Fairfax County Democratic Committee, 8500 Executive Park Ave, Fairfax, VA 22031 Destination Address: Dulles International Airport, Saarinen Circle, Dulles, VA	The source address is where Fairfax Democratic Committee is located, and the destination address is where Dulles International Airport in the Eastern United States is located. Jim could have planned to attack the Fairfax Democratic Committee, get to Dulles International Airport and escape from there. He may have been planning

	his escape route, the duration for the whole attack and how he can leave the country without getting caught.
Source Address: 21030 Whitfield Pl, Potomac Falls, VA 20165 Destination Address: Dulles International Airport, Saarinen Circle, Dulles, VA	The source address is where Cascades Loudoun County Public Library is located while the destination address is where Dulles International Airport in the Eastern United States is located. Cascades Loudoun County Public Library may have been another target that Jim wanted to attack. He may have planned to attack the library and escape from Dulles International Airport to another country. He could have been planning his escape route, how he should attack to leave the place and get to Dulles International Airport and leave the country without getting caught.
Northern Virginia Gun Works	Northern Virginia Gun Works does not have an official website. However, websites with related reviews to the place states that it is a place where gunsmiths help to repair and modify firearms. Jim may have gone there to repair or modify his firearm(s).
Hamad International Airport	Hamad International Airport is the airport located in Doha, capital of Qatar. This could have been one of the destinations that Jim planned to take a flight to after his attack from Dulles International Airport.

Figure 2.30: Location and Travel searches in Jim's laptop and their implications

## 2.4 Findings

From the evidence we have extracted and analysed, our main findings are as follows. Jim is planning for a mass shooting and fleeing the country right after the attack. His motive for doing so is because he does not like his right of possession of firearms to be taken away and believes that citizens in the country should have rights to protect themselves. His intention in doing so is to fight for what he believes is right and to express to the public that anti-gun laws are ineffective and may cause more problems in future. His preparation for the shooting includes finding out where to purchase



firearms, the location of the shooting, the escape route he is going to take from the location of the shooting to the nearest airport and the country he is going to flee to. For the possible places he visited to purchase his firearms are Northern Virginia Gun Works and Mr Gun Dealer located in Grand Rapids. Prior to the shooting he may have gone to the National Rifle Association of America to receive training on how to utilise his firearms and Northern Virginia Gun Works to modify his firearms. Possible locations of the shooting include Cascades Loudoun County Public Library where an anti-gun rally will take place, Fairfax County Democratic Committee office and Democratic National Committee office. The escape route he planned included from Fairfax County Democratic Committee office building to Dulles International Airport if the attack is at the Fairfax Democratic Committee office and from Cascades Loudoun County Public Library to Dulles International Airport if the attack is at the anti-gun rally. As for the country he plans to flee to, there are some criteria he wants the country to have. The criteria include currency being more affordable and no extradition so that he would not get sent back to the United States of America for trial. Possible countries include Vietnam, Indonesia, and Qatar. Thus, from the extracted and analysed evidence, Jim has planned for all the aspects that he needs to consider having the mass shooting and flee the country smoothly.

### 3.0 Conclusion

After gathering and analysing a lot of evidence, we can conclude that Jim most likely intended to engage in a mass shooting at the Fairfax County Democratic Committee building, then escape to Bali, Indonesia.

The most likely reason behind this intention is that he wants to protest anti-gun laws, believing that they are ineffective and will only do more harm than good.

Additionally, he most likely chose to escape to Bali as it does not have extradition with the United States of America, which can significantly decrease his chances of being punished by the law.

### 4.0 References

Facebook. (n.d.). Mr Gun Dealer. [online] Available at: <https://www.facebook.com/mrgundealer/> [Accessed 12 August 2022]

Yelp. (2013). Mr Gun Dealer – Grand Rapids, MI [online] Available at: <https://www.yelp.com/biz/mr-gun-dealer-grand-rapids> [Accessed 12 August 2022]

Wikipedia (n.d.). David Hogg [online] Available at: [https://en.wikipedia.org/wiki/David\\_Hogg](https://en.wikipedia.org/wiki/David_Hogg) [Accessed 12 August 2022]

Wikipedia (n.d.). Laura Ingraham [online] Available at: [https://en.wikipedia.org/wiki/Laura\\_Ingraham](https://en.wikipedia.org/wiki/Laura_Ingraham) [Accessed 12 August 2022]

Cleve R. Wootson R. (2018). Laura Ingraham mocked Parkland survivor David Hogg over college rejections. Now he's headed to Harvard [online] Los Angeles Times. Available at: <https://www.latimes.com/nation/la-na-parkland-student-harvard-20181222-story.html> [Accessed 12 August 2022]

National Rifle Association. (n.d.). What is the NRA? [online] Available at: <https://membership.nra.org/FAQ> [Accessed 12 August 2022]

BBC News. (n.d.). US gun control: What is the NRA and why is it so powerful? [online] Available at: <https://www.bbc.com/news/world-us-canada-35261394> [Accessed 12 August 2022]

Mapquest.com (n.d.). Democratic National Committee. [online] Available at: <https://www.mapquest.com/us/district-of-columbia/democratic-national-committee-303756116> [Accessed 12 August 2022]

Fairfax County Democratic Committee. (n.d.). Fairfax Democrats. [online] Available at: <https://www.fairfaxdemocrats.org> [Accessed 12 August 2022]

Loudoun County Public Library. (n.d.). Cascades. [online] Available at: <https://library.loudoun.gov/Cascades> [Accessed 12 August 2022]

Yelp. (n.d.) Northern Virginia Gun Works - Springfield, VA. [online] Available at: <https://www.yelp.com/biz/northern-virginia-gun-works-springfield> [Accessed 12 August 2022]

## 5.0 Reflection and Task Allocation

### 5.1 Reflection

The table below shows the team members' reflections.

Name	Reflection
Adeeb (p2107035)	This Assignment lets me have a better understanding on what digital forensics does. I learn how to use Magnet AXIOM & also the steps to gather all the evidence. I also learn that an investigator's work can be very messy & also how to create a report at the end of the investigation. By using AXIOM , I also learn that even deleted data could be recovered back.

	One problem I face is that some artifacts files are corrupted & I cannot view the media at all.I hope to apply my analytical skills in my future career.
Toh Yi Da (p2123488)	I liked using Axiom Process because of all the settings I could tinker with, like using Magnet.AI to categorize images. The toughest challenge I faced was presenting the evidence we obtained. I solved this problem by presenting the evidence in tables.
Chua Mun Ling (p2123516)	From this assignment, I have learnt and understood more about analysing and processing digital evidence. The assignment has allowed me to have a deeper understanding of the evidence analysis process by doing it hands on and knowing the thought process of what an investigator must have when analysing digital evidence. One of challenge that I have faced is linking the media artifacts found to what Jim may be planning or thinking or why he may access to these media files.

## 5.2 Task Allocation

The table below shows the team members' assigned tasks

Name	Tasks Allocated
Adeeb (p2107035)	<ul style="list-style-type: none"> <li>• Executive Summary</li> <li>• 2.1 Forensic Tools and Methodology <ul style="list-style-type: none"> <li>○ 2.1.1 Magnet Axiom</li> <li>○ 2.1.2 Small SEO Tools</li> </ul> </li> <li>• 2.2.1 Details of Jim Cloudy's Accounts</li> <li>• 2.2.2 Details of Jim Cloudy's Laptop</li> <li>• 2.2.3 Web Searches/URLs (Brother Chat &amp; AWS Amazon rootkey part only)</li> <li>• 2.2.5 Documents (.pptx and .csv files)</li> <li>• 2.3.1 Web Searches/URLs (Brother Chat &amp; AWS Amazon rootkey part only)</li> </ul>
Toh Yi Da (p2123488)	<ul style="list-style-type: none"> <li>• 1. Introduction</li> <li>• 2.2.3 Web Searches/URLs</li> <li>• 2.2.4 Media</li> <li>• 2.2.5 Documents (.docx files)</li> <li>• 2.3.1 Web Searches/URLs</li> <li>• 2.3.3 Documents (.docx files)</li> </ul>
Chua Mun Ling (p2123516)	<ul style="list-style-type: none"> <li>• 2.0 Detail Analysis</li> <li>• 2.2.4 Media</li> <li>• 2.2.6 Others</li> <li>• 2.3.3 Documents (Operation 2nd Hand Smoke.pptx)</li> <li>• 2.3.4 Others</li> </ul>

	• 2.4 Findings
--	----------------