Digital Forensics Investigative Report

Abdulla AlBassam / W23055814

KV5041

Word count: 3100

Table of Contents

Introduction:

Summary of Case:

The accused, Jim Cloudy, is currently under investigation following the discovery of documents suggesting plans for a politically motivated violent act. Digital copies of the suspect's RAM dump and hard disk image were recovered after his brother, Paul Cloudy, alerted authorities to concerning material stored in multiple cloud accounts belonging to the accused. The forensic analysis is expected to support the suspicion that Jim had developed and preserved plans for a "Lone Wolf" style attack.

Subject to investigation, but if found guilty, the digital evidence recovered may convict the suspect of multiple criminal offenses. These may include but are not limited to; (1) attempted domestic terrorism, (2) possession & dissemination of materials related to a planned violent or terror act, and (3) destruction of evidence (Virginia Law, 2024, 18.2-46.4).

Statement of Purpose:

The purpose of this report is to identify and analyse all suspicious digital artifacts from the suspect's devices to determine the presence of incriminating or exonerating evidence. The findings aim to assist other investigators and legal professionals in assessing whether the suspect was actively planning or preparing to commit a criminal offense(s).

Statement of Scope:

This document covers the forensic examination of a RAM and hard disk image provided by law enforcement supposedly belonging to the suspect. The scope of analysis includes user activity, recovered files, internet history, cloud storage, system logs, and evidence of planning or intent. Emphasis is placed on identifying signs of premeditated action and any supporting digital documentation.

The limitations of this investigation include:

- The original physical device was not on hand.
- Memory acquisition was not conducted live, limiting my analysis of volatile data to the provided RAM dump.
- Cloud storage accounts and any deleted files such as the various Google Doc Chats were not directly accessed; analysis is based on cached or recovered data.

- The investigation does not consider the psychological, social, or physical behaviour/state of the accused. **ONLY** digital evidence used to build a profile and timeline.
- Legal interpretation is outside the scope of this report; opinions and findings are presented for evidentiary purposes **ONLY**.

Forensic Examination:

Tools:

Software:	**Hardware**:
Autopsy (v4.22.2)	Apple Silicon M2 - MacOS: Sonoma 14.6.1 *
Volatility (v3.0)	CIS Lab Computers *

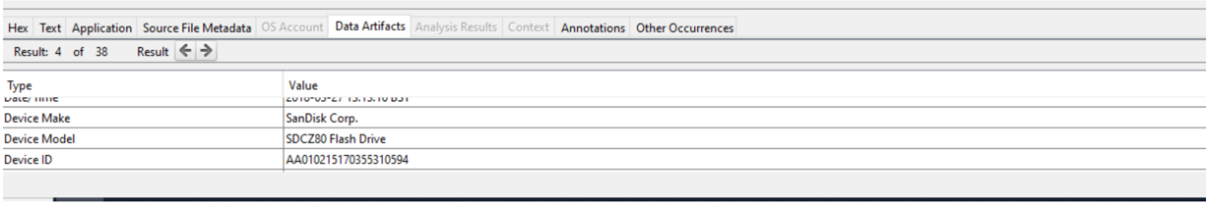
*MacOS used for the writing of this report only, forensics analysis conducted on CIS computers.

Evidence:

All evidence analysed was provided by the teaching team on Blackboard.

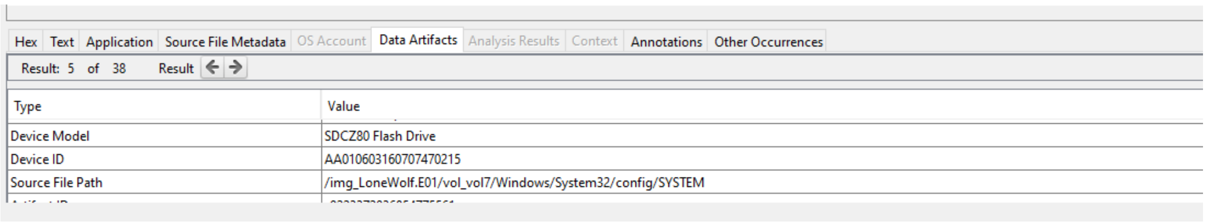
	Item	Description	Type
1	Hard Disk	In "Analysis"	H
2	Memory	In "Analysis"	RAM

Additional evidence of two other notable devices that had interacted with his computer was found, but no more information was able to be recovered.



Result: 4 of 38 Result

Type	Value
Date/Time	2018-03-27 13:13:10 BST
Device Make	SanDisk Corp.
Device Model	SDCZ80 Flash Drive
Device ID	AA010215170355310594



Type	Value
Device Model	SDCZ80 Flash Drive
Device ID	AA010603160707470215
Source File Path	/img_LoneWolf.E01/vol_vol7/Windows/System32/config/SYSTEM

Analysis:

Brief description of evidence items:

Original Device:

Laptop, Dell, Model Latitude E6430 ATG, Service Tag: DB2MN22.Evidence Property/Custody Document (EPCD) Item 3 Document Number 001-18.

Hard Disk:

Samsung SSD 850 PRO 512GB, Serial Number: S250NSAG505708H

Memory:

Windows 10 x64

Process Breakdown:

The forensic process began by analysing the provided memory dump using Volatility Workbench. Plugins such as pslist, psscan, and netscan was used to identify suspicious process behaviour and any evidence of remote access. Following this, the hard disk image was examined in Autopsy. The investigation involved reviewing web and search history, which revealed firearm-related content, escape planning, and encrypted communications. The most critical evidence was found on the suspect's desktop, where documents such as the "Cloudy Manifesto" and "Planning" were located. Although all areas of the drive were accessed and meticulously analysed, the majority of relevant artifacts were discovered within the high activity locations mentioned.

Memory Dump Examination:

The memory dump from Jim's laptop was analysed using Volatility Workbench. The process listings (pslist, psscan) showed multiple instances of cmd.exe and powershell.exe, which may not be suspicious on their own, but both of which are commonly used for scripting and exploitation (Nappy, 2025). Some processes had unusual extremely short lifespans, suggesting possible automation.

The most notable findings came from the netscan search, which showed that both cmd.exe and powershell.exe had open or recently closed network connections. This is generally abnormal and potentially indicates remote access. Additionally, an unfamiliar execution, TempApp.exe, also appeared with network activity, further suggesting suspicious behaviour.

Due to limitations in the analysis the exact purpose of these activities and availability of malware is unclear. However, the combination of command line tools communicating over the network and unexplained executables strongly indicates malicious activity. This investigation will shift focus onto the evidence found on the suspects hard drive, as that should reveal more than the small snapshot of the RAM dump. Screenshots of the results found based on the commands used are found in the appendix for clarity.

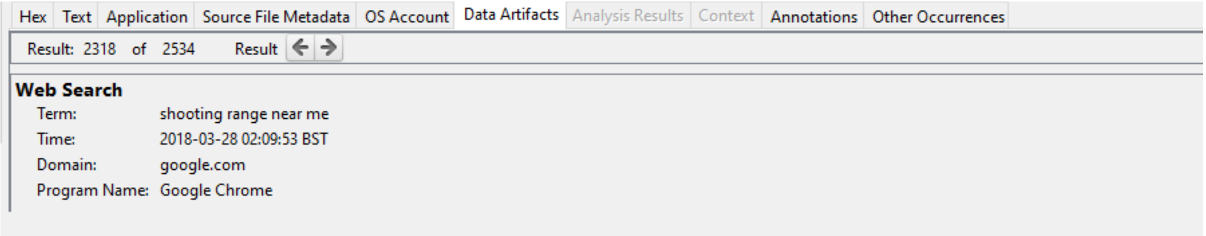
Autopsy Investigation:

The forensic analysis conducted focused on identifying digital artifacts indicating intent to commit the crimes accused of. Tagged evidence was grouped by theme to establish both motive and potential action. The following subsections detail each category of findings in hopes of building a timeline of events. Not every piece of evidence tagged has been mentioned/figured in efforts of conciseness. However, the Autopsy report includes everything found used to formulate my conclusions. The supplementary figures should be seen as evidence of acquisition.

---

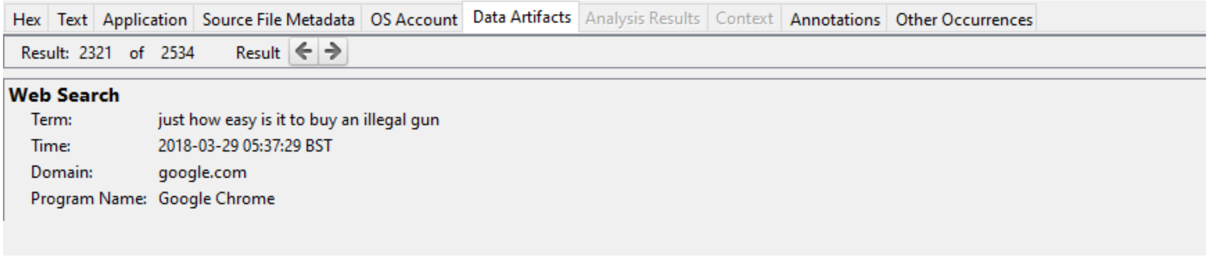
1. Mentions of Guns

A significant amount of search activity volume related to firearms was found. Web search history revealed the suspect had searched for gun laws in multiple states including firearm restrictions (Figure 4). YouTube search/viewing history included videos from various gun advocating channels and firearm reviews (Figure 7). He frequently searched for local gun stores (Figure 3). The most notable searches were those for automatic weapons (Figure 5). These digital artifacts suggest a strong and repeated interest in acquiring and understanding weapons (Figure 2 & 7) which is notable when put in context alongside other materials discovered.



Web Search
Term: shooting range near me
Time: 2018-03-28 02:09:53 BST
Domain: google.com
Program Name: Google Chrome

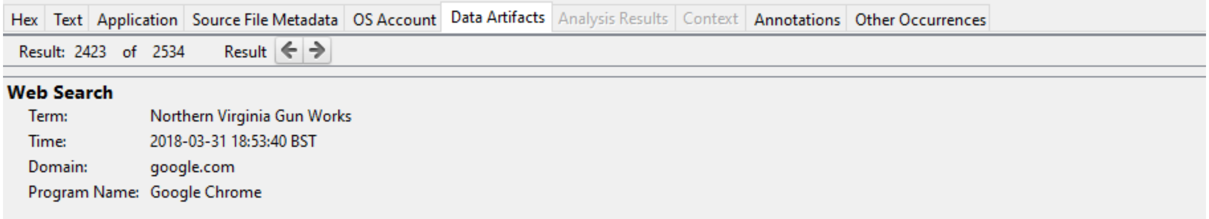
Figure 1: Search of a nearby shooting range



Web Search

Term: just how easy is it to buy an illegal gun
Time: 2018-03-29 05:37:29 BST
Domain: google.com
Program Name: Google Chrome

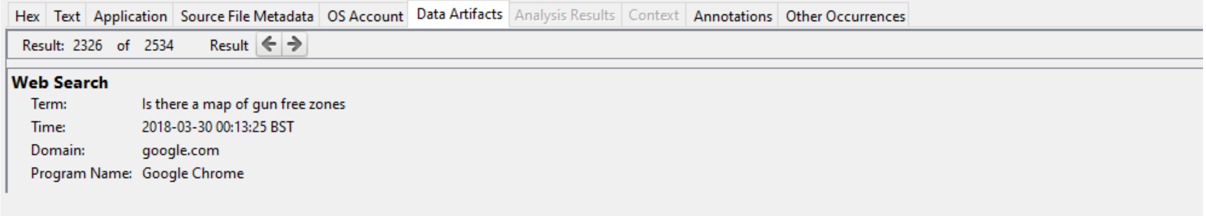
Figure 2: Looking up how easy it is to buy an illegal gun



Web Search

Term: Northern Virginia Gun Works
Time: 2018-03-31 18:53:40 BST
Domain: google.com
Program Name: Google Chrome

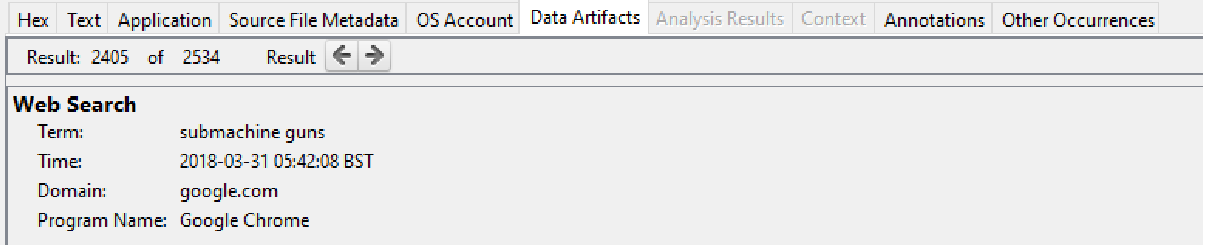
Figure 3: Accessed an Online Gun Store



Web Search

Term: Is there a map of gun free zones
Time: 2018-03-30 00:13:25 BST
Domain: google.com
Program Name: Google Chrome

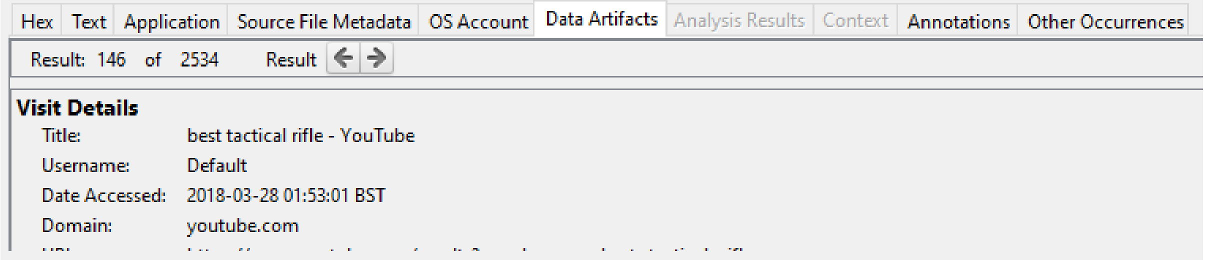
Figure 4: Looking up locations of "gun free zones"



Web Search

Term: submachine guns
Time: 2018-03-31 05:42:08 BST
Domain: google.com
Program Name: Google Chrome

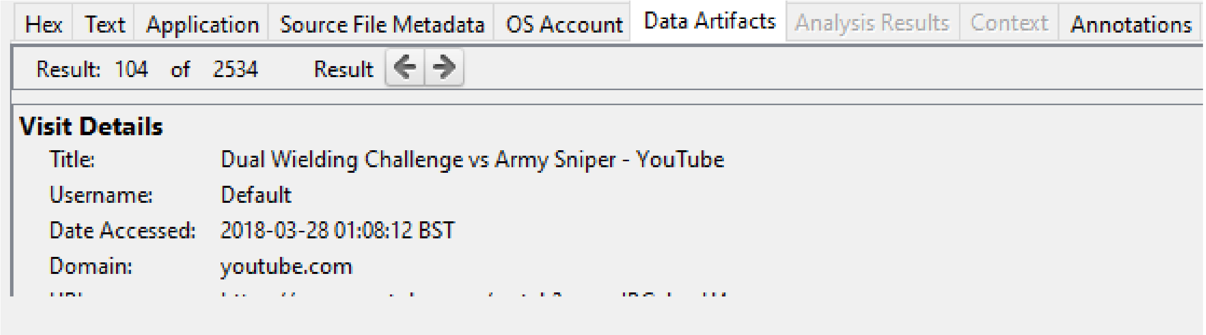
Figure 5: One of many Automatic Weapon Search



Visit Details

Title: best tactical rifle - YouTube
Username: Default
Date Accessed: 2018-03-28 01:53:01 BST
Domain: youtube.com

Figure 6: One of Many Searches for Rifles



Result: 104 of 2534

Visit Details

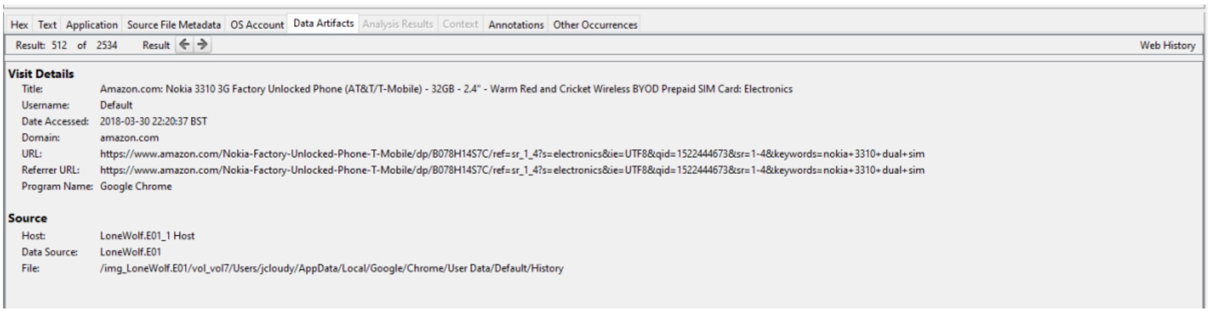
Title: Dual Wielding Challenge vs Army Sniper - YouTube
Username: Default
Date Accessed: 2018-03-28 01:08:12 BST
Domain: youtube.com

Figure 7: YouTube Gun Related Content

---

2. Possible Burner Phone

The suspect performed repeated web searches for Nokia dual sim phones including review videos (not pictured) and Amazon product listings (Figure 8). This behaviour is particularly suspicious given that the case takes place in 2018, and the model of the phone that he was viewing on Amazon was "Factory Unlocked", meaning that the phone, and in turn, the user, is not tied to a specific mobile carrier and can effectively be used with any SIM card worldwide. The phone would have been 5 years old at the time of the case, and even more outdated in terms of its technology. It is worth noting that Dual-SIM phones are often used in covert communication, suggesting possible intent to avoid detection.



Result: 512 of 2534

Visit Details

Title: Amazon.com: Nokia 3310 3G Factory Unlocked Phone (AT&T/T-Mobile) - 32GB - 2.4" - Warm Red and Cricket Wireless BYOD Prepaid SIM Card: Electronics
Username: Default
Date Accessed: 2018-03-30 22:20:37 BST
Domain: amazon.com
URL: https://www.amazon.com/Nokia-Factory-Unlocked-Phone-T-Mobile/dp/B078H14S7C/ref=sr_1_4?s=electronics&ie=UTF8&qid=1522444673&sr=1-4&keywords=nokia+3310+dual+sim
Referrer URL: https://www.amazon.com/Nokia-Factory-Unlocked-Phone-T-Mobile/dp/B078H14S7C/ref=sr_1_4?s=electronics&ie=UTF8&qid=1522444673&sr=1-4&keywords=nokia+3310+dual+sim
Program Name: Google Chrome

Source

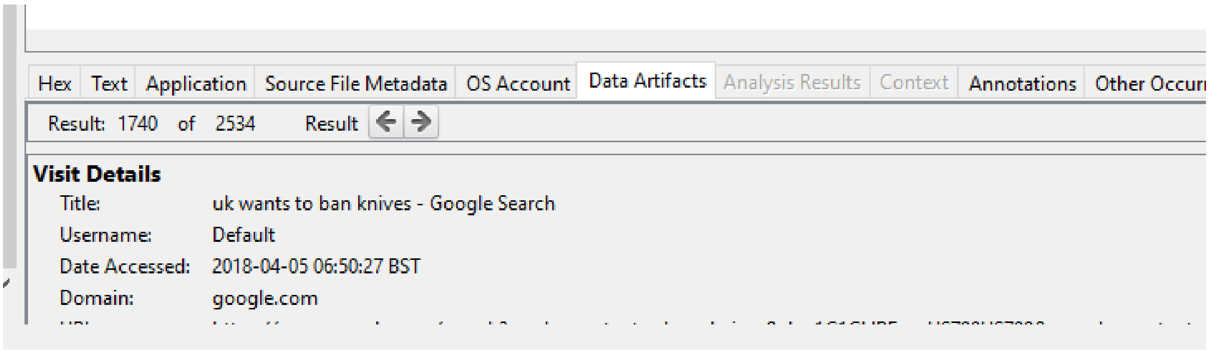
Host: LoneWolf.E01_1 Host
Data Source: LoneWolf.E01
File: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/History

Figure 8: Amazon Search for a Factory Unlocked Dual-Sim Phone

---

3. Interest in UK Law and Crime Rates

Various articles were accessed that examined the relationship between gun control legislation and crime rates in the UK (Figure 9 as reference, exact search tagged on autopsy report). The suspect appeared to be researching whether stricter gun laws result in fewer crimes and was especially focused on sources that argued otherwise (Figure 10). This may reflect an effort to build justification for the views he expressed in the discovered manifesto.



Visit Details

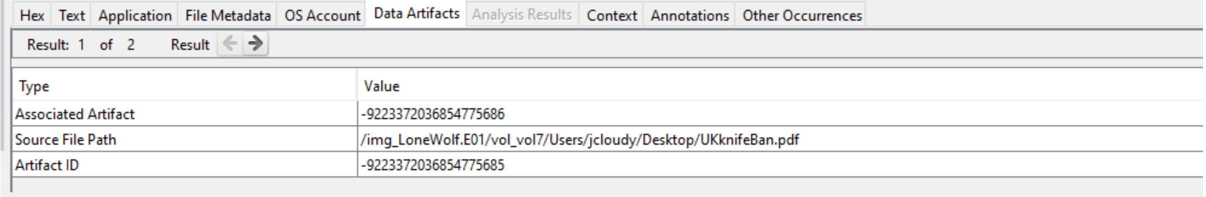
Title: uk wants to ban knives - Google Search

Username: Default

Date Accessed: 2018-04-05 06:50:27 BST

Domain: google.com

Figure 9: One of Many UK Crime/Knife/Gun Related Searches

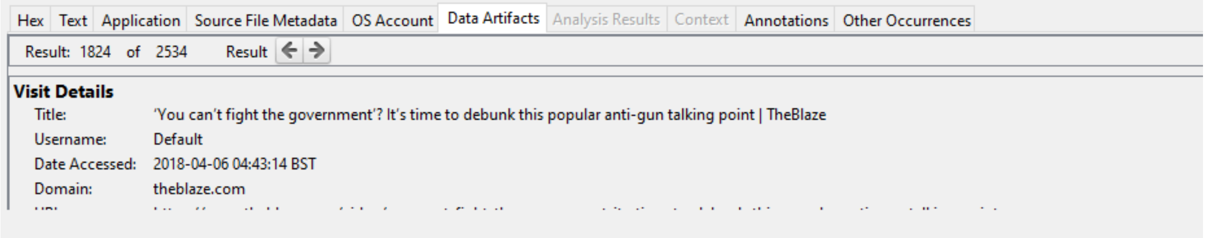


Type	Value
Associated Artifact	-9223372036854775686
Source File Path	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/UKknifeBan.pdf
Artifact ID	-9223372036854775685

Figure 10: One of Many UK Crime/Knife/Gun Related Searches

4. Extreme Right-Wing and Gun Rights Advocacy

Web history and social media posts/searches revealed frequent visits to content associated with far-right ideology and gun rights extremism, including Facebook and Twitter searches mentioning “Molon Labe”, which is Greek for “come and take them”. It is a slogan used to “express defiance and is frequently employed by gun-rights advocates in the US.” (Dictionary.com, n.d.) (Figures 11-14). These visits were routine, suggesting alignment or affiliation with communities that often promote anti-government rhetoric.



Visit Details

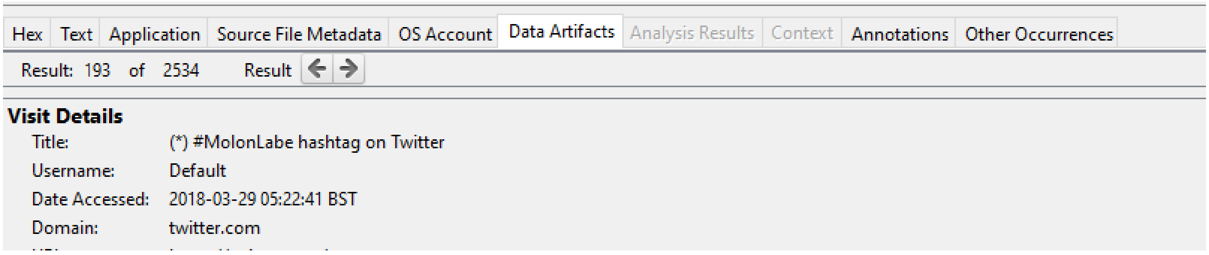
Title: ‘You can’t fight the government’? It’s time to debunk this popular anti-gun talking point | TheBlaze

Username: Default

Date Accessed: 2018-04-06 04:43:14 BST

Domain: theblaze.com

Figure 11: Anti-gov related search



Visit Details

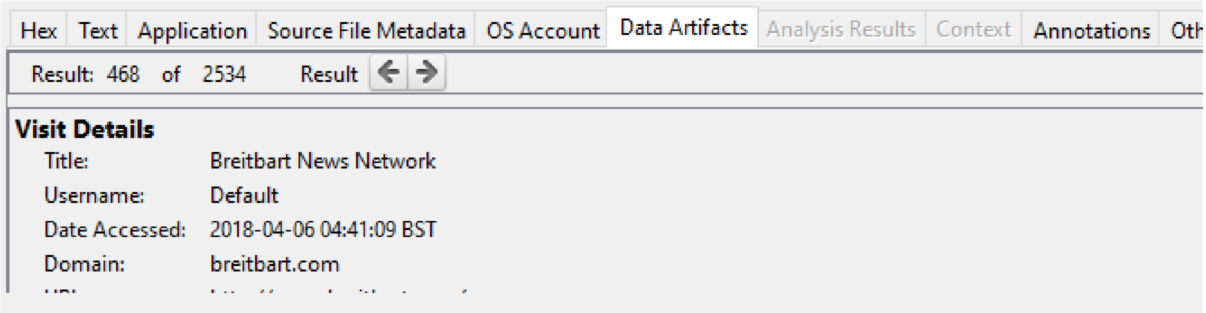
Title: (*) #MolonLabe hashtag on Twitter

Username: Default

Date Accessed: 2018-03-29 05:22:41 BST

Domain: twitter.com

Figure 12: Molon Labe Search

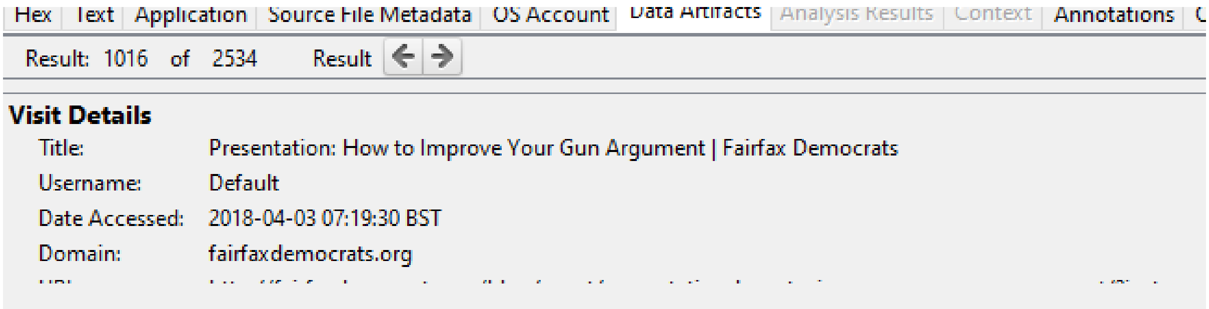


Result: 468 of 2534 Result

Visit Details

Title: Breitbart News Network
Username: Default
Date Accessed: 2018-04-06 04:41:09 BST
Domain: breitbart.com

Figure 13: Far-Right News Network



Result: 1016 of 2534 Result

Visit Details

Title: Presentation: How to Improve Your Gun Argument | Fairfax Democrats
Username: Default
Date Accessed: 2018-04-03 07:19:30 BST
Domain: fairfaxdemocrats.org

Figure 14

---

5. Manifesto

A Google Document containing Jim's manifesto was recovered in its entirety. Several images embedded within it were retrieved (pictured and analysed below).

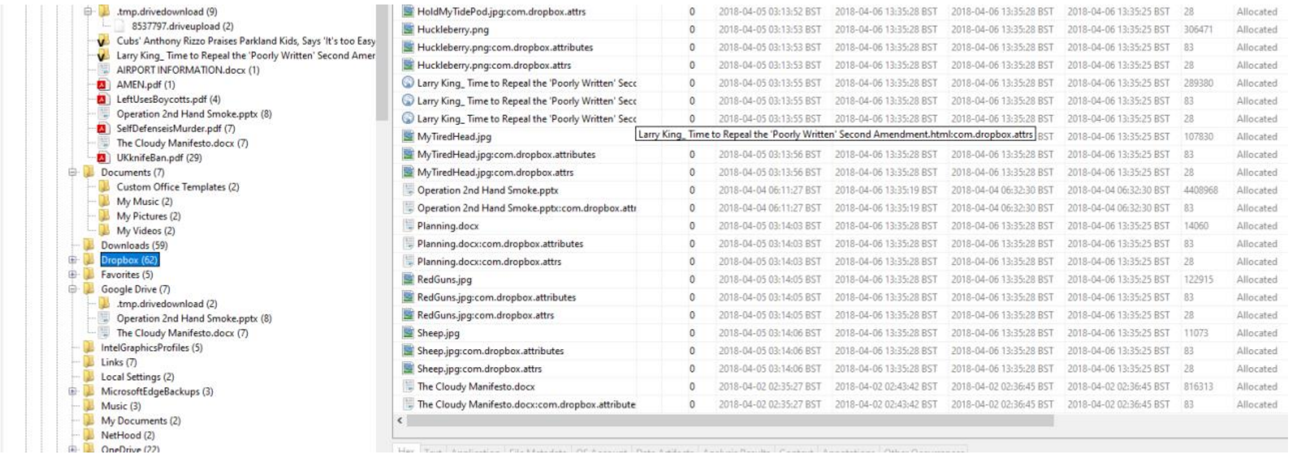
Figure 15 depicts a poster that flips the famous slogan defending gun ownership "from my cold dead hands", seemingly mocking and opposing it. The cowboy seems to represent old school gun culture and how it may be seen as "cool".

Figure 16 shows a group of possible activists comparing gun control movements are similar to those who supported Hitler, Castro, and Zhedong. This is evident propaganda, using fear from past historical figures and events to discredit gun control efforts. It attempts to illicit distrust in gun control activism by linking it to authoritarian regimes.

Figures 17 and 18 could be described as "memes", poking fun of sensitive topics through humour. Figure 18 promotes the idea of rugged individualism and emotional isolation as a good thing, both often associated with those who reject societal rules or feel misunderstood. (Webster, n.d.). The "lone wolf" mindset is also often romanticized in extremist or anti-authority narratives. Figure 17 shows a 'satirical' take on former democratic senator Dianne Feinstein's 'logic'. It is meant to undermine gun control arguments by presenting them as naive. It also frames disarming as unrealistic and mocks democratic political figures.

The text within the document titled "*The Cloudy Manifesto*" serves as clear ideological justification for a premeditated attack, specifically in the context of anti-government and anti-gun control extremism once again. The language throughout indicates a high level of radicalization, social isolation, and a willingness to act on extremist beliefs. Jim explicitly

states that collateral damage is acceptable, reinforcing the mindset that prioritizes ideology over tangible human life. The manifesto expresses deep anti-government sentiment, portraying state institutions as oppressive and untrustworthy. References to figures like Clive Bundy and the Snake River Ranchers, known for armed standoffs with authorities, are used to support the claim that disarming the people leads to the government overreaching their ground. It also includes a heated critique of gun control laws, arguing that legislation is ineffective at stopping crime and only serves to disempower law abiding citizens. Jim compares gun laws to other laws that are frequently broken, such as drugs and speeding, in an attempt to dismiss the laws effectiveness. Most alarmingly, the manifesto escalates into an explicit call for attack: he announces his intention to break the law and carry out an attack to "prove" that gun-free zones are ineffective. The document ends with disturbing imagery of mass casualties, "you will soon see when the blood has been shed and the defenceless bodies stacked high…" positioning the author as a "lone wolf" and so called "revolutionary" intended on making history through violence. He uploaded this document, along with others, on cloud storage services such as Dropbox to "preserve his work", as he says in the manifesto (Figure 15).



```
    .tmp.drivedownload (9)
        8537797.driveupload (2)
    Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy
    Larry King_ Time to Repeal the 'Poorly Written' Second Amer
    AIRPORT INFORMATION.docx (1)
    AMEN.pdf (1)
    LeftUsesBoycotts.pdf (4)
    Operation 2nd Hand Smoke.pptx (8)
    SelfDefenseisMurder.pdf (7)
    The Cloudy Manifesto.docx (7)
    UKknifeBan.pdf (29)
Documents (7)
    Custom Office Templates (2)
    My Music (2)
    My Pictures (2)
    My Videos (2)
Downloads (59)
Dropbox (62)
Favorites (5)
Google Drive (7)
    .tmp.drivedownload (2)
    Operation 2nd Hand Smoke.pptx (8)
    The Cloudy Manifesto.docx (7)
IntelGraphicsProfiles (5)
Links (7)
Local Settings (2)
MicrosoftEdgeBackups (3)
Music (3)
My Documents (2)
NetHood (2)
OneDrive (22)
```

HoldMyTidePod.jpg:com.dropbox.attrs	0	2018-04-05 03:13:52 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated
Huckleberry.png	0	2018-04-05 03:13:53 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	306471	Allocated
Huckleberry.png:com.dropbox.attributes	0	2018-04-05 03:13:53 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated
Huckleberry.png:com.dropbox.attrs	0	2018-04-05 03:13:53 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated
Larry King_ Time to Repeal the 'Poorly Written' Secc	0	2018-04-05 03:13:55 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	289380	Allocated
Larry King_ Time to Repeal the 'Poorly Written' Secc	0	2018-04-05 03:13:55 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated
Larry King_ Time to Repeal the 'Poorly Written' Secc	0	2018-04-05 03:13:55 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated
MyTiredHead.jpg	Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html:com.dropbox.attrs			BST	2018-04-06 13:35:25 BST	107830	Allocated
MyTiredHead.jpg:com.dropbox.attributes	0	2018-04-05 03:13:56 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated
MyTiredHead.jpg:com.dropbox.attrs	0	2018-04-05 03:13:56 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated
Operation 2nd Hand Smoke.pptx	0	2018-04-04 06:11:27 BST	2018-04-06 13:35:19 BST	2018-04-04 06:32:30 BST	2018-04-04 06:32:30 BST	4408968	Allocated
Operation 2nd Hand Smoke.pptx:com.dropbox.attr	0	2018-04-04 06:11:27 BST	2018-04-06 13:35:19 BST	2018-04-04 06:32:30 BST	2018-04-04 06:32:30 BST	83	Allocated
Planning.docx	0	2018-04-05 03:14:03 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	14060	Allocated
Planning.docx:com.dropbox.attributes	0	2018-04-05 03:14:03 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated
Planning.docx:com.dropbox.attrs	0	2018-04-05 03:14:03 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated
RedGuns.jpg	0	2018-04-05 03:14:05 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	122915	Allocated
RedGuns.jpg:com.dropbox.attributes	0	2018-04-05 03:14:05 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated
RedGuns.jpg:com.dropbox.attrs	0	2018-04-05 03:14:05 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated
Sheep.jpg	0	2018-04-05 03:14:06 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	11073	Allocated
Sheep.jpg:com.dropbox.attributes	0	2018-04-05 03:14:06 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	83	Allocated
Sheep.jpg:com.dropbox.attrs	0	2018-04-05 03:14:06 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:28 BST	2018-04-06 13:35:25 BST	28	Allocated
The Cloudy Manifesto.docx	0	2018-04-02 02:35:27 BST	2018-04-02 02:43:42 BST	2018-04-02 02:36:45 BST	2018-04-02 02:36:45 BST	816313	Allocated
The Cloudy Manifesto.docx:com.dropbox.attribute	0	2018-04-02 02:35:27 BST	2018-04-02 02:43:42 BST	2018-04-02 02:36:45 BST	2018-04-02 02:36:45 BST	83	Allocated

Figure 15: Manifesto was found in Dropbox (accessible on "desktop", not pictured)

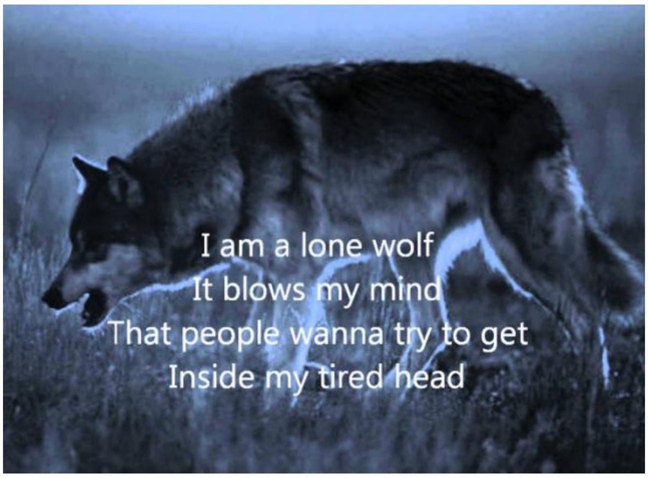


Figure 17: Lone Wolf Meme

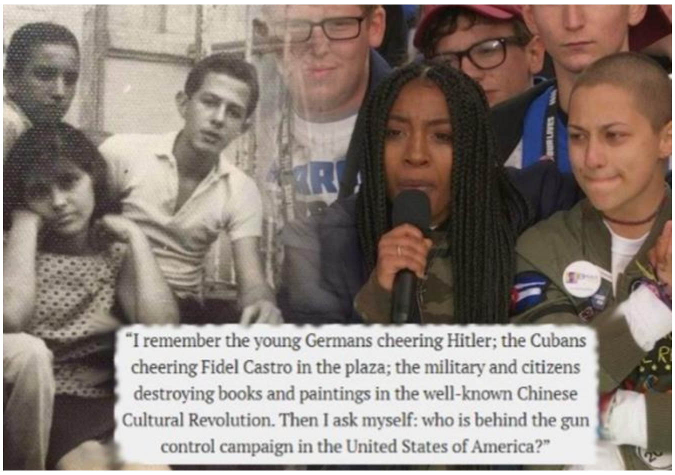

"I remember the young Germans cheering Hitler; the Cubans cheering Fidel Castro in the plaza; the military and citizens destroying books and paintings in the well-known Chinese Cultural Revolution. Then I ask myself: who is behind the gun control campaign in the United States of America?"

Figure 16: Gun Control + Historical Regime

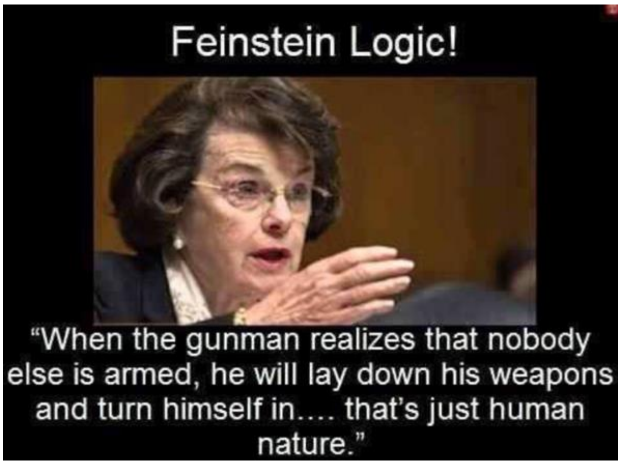

Feinstein Logic!
"When the gunman realizes that nobody else is armed, he will lay down his weapons and turn himself in.... that's just human nature."

Figure 18: Feinstein "Logic" Meme

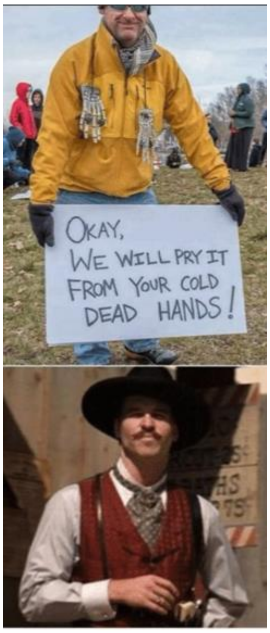


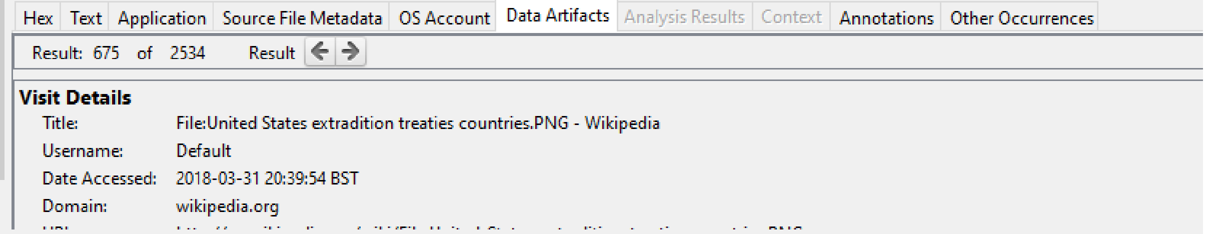
Figure 19: Cold Dead Hands Mock and Cowboy

DV6

6. Evidence of a Planned Attack Followed by Fleeing / Re-location:

The suspect used Google Maps to examine the Cascades Library, which so happens to be at the exact location of an anti-gun rally (Figure 31) that Jim had previously mentioned in his planning PowerPoint document (Not on this document but found on the Autopsy report). He also has various web searches preluding to anti-gun rallies in his area. Various searches related to police response times in different areas were retrieved (Figure 27).

The suspects web searches and access history indicate that he was planning on relocating to Indonesia. There are multiple instances of him searching for countries that have nonextradition treaties with the U.S. One of the many articles relating to fleeing the country he accessed was titled "The Best Countries for Your Escape Plan". Upon further research, Indonesia and other Southeast Asian countries frequent these lists (Asean, 1979). He also searched for property listings (Figure 33), airport routes from the location of his supposed planned attack in Virginia to Bali (Figures 24 & 26), and how to move money undetected (Figure 22). Evidence of confirmation of ticket bookings from the U.S to Bali and back were also found, suggesting he intended to leave and later return (Figure 30).

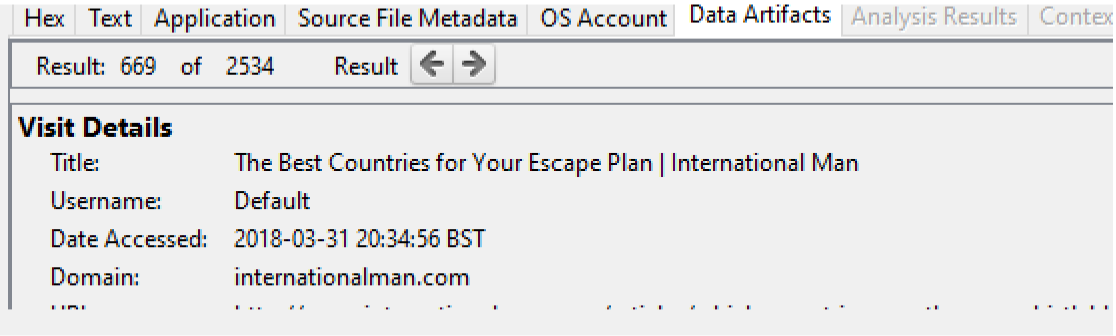


Result: 675 of 2534

Visit Details

Title: File:United States extradition treaties countries.PNG - Wikipedia
Username: Default
Date Accessed: 2018-03-31 20:39:54 BST
Domain: wikipedia.org

Figure 20: Extradition Search

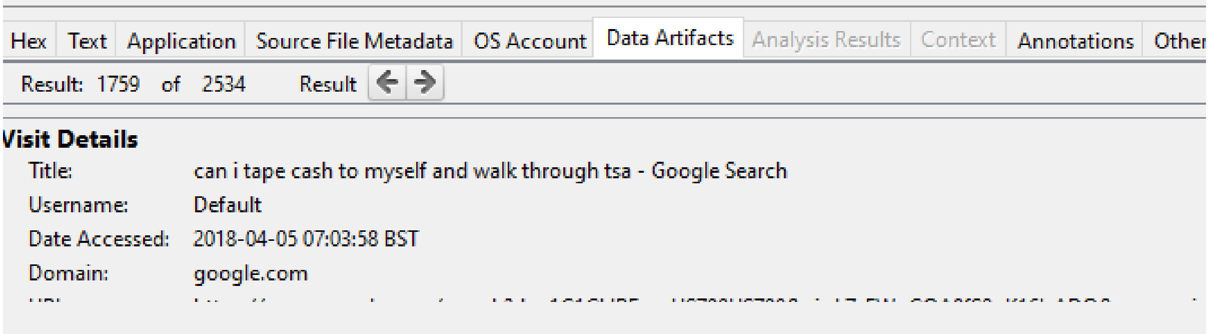


Result: 669 of 2534

Visit Details

Title: The Best Countries for Your Escape Plan | International Man
Username: Default
Date Accessed: 2018-03-31 20:34:56 BST
Domain: internationalman.com

Figure 21: Blatant Escape Plan Search

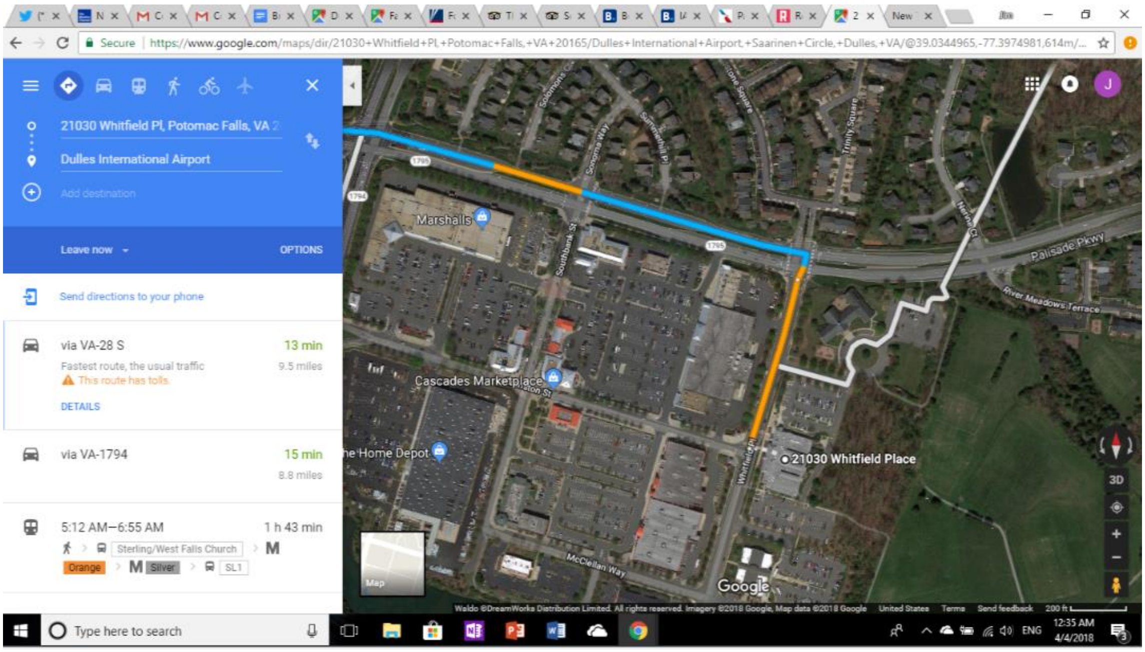


Result: 1759 of 2534

Visit Details

Title: can i tape cash to myself and walk through tsa - Google Search
Username: Default
Date Accessed: 2018-04-05 07:03:58 BST
Domain: google.com

Figure 22: Smuggling Cash Query



https://www.google.com/maps/dir/21030+Whitfield+Pl,+Potomac+Falls,+VA+20165/Dulles+International+Airport,+Saarinen+Circle,+Dulles,+VA/@39.0344965,-77.3974981,614m/...

21030 Whitfield Pl, Potomac Falls, VA 2

Dulles International Airport

Add destination

Leave now OPTIONS

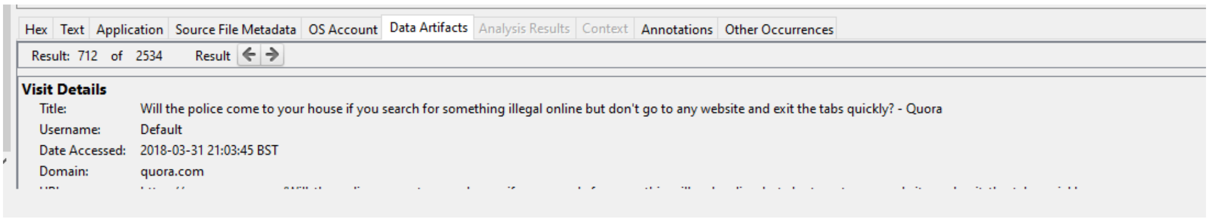
Send directions to your phone

via VA-28 S 13 min
Fastest route, the usual traffic 9.5 miles
This route has tolls.
DETAILS

via VA-1794 15 min
8.8 miles

5:12 AM—6:55 AM 1 h 43 min
Sterling/West Falls Church M
Orange M Silver SL1

Figure 24: Google Maps from the Library to Dulles Airport



Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 712 of 2534 Result

Visit Details

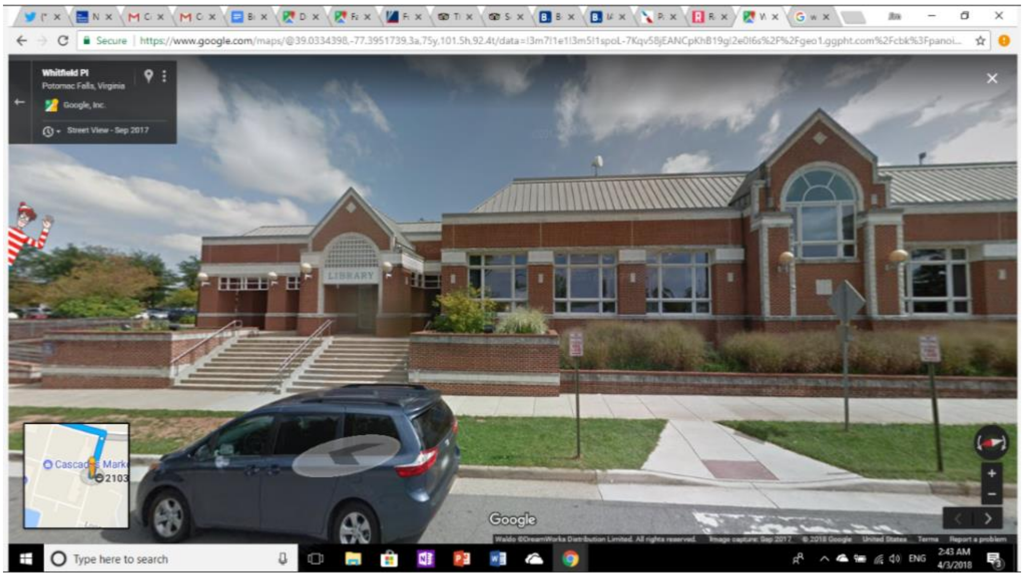
Title: Will the police come to your house if you search for something illegal online but don't go to any website and exit the tabs quickly? - Quora

Username: Default

Date Accessed: 2018-03-31 21:03:45 BST

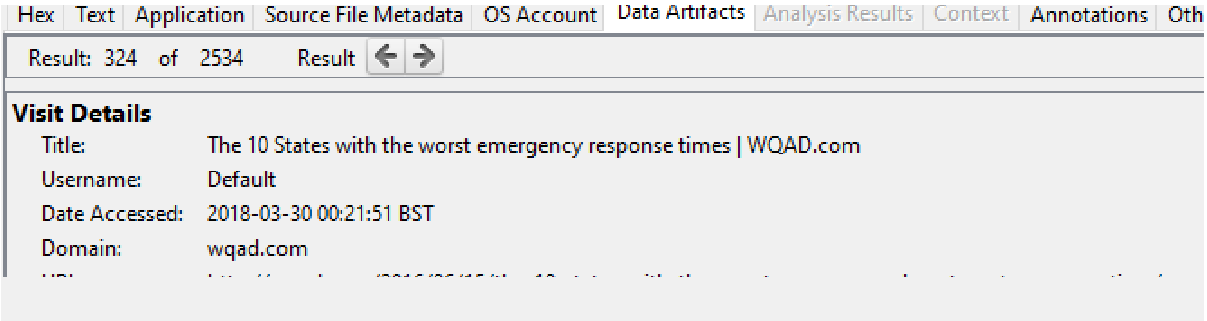
Domain: quora.com

Figure 25: One of Many Pre-Offense Risk-Aware Searches



https://www.google.com/maps/@39.0334398,-77.3951739,3a,75y,101.5h,92.4t/data=!3m7!1e1!3m5!1spoL-7Kqv58jEANCpKhB19g!2e0!6s%2F%2Fgeo1.ggpht.com%2Fcbk%3Fpanoi...

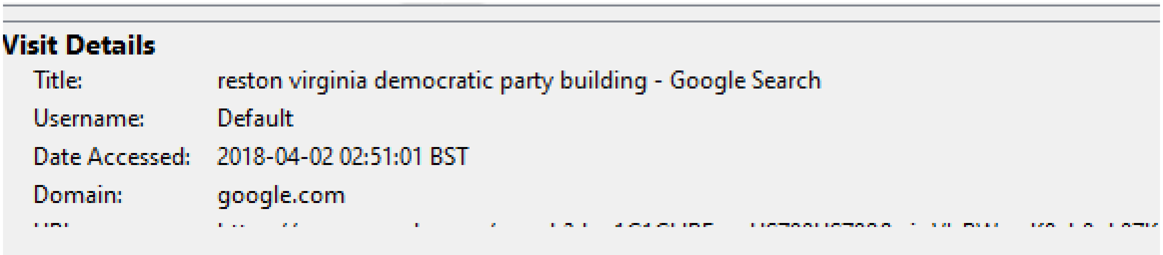
Figure 26: A Street-View Image of the Library



Visit Details

Title: The 10 States with the worst emergency response times | WQAD.com
Username: Default
Date Accessed: 2018-03-30 00:21:51 BST
Domain: wqad.com

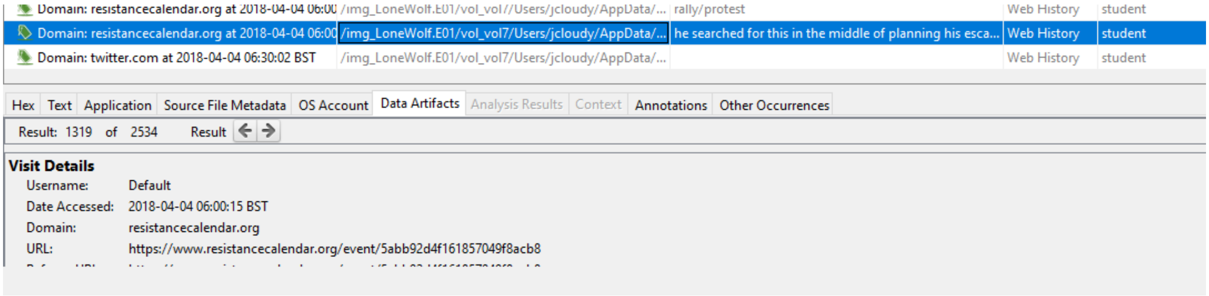
Figure 27: Emergency Response Time Search



Visit Details

Title: reston virginia democratic party building - Google Search
Username: Default
Date Accessed: 2018-04-02 02:51:01 BST
Domain: google.com

Figure 28: Possible Alternate Target

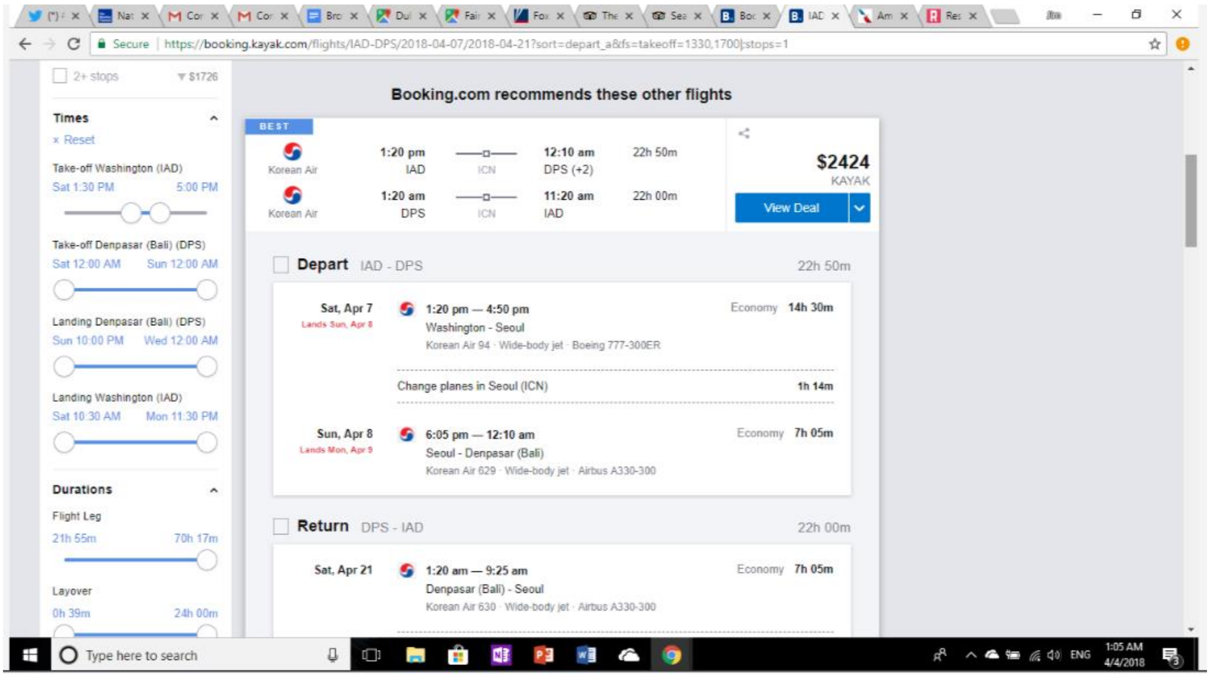


Domain: resistancecalendar.org at 2018-04-04 06:00	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/...	rally/protest	Web History	student
Domain: resistancecalendar.org at 2018-04-04 06:00	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/...	he searched for this in the middle of planning his esca...	Web History	student
Domain: twitter.com at 2018-04-04 06:30:02 BST	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/...		Web History	student

Visit Details

Username: Default
Date Accessed: 2018-04-04 06:00:15 BST
Domain: resistancecalendar.org
URL: https://www.resistancecalendar.org/event/5abb92d4f161857049f8acb8

Figure 29: A calendar used to organize protests related to political activism



https://booking.kayak.com/flights/IAD-DPS/2018-04-07/2018-04-21?sort=depart_a&fs=takeoff=1330,1700;stops=1

Booking.com recommends these other flights

BEST

Korean Air	1:20 pm IAD	ICN	12:10 am DPS (+2)	22h 50m	$2424 KAYAK
Korean Air	1:20 am DPS	ICN	11:20 am IAD	22h 00m	View Deal

Times

Take-off Washington (IAD): Sat 1:30 PM – 5:00 PM

Take-off Denpasar (Bali) (DPS): Sat 12:00 AM – Sun 12:00 AM

Landing Denpasar (Bali) (DPS): Sun 10:00 PM – Wed 12:00 AM

Landing Washington (IAD): Sat 10:30 AM – Mon 11:30 PM

Durations

Flight Leg: 21h 55m – 70h 17m

Layover: 0h 39m – 24h 00m

□ Depart IAD - DPS 22h 50m

Sat, Apr 7 (Lands Sun, Apr 8) — 1:20 pm — 4:50 pm, Washington - Seoul, Korean Air 94 · Wide-body jet · Boeing 777-300ER — Economy 14h 30m

Change planes in Seoul (ICN) 1h 14m

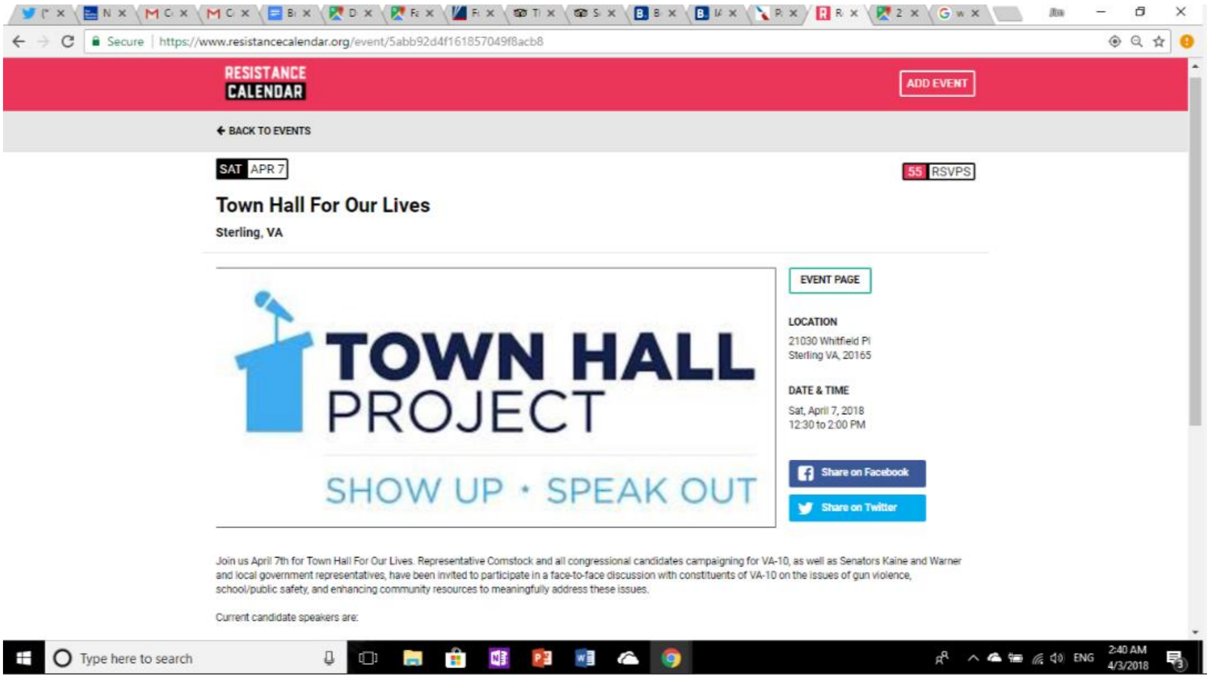
Sun, Apr 8 (Lands Mon, Apr 9) — 6:05 pm — 12:10 am, Seoul - Denpasar (Bali), Korean Air 629 · Wide-body jet · Airbus A330-300 — Economy 7h 05m

□ Return DPS - IAD 22h 00m

Sat, Apr 21 — 1:20 am — 9:25 am, Denpasar (Bali) - Seoul, Korean Air 630 · Wide-body jet · Airbus A330-300 — Economy 7h 05m

1:05 AM 4/4/2018

Figure 30: Booking.com ticket booking page



https://www.resistancecalendar.org/event/5abb92d4f161857049f8acb8

RESISTANCE CALENDAR

ADD EVENT

BACK TO EVENTS

SAT APR 7

55 RSVPS

Town Hall For Our Lives

Sterling, VA

EVENT PAGE

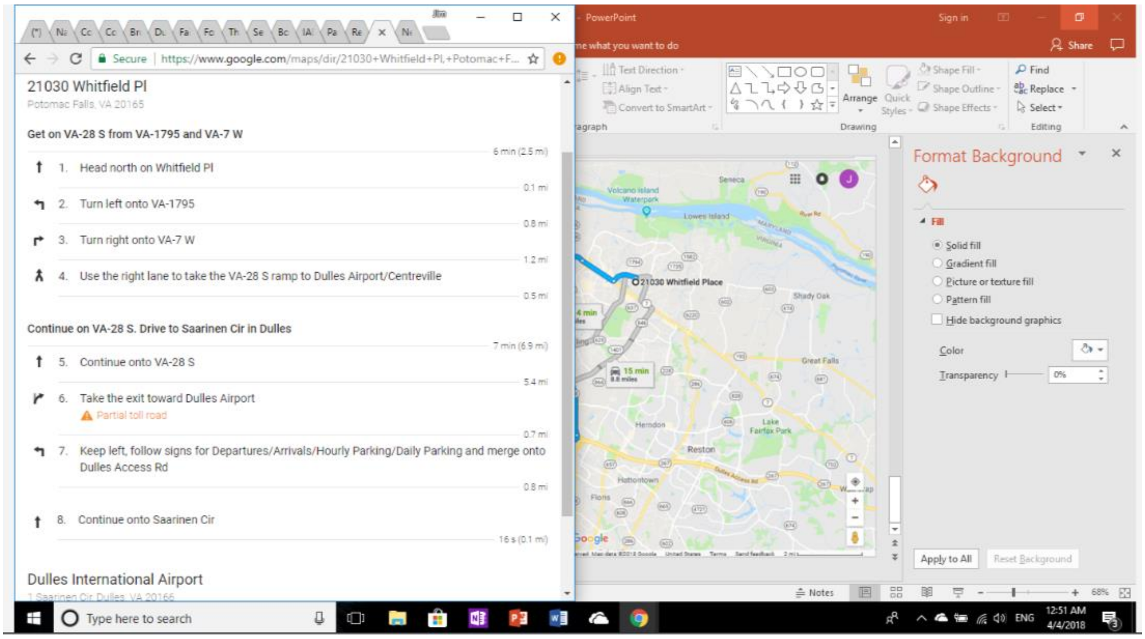
LOCATION
21030 Whitfield Pl
Sterling VA, 20165

DATE & TIME
Sat, April 7, 2018
12:30 to 2:00 PM

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

Current candidate speakers are:

Figure 31: The Main Point of Attack based on Manifesto



https://www.google.com/maps/dir/21030+Whitfield+Pl,+Potomac+F...

21030 Whitfield Pl
Potomac Falls, VA 20165

Get on VA-28 S from VA-1795 and VA-7 W — 6 min (2.5 mi)

1. Head north on Whitfield Pl — 0.1 mi
2. Turn left onto VA-1795 — 0.8 mi
3. Turn right onto VA-7 W — 1.2 mi
4. Use the right lane to take the VA-28 S ramp to Dulles Airport/Centreville — 0.5 mi

Continue on VA-28 S. Drive to Saarinen Cir in Dulles — 7 min (6.9 mi)

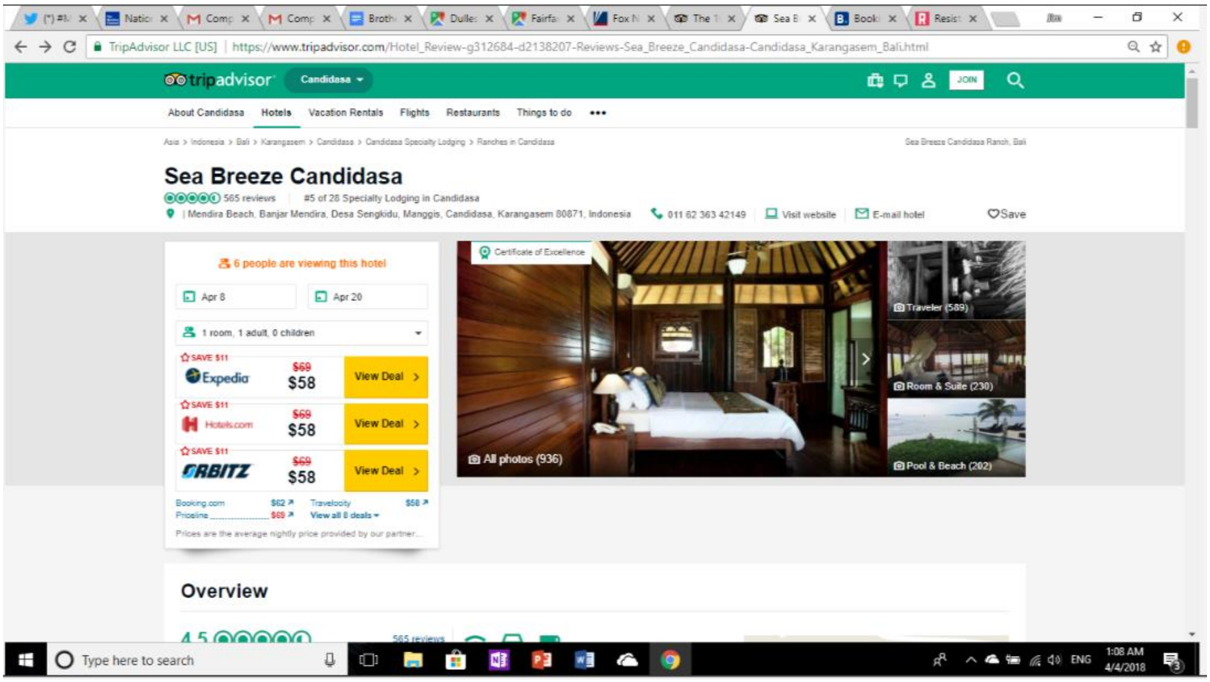
5. Continue onto VA-28 S — 5.4 mi
6. Take the exit toward Dulles Airport
   ⚠ Partial toll road — 0.7 mi
7. Keep left, follow signs for Departures/Arrivals/Hourly Parking/Daily Parking and merge onto Dulles Access Rd — 0.8 mi
8. Continue onto Saarinen Cir — 16 s (0.1 mi)

Dulles International Airport
1 Saarinen Cir, Dulles, VA 20166

Format Background

Fill
● Solid fill
○ Gradient fill
○ Picture or texture fill
○ Pattern fill
□ Hide background graphics
Color
Transparency 0%

Figure 32: Another similar Google Maps search



https://www.tripadvisor.com/Hotel_Review-g312684-d2138207-Reviews-Sea_Breeze_Candidasa-Candidasa_Karangasem_Bali.html

About Candidasa | Hotels | Vacation Rentals | Flights | Restaurants | Things to do

Asia > Indonesia > Bali > Karangasem > Candidasa > Candidasa Specialty Lodging > Ranches in Candidasa

Sea Breeze Candidasa

565 reviews | #5 of 28 Specialty Lodging in Candidasa

Mendira Beach, Banjar Mendira, Desa Sengkidu, Manggis, Candidasa, Karangasem 80871, Indonesia | 011 62 363 42149 | Visit website | E-mail hotel | ♡Save

6 people are viewing this hotel

Apr 8 | Apr 20

1 room, 1 adult, 0 children

SAVE $11 Expedia	~~$69~~ $58	View Deal
SAVE $11 Hotels.com	~~$69~~ $58	View Deal
SAVE $11 ORBITZ	~~$69~~ $58	View Deal

Booking.com	$62	Travelocity	$58
Priceline	$69	View all 8 deals	

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

Certificate of Excellence
All photos (936)
Traveler (589)
Room & Suite (230)
Pool & Beach (202)

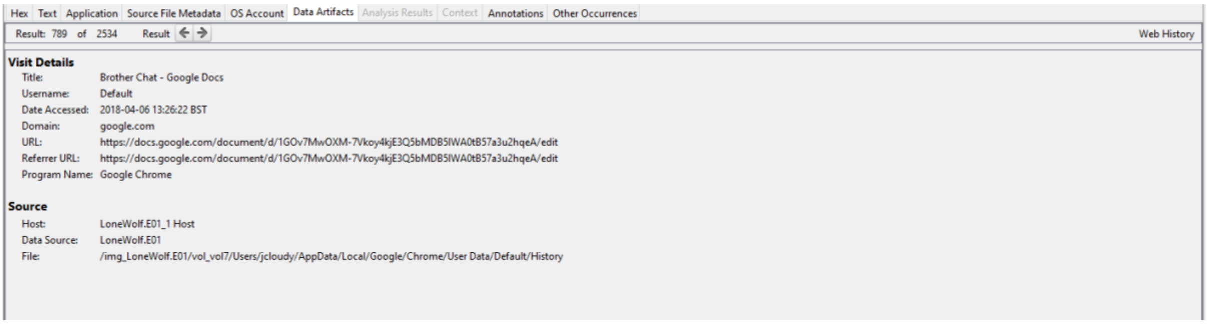
Overview

4.5 565 reviews

Figure 33: Property Search in Indonesia

7. Use of Google Docs as Possible Covert Chat

Search history revealed the search “how to use Google Documents as chat” (Figure 35). Shortly after, his Google Document history was found with over 700 back and forth conversations between the suspect and his brother (Figure 34). There were various instances where he would communicate on the Google Doc in the middle of him allegedly planning and researching his attack and escape. The unusual choice of medium and the timings raise suspicions of an attempt to communicate secretly or off-record. However, due to the deletion of this document(s), no text or useful information was able to be retrieved.



Result: 789 of 2534

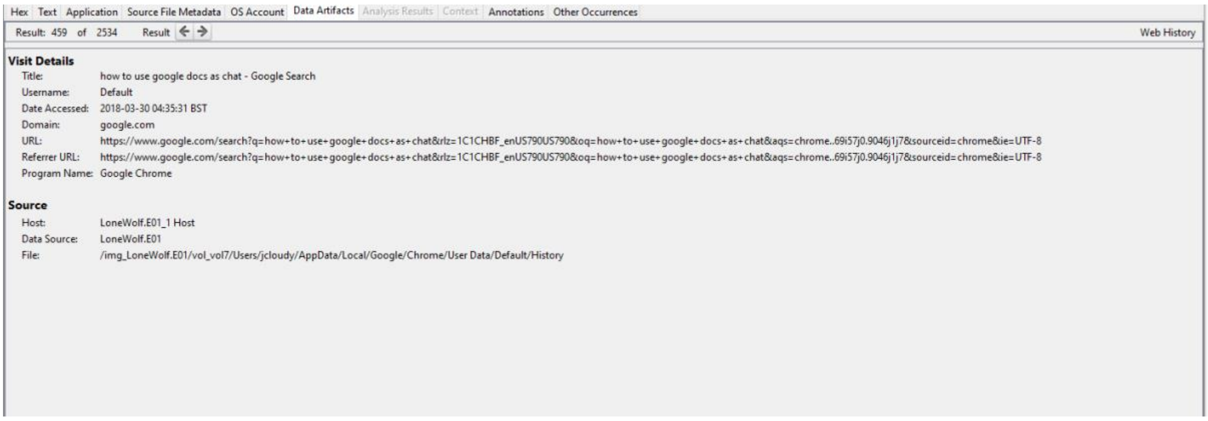
Visit Details

```
Title:          Brother Chat - Google Docs
Username:       Default
Date Accessed:  2018-04-06 13:26:22 BST
Domain:         google.com
URL:            https://docs.google.com/document/d/1GOv7MwOXM-7Vkoy4kjE3Q5bMDB5IWA0tB57a3u2hqeA/edit
Referrer URL:   https://docs.google.com/document/d/1GOv7MwOXM-7Vkoy4kjE3Q5bMDB5IWA0tB57a3u2hqeA/edit
Program Name:   Google Chrome
```

Source

```
Host:           LoneWolf.E01_1 Host
Data Source:    LoneWolf.E01
File:           /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/History
```

Figure 34: One of over 700 back and forth activity found on "brother chat" docs



Result: 459 of 2534

Visit Details

```
Title:          how to use google docs as chat - Google Search
Username:       Default
Date Accessed:  2018-03-30 04:35:31 BST
Domain:         google.com
URL:            https://www.google.com/search?q=how+to+use+google+docs+as+chat&rlz=1C1CHBF_enUS790US790&oq=how+to+use+google+docs+as+chat&aqs=chrome..69i57j0.9046j1j7&sourceid=chrome&ie=UTF-8
Referrer URL:   https://www.google.com/search?q=how+to+use+google+docs+as+chat&rlz=1C1CHBF_enUS790US790&oq=how+to+use+google+docs+as+chat&aqs=chrome..69i57j0.9046j1j7&sourceid=chrome&ie=UTF-8
Program Name:   Google Chrome
```

Source

```
Host:           LoneWolf.E01_1 Host
Data Source:    LoneWolf.E01
File:           /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/History
```

Figure 35: Previous Research on Google Docs as Chat

Findings:

The analysis uncovered hundreds of artifacts indicating premeditated criminal intent. The memory dump revealed abnormal command-line activity (cmd.exe, powershell.exe) with active or recently closed network connections. A suspicious executable (tempapp.exe) was also active in memory. Nothing from these findings seemingly holds water, so it seemed best to focus on the cold-hard evidence found on the suspect's drive.

Autopsy revealed extensive search history related to firearms, gun-free zones, and anti-gun control arguments. A strong focus on circumventing law enforcement and evading capture was found through searches on dual SIM Nokia phones. Odd for someone seemingly tech-savvy (e.g. uses cloud storage) to be using an outdated phone. Additionally, research about extradition laws that countries have with the states is not something an innocent person should have interest in. Finally, curiosity on how easy it is to smuggle money draws the profile of someone running away from consequences.

The most incriminating pieces of content were the "Cloudy Manifesto", and the "Planning" PowerPoint that had screenshots embedded that proved not just intention, but the accused actively conducting his plan, as detailed previously. The Manifesto promoted violent anti-government rhetoric, supported lone wolf style attacks, and referenced the suspect's plans and intended targets. Embedded imagery reflected extremist propaganda, further building the image of a man that has had enough.

Furthermore, over 700 interactions with a Google Document titled "brother chat" were found, suggesting covert communication.

Several figures and screenshots support these findings throughout the document and appendix.

Together, these artifacts form a digital narrative that supports a strong case for premeditation, motive, and intended action.

Conclusions:

The entirety of the evidence gathered from the digital forensic investigation into the accused Jim Cloudy's device leaves little doubt that he was engaging in deliberate, ideologically motivated planning for a lone wolf style terrorist attack. Both memory and disk analysis unearthed a disturbing volume of material that points to premeditation, extremist ideology, and active preparation. This behaviour does not paint a picture of a casual or coincidental digital footprint, this was part of a pattern of behaviour that is deliberate, consistent, and necessitating a federal investigation.

The findings from the memory dump alone, while speculative, raised red flags. The presence of multiple processes with network activity suggests the use of scripting or command line operations for either covert communication or system manipulation. This is far from normal user behaviour and may indicate the presence of malware, or other forms of unauthorized remote interaction. The detection of an unfamiliar executable,

tempapp.exe, running alongside all mentioned, strengthens a hypothesis of a custom-built payload of some sorts being created. Although further analysis was limited, the context in which these processes occurred cannot be ignored.

More definitively, the hard disk Autopsy analysis revealed a plethora of evidence tying the suspect's digital behaviour directly to radical and unlawful intent. Search history spanning topics such as automatic firearms, which are very rarely if ever used as a method of "self-defence", smuggling, and evasion from law enforcement, to note a few, paint the picture of a person exploring how to prepare for and escape from a criminal act. Notably, the suspect's interest in burner phones and extradition treaties between countries and the United States is not behaviour expected from a "normal" individual. These actions instead reflect the mindset of someone planning a high-risk operation and anticipating real legal consequences, the very definition of premeditation.

The most revealing pieces of digital evidence were found on the desktop: the "Cloudy Manifesto" and the "Planning" PPT. The manifesto was not a harmless rant or poorly thought out document that the accused would wish was hidden from view; it was a coherent and structured expression of anti-government ideology, advocating for armed resistance and glorifying lone wolf violence, plastered in as many cloud drives, he could get his hands on in order to preserve his "work". It framed the suspect as he frames himself; a revolutionary that is willing to sacrifice others for a cause he considered greater than himself. When considered alongside the embedded propaganda imagery, this document shifts from ideological expression into intent. The "Planning" PowerPoint further solidified this, visually documenting tactical considerations and potential strategies to execute his attack.

The discovery of over 700 interactions with a Google Document titled "brother chat", along with evidence suggesting it was used for covert communications, indicates that Jim Cloudy may not have been acting entirely alone. While no conclusive evidence of collaboration was found, this artifact points to active engagement with at least one confidant, raising further concern about broader implications or accomplices. It is worth noting, it was his brother that contacted the authorities after "discovering" his documents.

In conclusion, the evidence paints a clear, cohesive narrative. Jim Cloudy was not merely exploring radical content or engaging in provocative speech for pleasure, he was preparing to act. From the digital investigation and personal justification to practical planning and communication, the data confirms both motive and capability. This investigation not only demonstrates that the suspect posed a real threat, but also highlights the crucial role of digital forensics in pre-emptively identifying and stopping acts of mass violence.

Appendix:

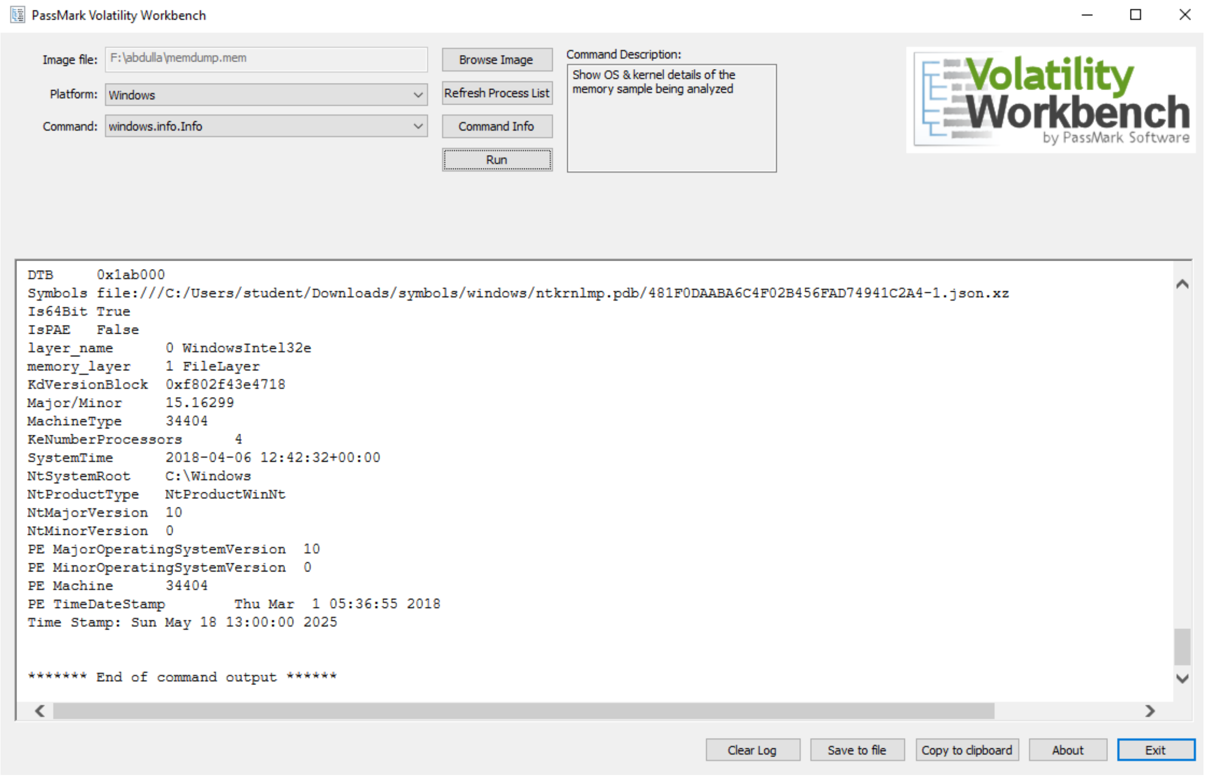


Image file: F:\abdulla\memdump.mem

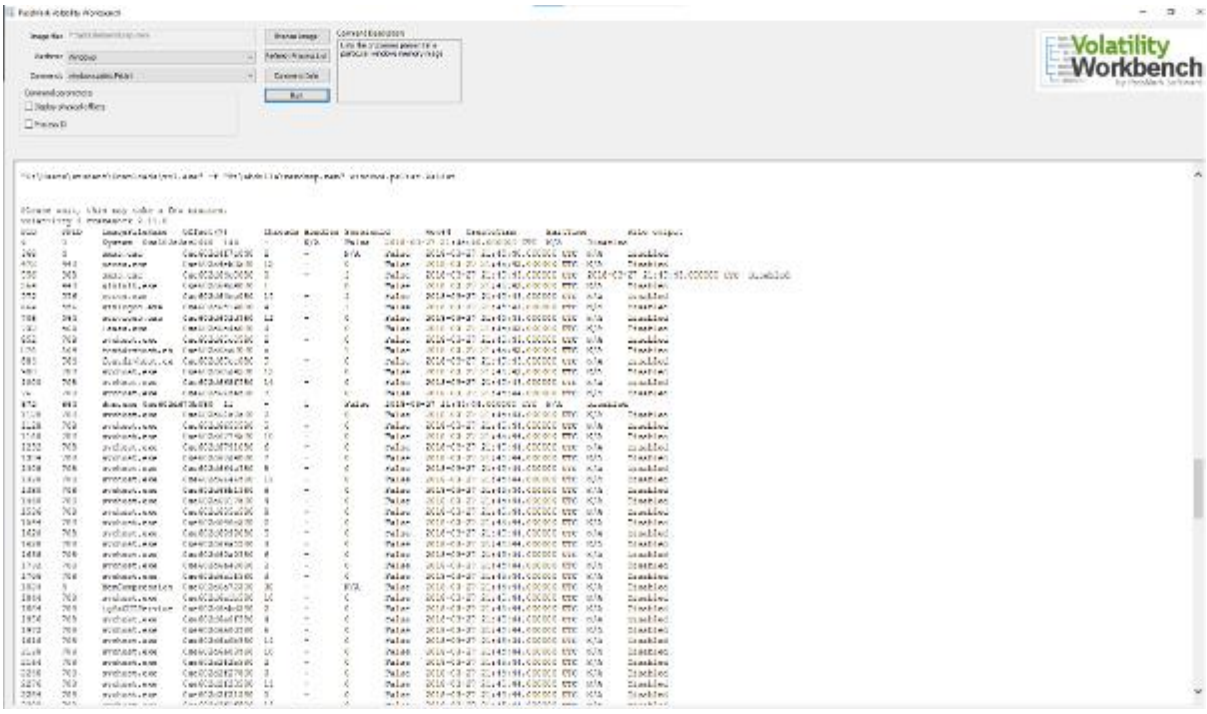
Platform: Windows

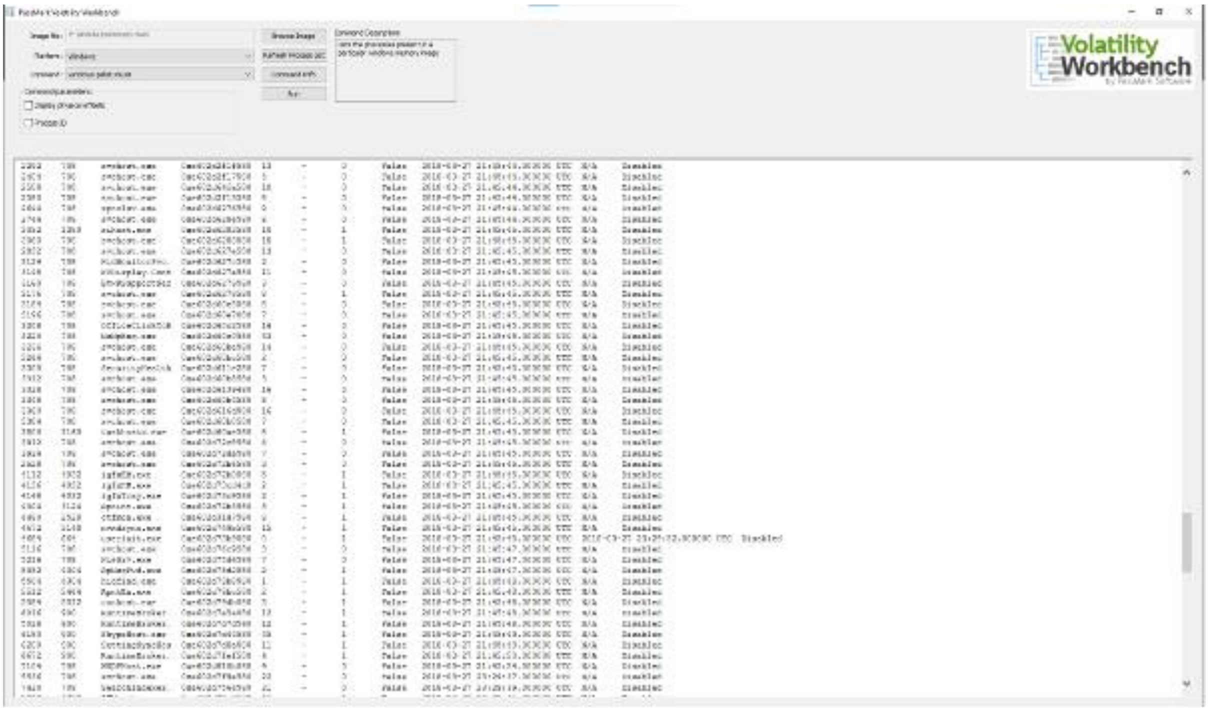
Command: windows.info.Info

Command Description:
Show OS & kernel details of the memory sample being analyzed

```
DTB     0x1ab000
Symbols file:///C:/Users/student/Downloads/symbols/windows/ntkrnlmp.pdb/481F0DAABA6C4F02B456FAD74941C2A4-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf802f43e4718
Major/Minor     15.16299
MachineType     34404
KeNumberProcessors      4
SystemTime      2018-04-06 12:42:32+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Thu Mar  1 05:36:55 2018
Time Stamp: Sun May 18 13:00:00 2025


******* End of command output ******
```





PassMark Volatility Workbench

Image file:

Platform: Windows

Command: windows.pslist.PsList

Command parameters:

□ Display physical offsets

□ Process ID

Browse Image

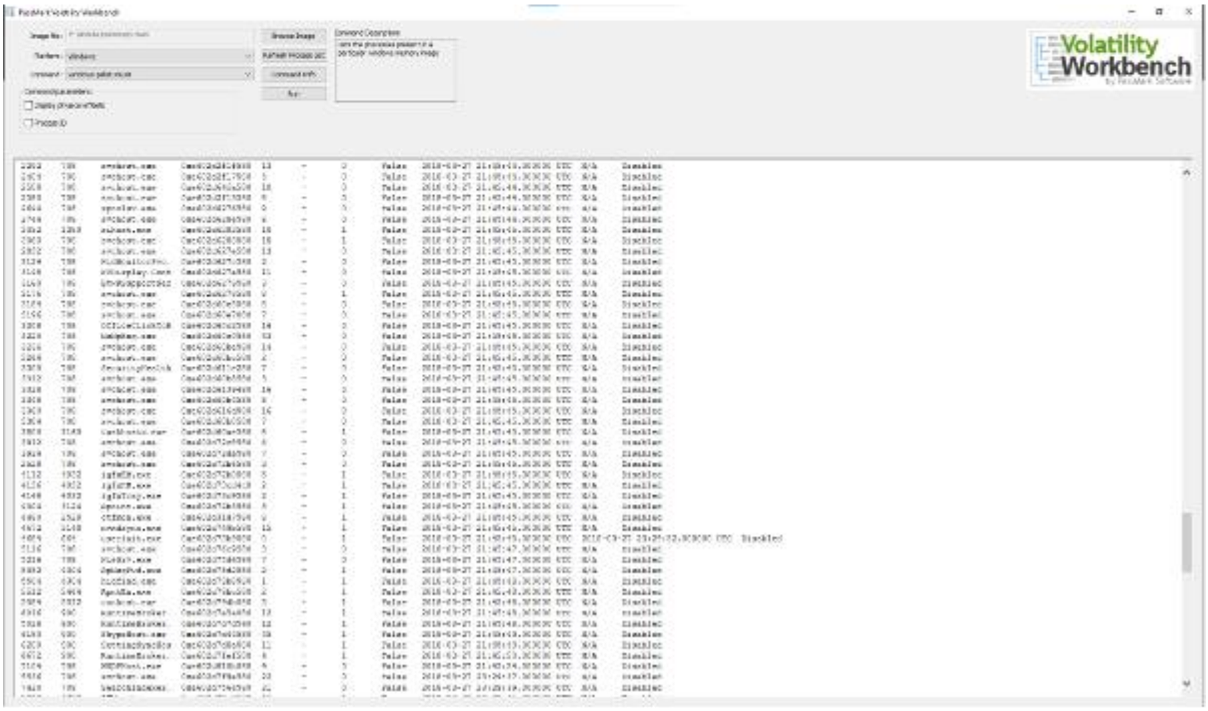
Refresh Process List

Command Info

Run

Command Description

Lists the processes present in a particular windows memory image



PassMark Volatility Workbench

Image file:

Platform: Windows

Command: windows.pslist.PsList

Command parameters:

□ Display physical offsets

□ Process ID

Browse Image

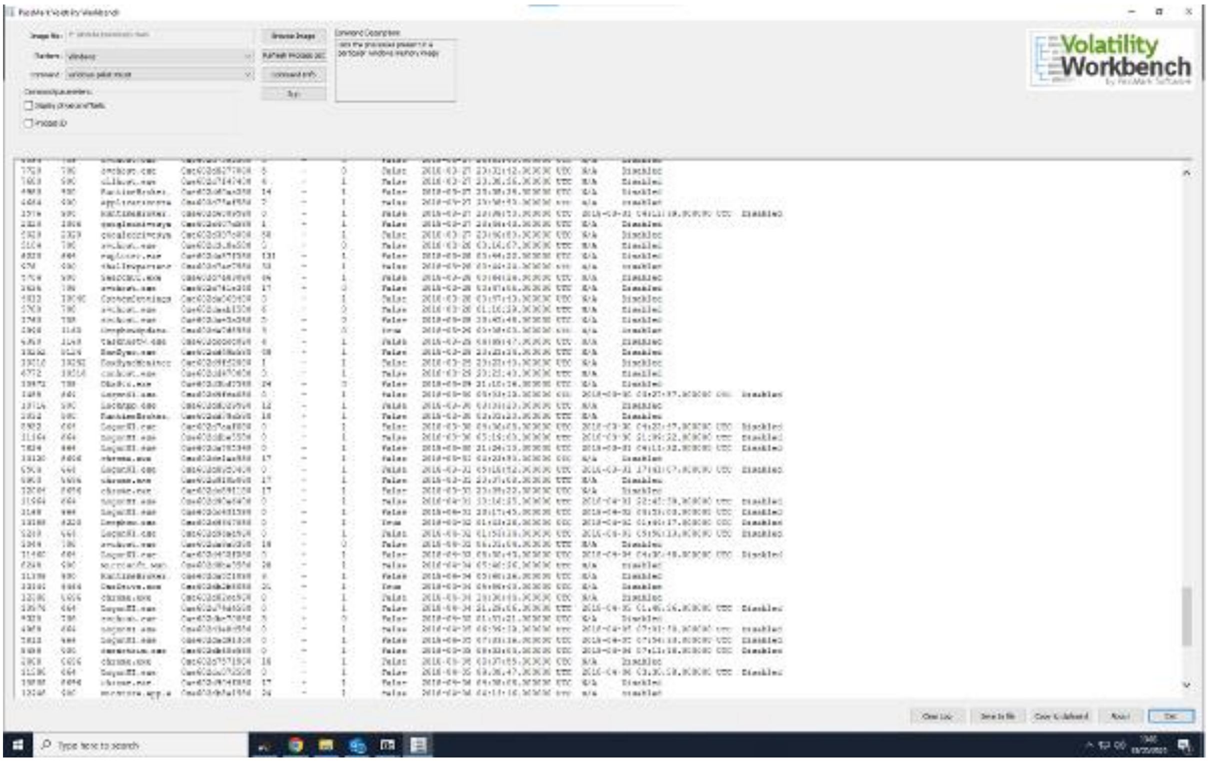
Refresh Process List

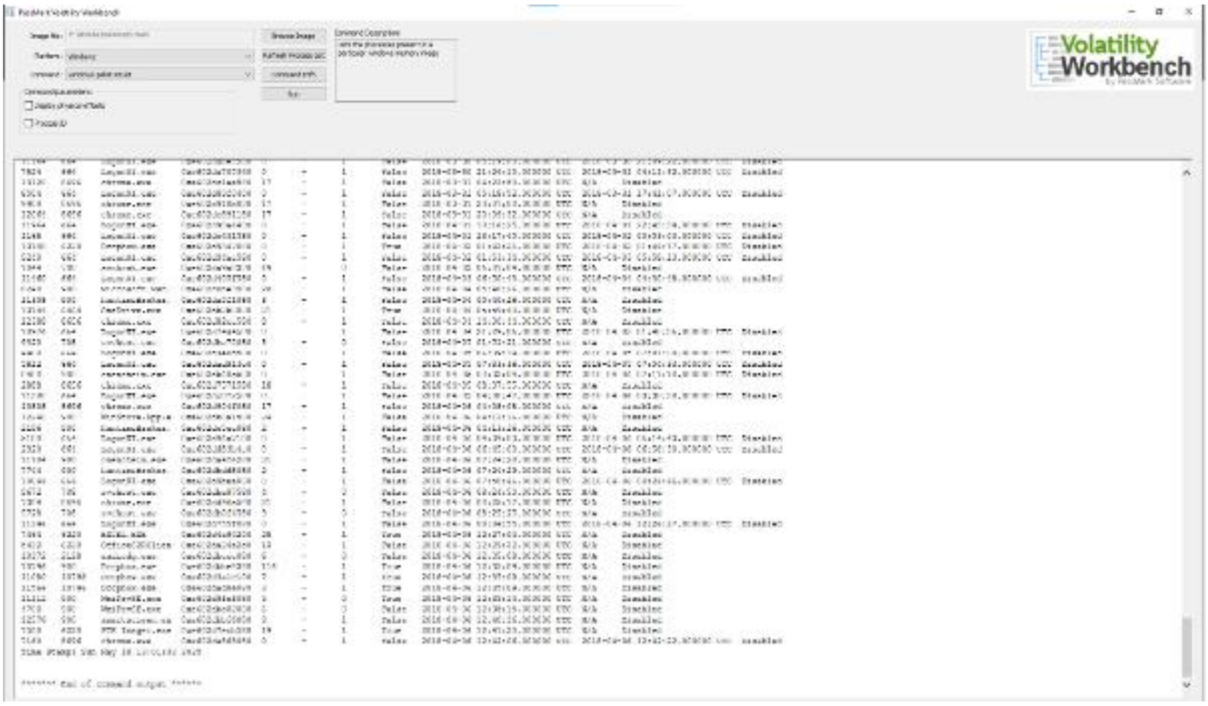
Command Info

Run

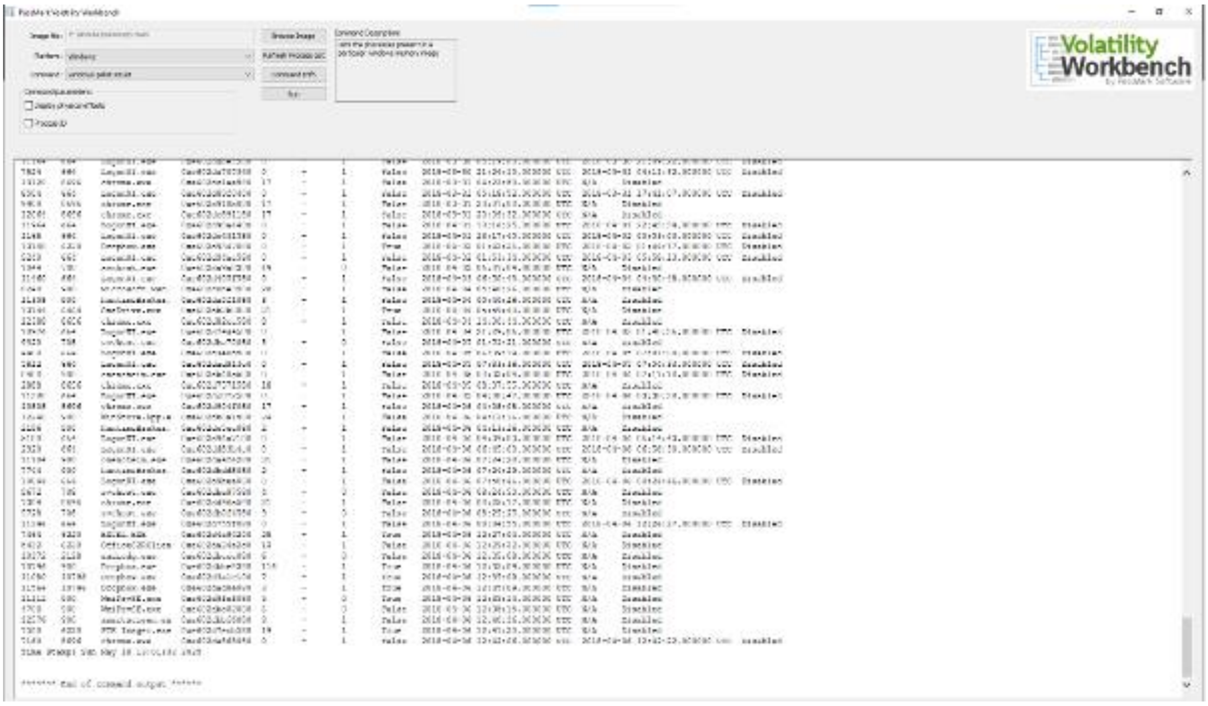
Command Description

Lists the processes present in a particular windows memory image

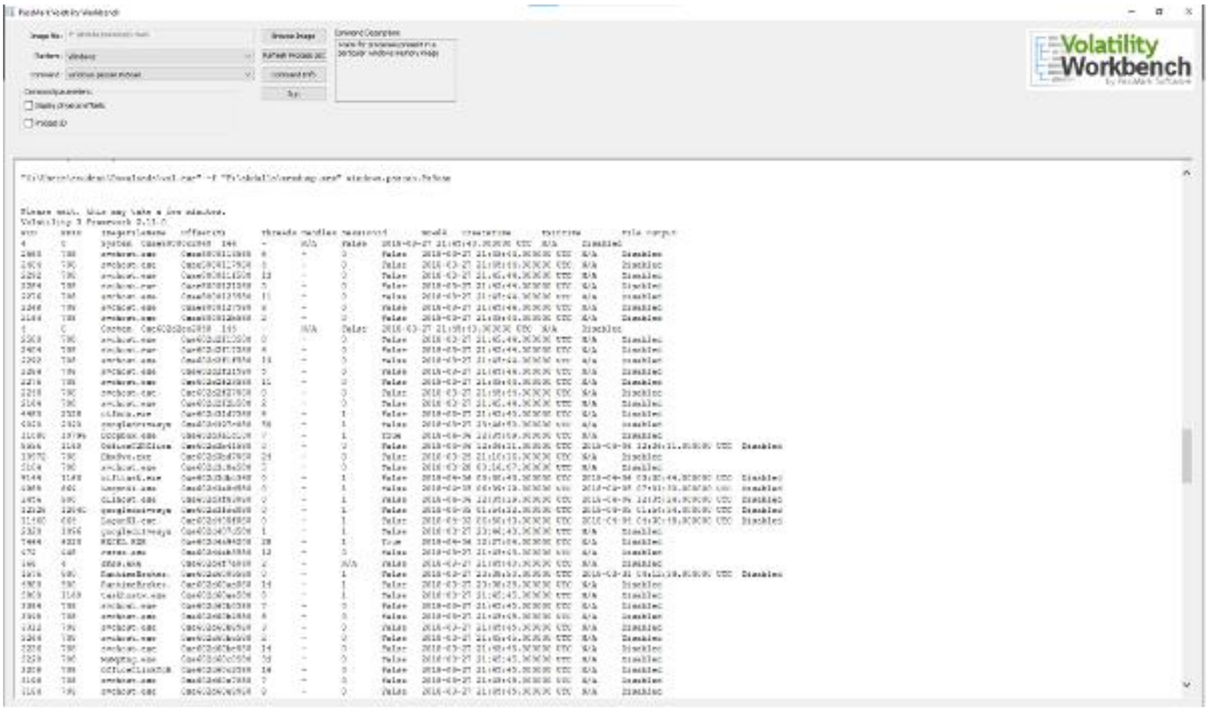




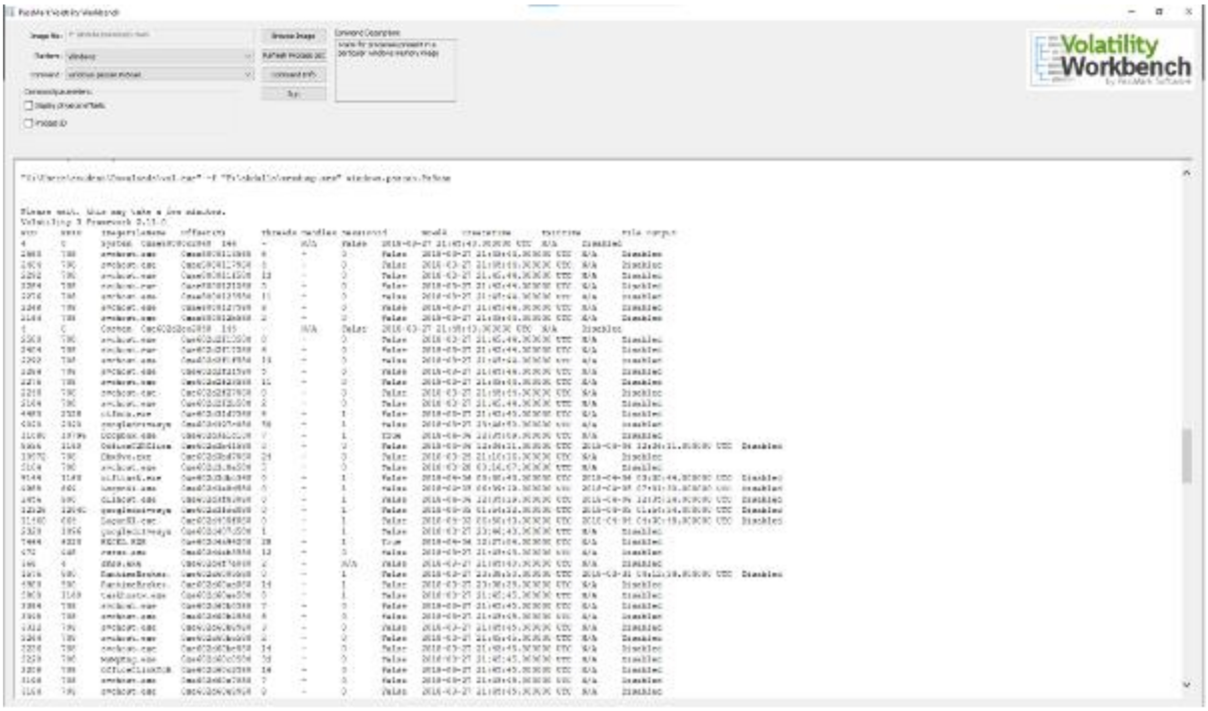
```
****** End of command output ******
```



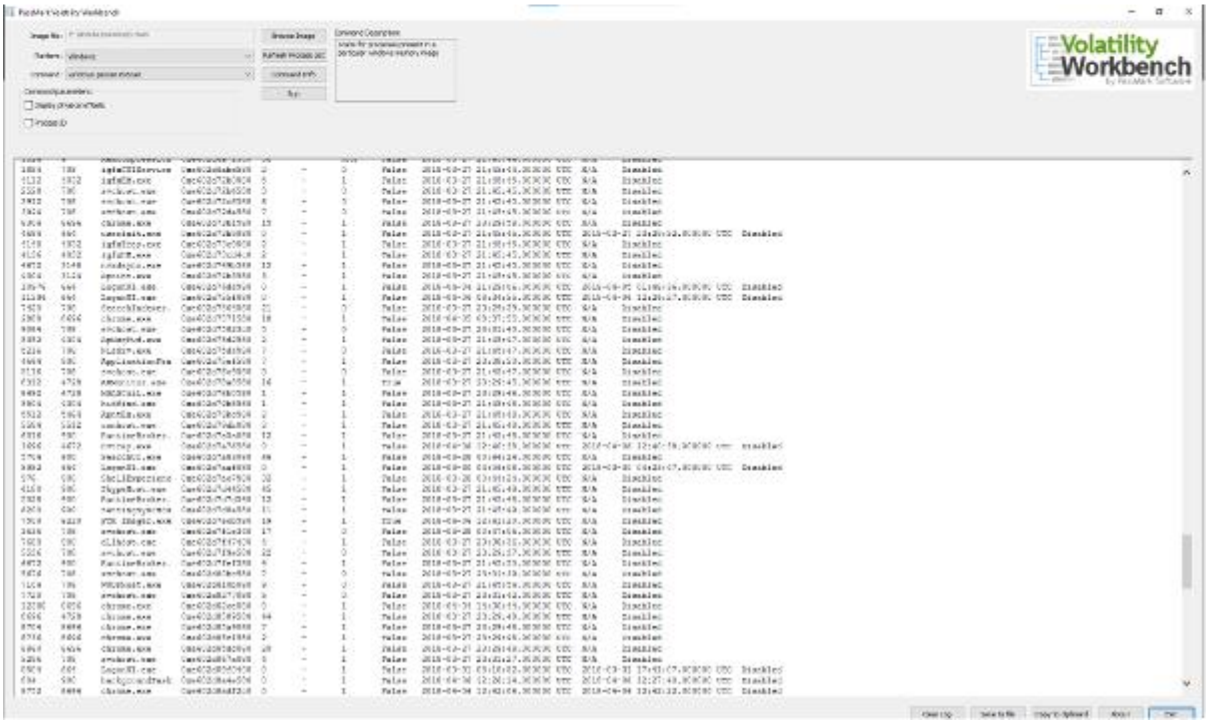
```
***** End of command output *****
```



```
Please wait, this may take a few minutes.
Volatility 3 Framework 2.11.0
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output
4       0       System  [illegible]
```



```
Please wait, this may take a few minutes.
Volatility 3 Framework 2.11.0
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output
```



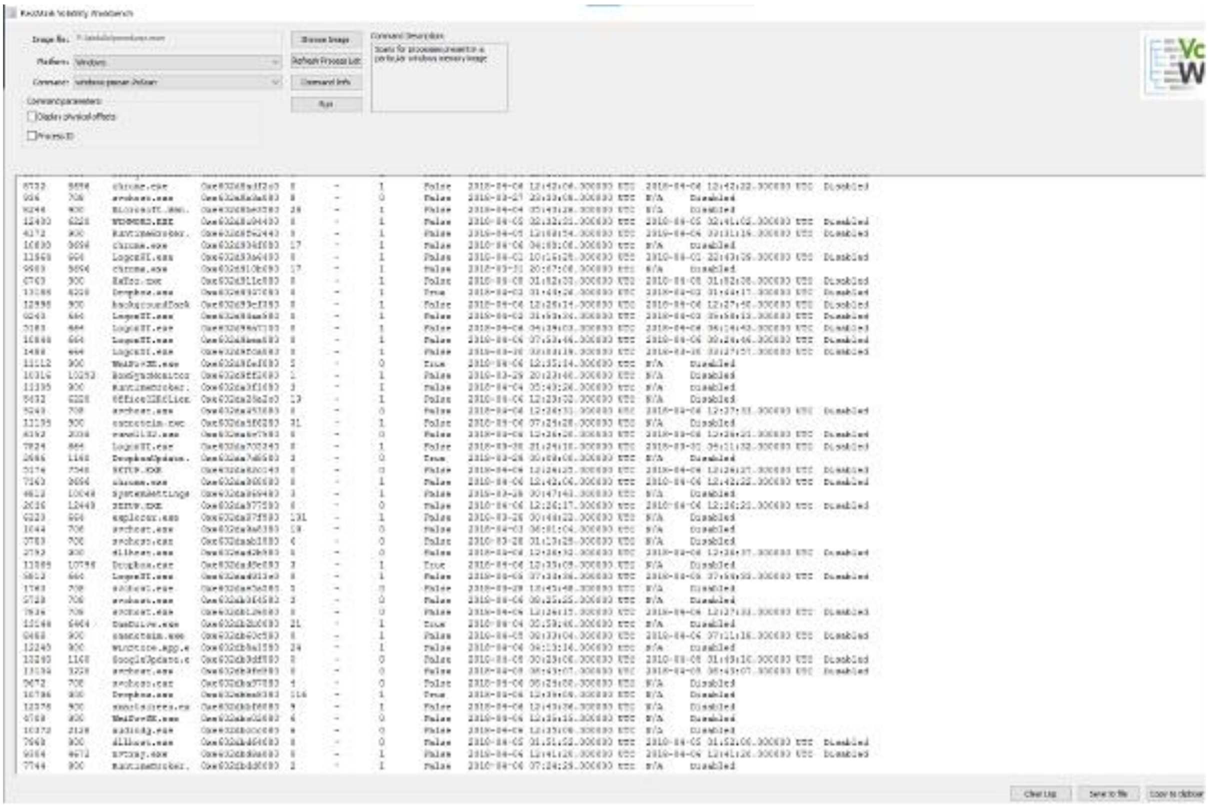


Image file: [illegible]

Platform: Windows

Command: windows.psscan.PsScan

Command parameters

□ Display physical offsets

□ Process ID

Command Description:
Scans for processes present in a particular windows memory image

```
8732    8696    chrome.exe      0xe602d8adf2c0  8       -       1       False   2018-04-06 12:42:06.000000 UTC  2018-04-06 12:42:22.000000 UTC  Disabled
936     708     svchost.exe     0xe602d8a0a680  8       -       0       False   2018-03-27 22:33:08.000000 UTC  N/A     Disabled
9244    900     MicrosoftEdge.  0xe602d8be0780  28      -       1       False   2018-04-04 05:43:28.000000 UTC  N/A     Disabled
12400   6228    WINWORD.EXE     0xe602d8a04400  8       -       1       False   2018-04-05 02:32:01.000000 UTC  2018-04-05 02:41:02.000000 UTC  Disabled
4172    900     RuntimeBroker.  0xe602d8f62440  0       -       1       False   2018-04-05 12:08:54.000000 UTC  2018-04-06 03:31:16.000000 UTC  Disabled
10600   8696    chrome.exe      0xe602d934f080  17      -       1       False   2018-04-06 04:03:06.000000 UTC  N/A     Disabled
11568   664     LogonUI.exe     0xe602d93a6400  0       -       1       False   2018-04-02 10:16:28.000000 UTC  2018-04-02 22:43:06.000000 UTC  Disabled
9680    8696    chrome.exe      0xe602d910b080  17      -       1       False   2018-03-31 20:07:06.000000 UTC  N/A     Disabled
6760    900     RaTcc.exe       0xe602d911c080  0       -       1       False   2018-04-06 01:52:03.000000 UTC  2018-04-06 01:52:06.000000 UTC  Disabled
13188   6228    Dropbox.exe     0xe602d9327080  0       -       1       True    2018-04-02 01:44:26.000000 UTC  2018-04-02 01:44:17.000000 UTC  Disabled
12898   900     backgroundTask  0xe602d93ef380  0       -       1       False   2018-04-06 12:26:14.000000 UTC  2018-04-06 12:27:45.000000 UTC  Disabled
6243    664     LogonUI.exe     0xe602d94aa580  0       -       1       False   2018-04-02 01:53:30.000000 UTC  2018-04-03 05:58:13.000000 UTC  Disabled
3183    664     LogonUI.exe     0xe602d9667180  0       -       1       False   2018-04-06 04:39:03.000000 UTC  2018-04-06 06:14:43.000000 UTC  Disabled
10848   664     LogonUI.exe     0xe602d8bea680  0       -       1       False   2018-04-06 07:53:46.000000 UTC  2018-04-06 08:24:46.000000 UTC  Disabled
1488    664     LogonUI.exe     0xe602d8f0a880  0       -       1       False   2018-03-30 02:03:19.000000 UTC  2018-03-30 03:27:57.000000 UTC  Disabled
11112   900     WmiPrvSE.exe    0xe602d9fef080  5       -       0       True    2018-04-06 12:35:14.000000 UTC  N/A     Disabled
10316   10252   BoxSyncMonitor  0xe602d9ff2080  1       -       1       False   2018-03-29 20:23:46.000000 UTC  N/A     Disabled
11395   900     RuntimeBroker.  0xe602da3f1080  3       -       1       False   2018-04-04 05:43:26.000000 UTC  N/A     Disabled
5632    6228    OfficeC2RClien  0xe602da28a2c0  13      -       1       False   2018-04-06 12:23:02.000000 UTC  N/A     Disabled
5243    708     svchost.exe     0xe602da451080  0       -       0       False   2018-04-06 12:26:31.000000 UTC  2018-04-06 12:27:31.000000 UTC  Disabled
12135   900     csrnctcim.exe   0xe602da5f0280  31      -       1       False   2018-04-06 07:25:28.000000 UTC  N/A     Disabled
8392    2008    rundll32.exe    0xe602da6e7580  0       -       0       False   2018-04-06 12:26:20.000000 UTC  2018-04-06 12:26:21.000000 UTC  Disabled
7824    664     LogonUI.exe     0xe602da702340  0       -       1       False   2018-03-30 21:24:10.000000 UTC  2018-03-31 05:11:32.000000 UTC  Disabled
2666    1168    DropboxUpdate.  0xe602da7a6680  3       -       0       True    2018-03-28 00:08:06.000000 UTC  N/A     Disabled
3176    7348    SETUP.EXE       0xe602da820140  0       -       0       False   2018-04-06 12:26:23.000000 UTC  2018-04-06 12:26:27.000000 UTC  Disabled
7163    8696    chrome.exe      0xe602da900080  0       -       1       False   2018-04-06 12:42:06.000000 UTC  2018-04-06 12:42:22.000000 UTC  Disabled
4612    10048   SystemSettings  0xe602da860480  3       -       1       False   2018-03-28 00:47:40.000000 UTC  N/A     Disabled
2036    12440   SETUP.EXE       0xe602da977580  0       -       0       False   2018-04-06 12:26:17.000000 UTC  2018-04-06 12:26:21.000000 UTC  Disabled
6223    664     explorer.exe    0xe602da97f580  131     -       1       False   2018-03-28 00:48:22.000000 UTC  N/A     Disabled
1644    708     svchost.exe     0xe602da9a0380  18      -       0       False   2018-04-03 06:01:04.000000 UTC  N/A     Disabled
3700    708     svchost.exe     0xe602daab1880  6       -       0       False   2018-03-28 01:13:25.000000 UTC  N/A     Disabled
2792    900     dllhost.exe     0xe602dad2b080  0       -       0       False   2018-04-06 12:26:32.000000 UTC  2018-04-06 12:26:37.000000 UTC  Disabled
11364   10796   Dropbox.exe     0xe602dad0e080  3       -       1       True    2018-04-06 12:35:05.000000 UTC  N/A     Disabled
5612    664     LogonUI.exe     0xe602dad012e0  0       -       1       False   2018-04-05 07:33:36.000000 UTC  2018-04-05 07:54:33.000000 UTC  Disabled
1760    708     svchost.exe     0xe602dae5a580  5       -       0       False   2018-03-28 18:45:48.000000 UTC  N/A     Disabled
5728    708     svchost.exe     0xe602db0f4580  3       -       0       False   2018-04-06 08:25:25.000000 UTC  N/A     Disabled
7836    708     svchost.exe     0xe602db126080  0       -       0       False   2018-04-06 12:26:15.000000 UTC  2018-04-06 12:27:33.000000 UTC  Disabled
13144   6464    OneDrive.exe    0xe602db2b6080  21      -       1       True    2018-04-04 05:58:40.000000 UTC  N/A     Disabled
5688    900     csrnctcim.exe   0xe602db60c580  0       -       1       False   2018-04-05 08:33:04.000000 UTC  2018-04-06 07:11:16.000000 UTC  Disabled
12240   900     WinStore.App.e  0xe602db8a1580  24      -       1       False   2018-04-06 04:13:16.000000 UTC  N/A     Disabled
13240   1168    GoogleUpdate.e  0xe602db9df580  0       -       0       False   2018-04-05 00:28:06.000000 UTC  2018-04-05 01:49:10.000000 UTC  Disabled
13104   3220    svchost.exe     0xe602db9d6580  0       -       0       False   2018-04-05 08:43:07.000000 UTC  2018-04-05 08:43:07.000000 UTC  Disabled
5672    708     svchost.exe     0xe602dba97580  4       -       0       False   2018-04-06 08:24:50.000000 UTC  N/A     Disabled
10796   900     Dropbox.exe     0xe602dbba8380  116     -       1       True    2018-04-06 12:35:09.000000 UTC  N/A     Disabled
12576   900     smartscreen.ex  0xe602dbbf8080  5       -       1       False   2018-04-06 12:40:36.000000 UTC  N/A     Disabled
4708    900     WmiPrvSE.exe    0xe602dbc02080  6       -       0       False   2018-04-06 12:35:15.000000 UTC  N/A     Disabled
10372   2128    audiodg.exe     0xe602dbccc080  6       -       0       False   2018-04-06 12:35:08.000000 UTC  N/A     Disabled
7868    900     dllhost.exe     0xe602dbd64080  0       -       0       False   2018-04-05 01:51:52.000000 UTC  2018-04-05 01:52:00.000000 UTC  Disabled
9304    4672    sttray.exe      0xe602dbd8a080  0       -       1       False   2018-04-06 12:41:20.000000 UTC  2018-04-06 12:41:20.000000 UTC  Disabled
7744    900     RuntimeBroker.  0xe602dbdd8080  2       -       1       False   2018-04-06 07:24:28.000000 UTC  N/A     Disabled
```

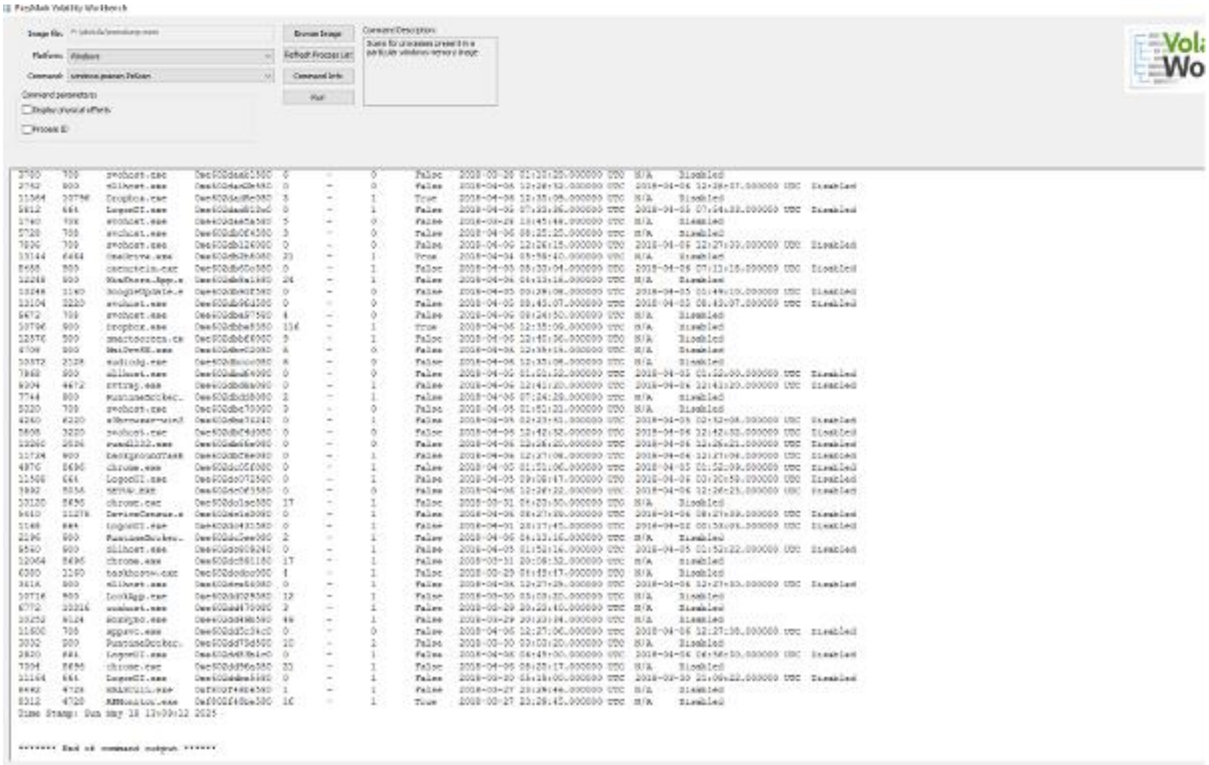


Image file: [illegible]

Platform: Windows

Command: windows.psscan.PsScan

Command parameters

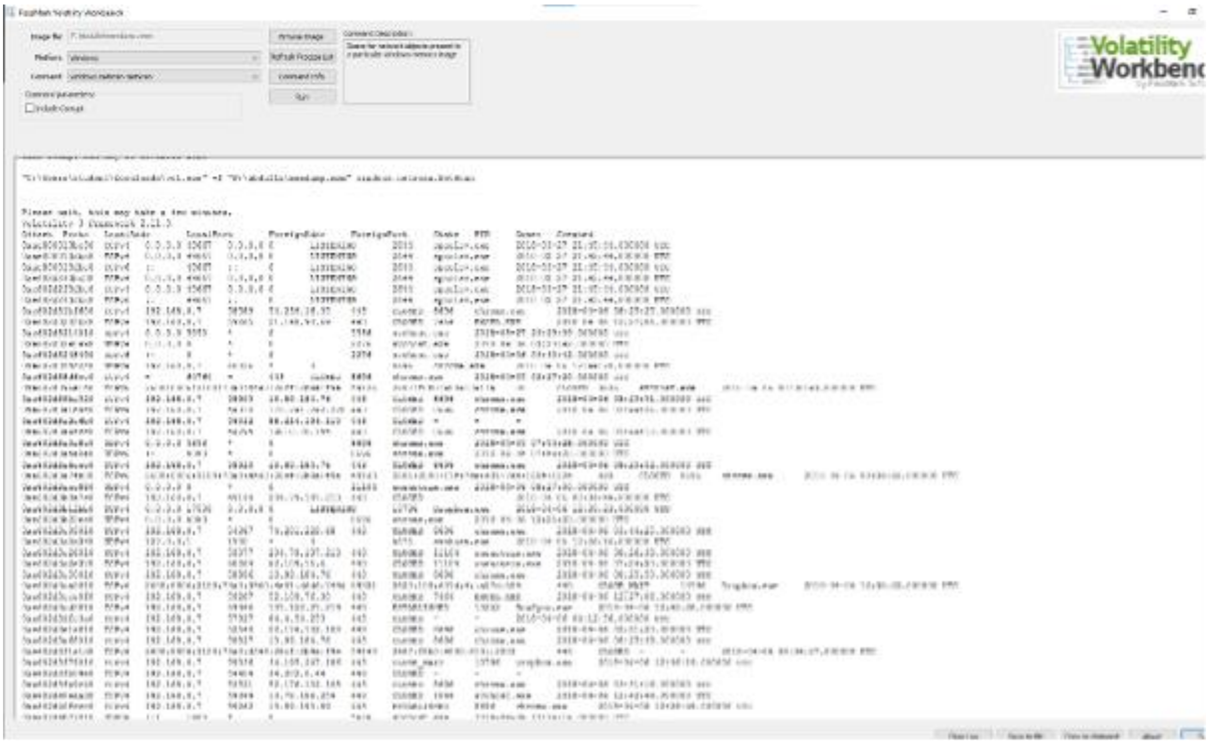
□ Display physical offsets

□ Process ID

Command Description:
Scans for processes present in a particular windows memory image

```
3700    708     svchost.exe     0xe602daab1880  6       -       0       False   2018-03-28 01:13:25.000000 UTC  N/A     Disabled
2792    900     dllhost.exe     0xe602dad2b080  0       -       0       False   2018-04-06 12:26:32.000000 UTC  2018-04-06 12:26:37.000000 UTC  Disabled
11364   10796   Dropbox.exe     0xe602dad0e080  3       -       1       True    2018-04-06 12:35:05.000000 UTC  N/A     Disabled
5612    664     LogonUI.exe     0xe602dad012e0  0       -       1       False   2018-04-05 07:33:36.000000 UTC  2018-04-05 07:54:33.000000 UTC  Disabled
1760    708     svchost.exe     0xe602dae5a580  5       -       0       False   2018-03-28 18:45:48.000000 UTC  N/A     Disabled
5728    708     svchost.exe     0xe602db0f4580  3       -       0       False   2018-04-06 08:25:25.000000 UTC  N/A     Disabled
7836    708     svchost.exe     0xe602db126080  0       -       0       False   2018-04-06 12:26:15.000000 UTC  2018-04-06 12:27:33.000000 UTC  Disabled
13144   6464    OneDrive.exe    0xe602db2b6080  21      -       1       True    2018-04-04 05:58:40.000000 UTC  N/A     Disabled
5688    900     csrnctcim.exe   0xe602db60c580  0       -       1       False   2018-04-05 08:33:04.000000 UTC  2018-04-06 07:11:16.000000 UTC  Disabled
12248   900     WinStore.App.e  0xe602db8a1580  24      -       1       False   2018-04-06 04:13:16.000000 UTC  N/A     Disabled
13248   1168    GoogleUpdate.e  0xe602db9df580  0       -       0       False   2018-04-05 00:28:06.000000 UTC  2018-04-05 01:49:10.000000 UTC  Disabled
13104   3220    svchost.exe     0xe602db9d6580  0       -       0       False   2018-04-05 08:43:07.000000 UTC  2018-04-05 08:43:07.000000 UTC  Disabled
5672    708     svchost.exe     0xe602dba97580  4       -       0       False   2018-04-06 08:24:50.000000 UTC  N/A     Disabled
10796   900     Dropbox.exe     0xe602dbba8380  116     -       1       True    2018-04-06 12:35:09.000000 UTC  N/A     Disabled
12576   900     smartscreen.ex  0xe602dbbf8080  5       -       1       False   2018-04-06 12:40:36.000000 UTC  N/A     Disabled
4708    900     WmiPrvSE.exe    0xe602dbc02080  6       -       0       False   2018-04-06 12:35:15.000000 UTC  N/A     Disabled
10372   2128    audiodg.exe     0xe602dbccc080  6       -       0       False   2018-04-06 12:35:08.000000 UTC  N/A     Disabled
7868    900     dllhost.exe     0xe602dbd64080  0       -       0       False   2018-04-05 01:51:52.000000 UTC  2018-04-05 01:52:00.000000 UTC  Disabled
9304    4672    sttray.exe      0xe602dbd8a080  0       -       1       False   2018-04-06 12:41:20.000000 UTC  2018-04-06 12:41:20.000000 UTC  Disabled
7744    900     RuntimeBroker.  0xe602dbdd8080  2       -       1       False   2018-04-06 07:24:28.000000 UTC  N/A     Disabled
5320    708     svchost.exe     0xe602dbe70080  3       -       0       False   2018-04-05 01:52:21.000000 UTC  N/A     Disabled
4260    6220    s3browser-win3  0xe602dbe76240  0       -       1       False   2018-04-05 02:23:51.000000 UTC  2018-04-05 02:32:08.000000 UTC  Disabled
5808    3220    svchost.exe     0xe602dbf4d080  0       -       0       False   2018-04-06 12:42:32.000000 UTC  2018-04-06 12:42:32.000000 UTC  Disabled
13260   2636    rundll32.exe    0xe602dbf6e080  0       -       0       False   2018-04-06 12:26:20.000000 UTC  2018-04-06 12:26:21.000000 UTC  Disabled
11724   900     backgroundTask  0xe602dbfbe080  0       -       1       False   2018-04-06 12:27:08.000000 UTC  2018-04-06 12:27:08.000000 UTC  Disabled
4876    8696    chrome.exe      0xe602dc05f080  0       -       1       False   2018-04-05 01:51:06.000000 UTC  2018-04-05 01:52:09.000000 UTC  Disabled
11568   664     LogonUI.exe     0xe602dc072580  0       -       1       False   2018-04-05 09:08:47.000000 UTC  2018-04-06 03:30:59.000000 UTC  Disabled
7892    5036    SETUP.EXE       0xe602dc0f3580  0       -       0       False   2018-04-06 12:26:22.000000 UTC  2018-04-06 12:26:25.000000 UTC  Disabled
10120   8696    chrome.exe      0xe602dc1ac580  17      -       1       False   2018-03-31 04:23:50.000000 UTC  N/A     Disabled
5610    11276   DeviceCensus.e  0xe602dc1e3080  0       -       1       False   2018-04-06 08:27:28.000000 UTC  2018-04-06 08:27:29.000000 UTC  Disabled
3148    664     LogonUI.exe     0xe602dc431580  0       -       1       False   2018-04-01 20:17:45.000000 UTC  2018-04-02 00:30:05.000000 UTC  Disabled
2196    900     RuntimeBroker.  0xe602dc5ee080  2       -       1       False   2018-04-06 04:13:16.000000 UTC  N/A     Disabled
8560    900     dllhost.exe     0xe602dc608240  0       -       1       False   2018-04-05 01:52:16.000000 UTC  2018-04-05 01:52:22.000000 UTC  Disabled
12064   8696    chrome.exe      0xe602dc861180  17      -       1       False   2018-03-31 20:08:32.000000 UTC  N/A     Disabled
6380    1180    taskhostw.exe   0xe602dcdcc080  1       -       1       False   2018-03-29 01:45:47.000000 UTC  N/A     Disabled
3616    900     dllhost.exe     0xe602dce56080  0       -       1       False   2018-04-06 12:27:28.000000 UTC  2018-04-06 12:27:33.000000 UTC  Disabled
10716   900     LockApp.exe     0xe602dd025580  12      -       1       False   2018-03-30 03:08:30.000000 UTC  N/A     Disabled
6772    10316   conhost.exe     0xe602dd470080  3       -       1       False   2018-03-29 20:23:40.000000 UTC  N/A     Disabled
10252   6124    BoxSync.exe     0xe602dd49b580  46      -       1       False   2018-03-29 20:23:34.000000 UTC  N/A     Disabled
11600   708     sppsvc.exe      0xe602dd5c34c0  0       -       0       False   2018-04-06 12:27:06.000000 UTC  2018-04-06 12:27:38.000000 UTC  Disabled
3032    900     RuntimeBroker.  0xe602dd75d580  10      -       1       False   2018-03-30 03:03:20.000000 UTC  N/A     Disabled
2820    664     LogonUI.exe     0xe602dd83b4c0  0       -       1       False   2018-04-06 04:49:00.000000 UTC  2018-04-06 04:56:30.000000 UTC  Disabled
7304    8696    chrome.exe      0xe602dd96a580  20      -       1       False   2018-04-05 08:28:17.000000 UTC  N/A     Disabled
11164   664     LogonUI.exe     0xe602dde3b580  0       -       1       False   2018-03-30 21:18:00.000000 UTC  2018-03-30 21:06:22.000000 UTC  Disabled
8492    4728    RAVBg64.exe     0xf802f48b4580  1       -       1       False   2018-03-27 23:29:46.000000 UTC  N/A     Disabled
8312    4728    RMMonitor.exe   0xf802f48ba580  10      -       1       True    2018-03-27 23:29:45.000000 UTC  N/A     Disabled
Time Stamp: Sun May 18 13:09:12 2025


******* End of command output ******
```

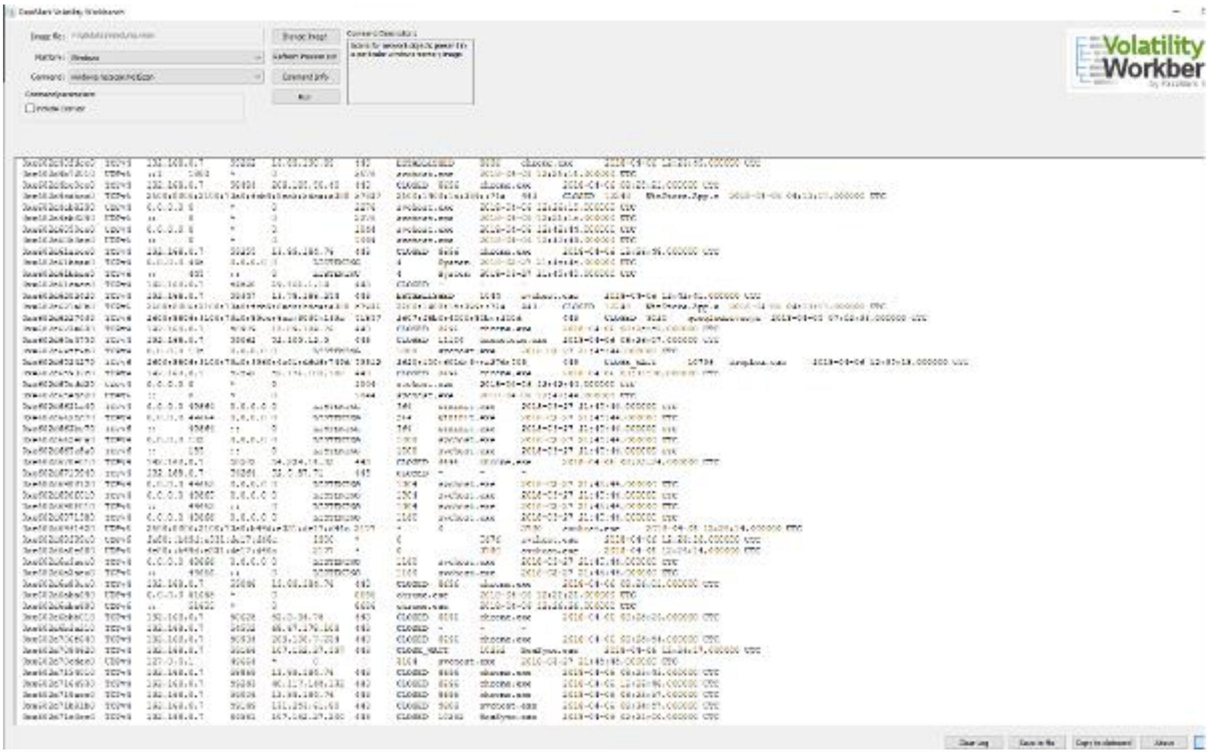


Platform: Windows

Command: windows.netscan.NetScan

Command Description: Scans for network objects present in a particular windows memory image

```
Please wait, this may take a few minutes.
Volatility 3 Framework 2.11.0
Offset  Proto  LocalAddr  LocalPort  ForeignAddr  ForeignPort  State  PID  Owner  Created
[illegible]
```

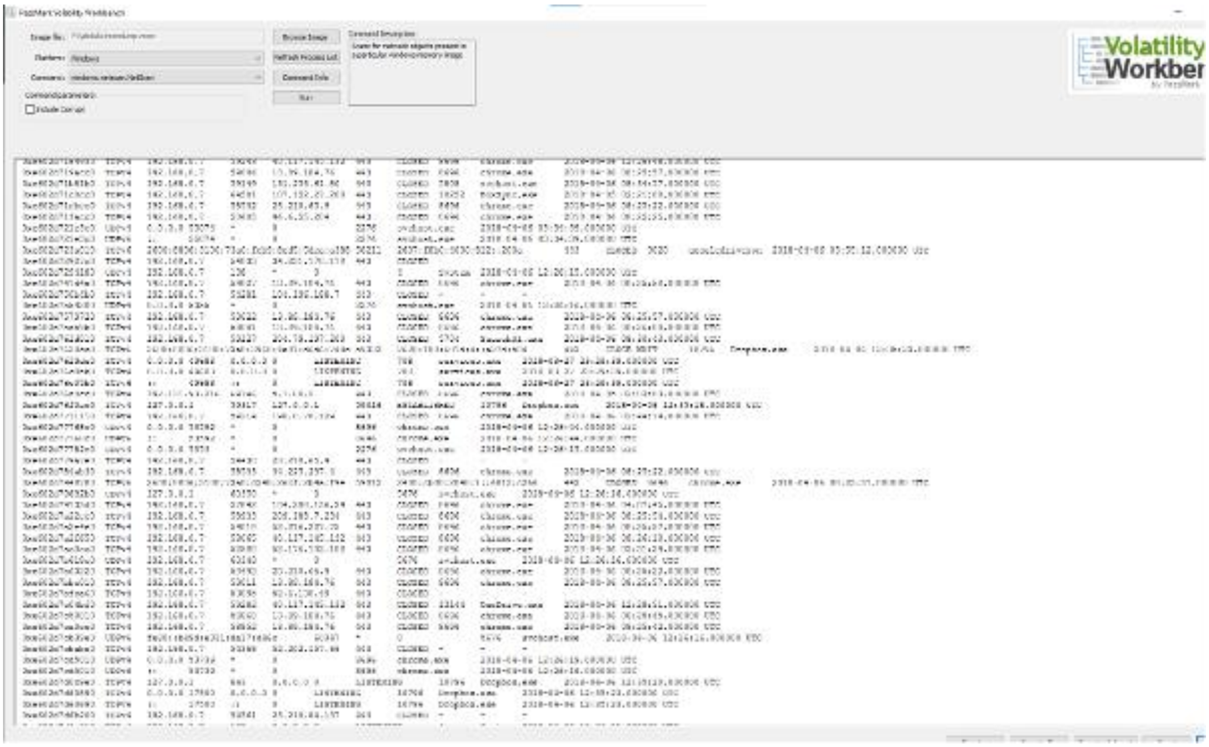


Platform: Windows

Command: windows.netscan.NetScan

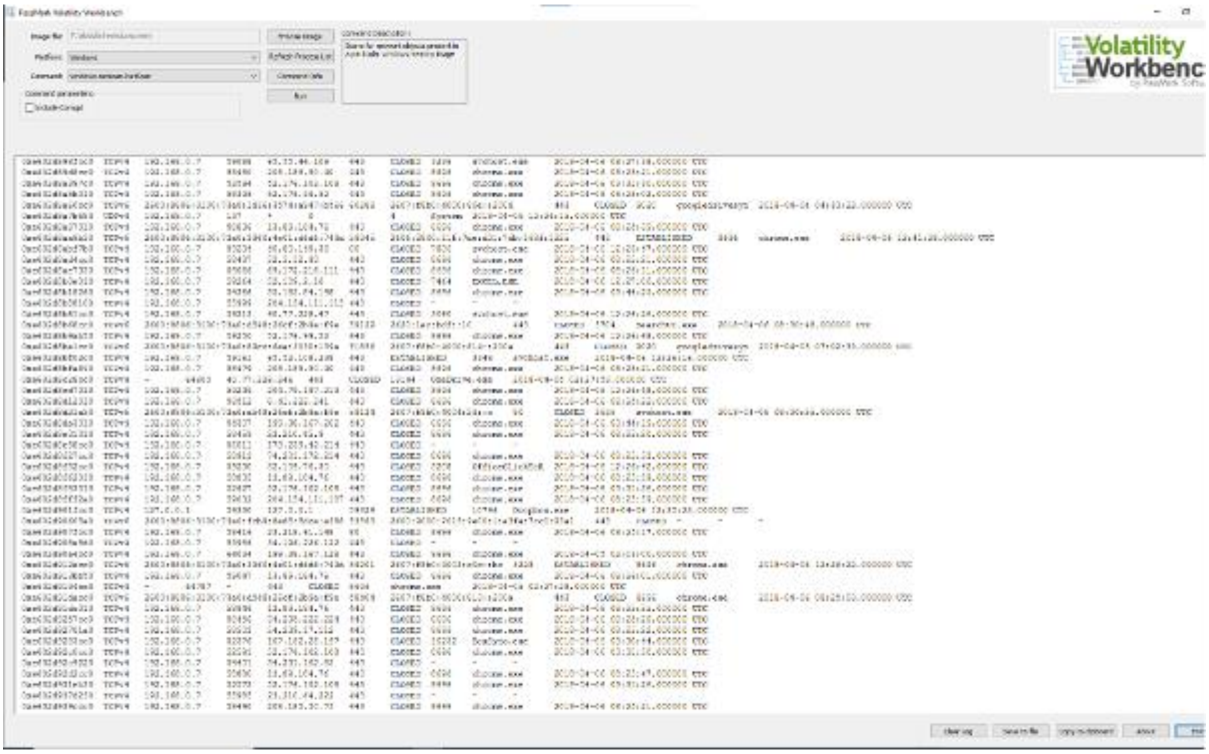
Command Description: Scans for network objects present in a particular windows memory image

```
[illegible]
```



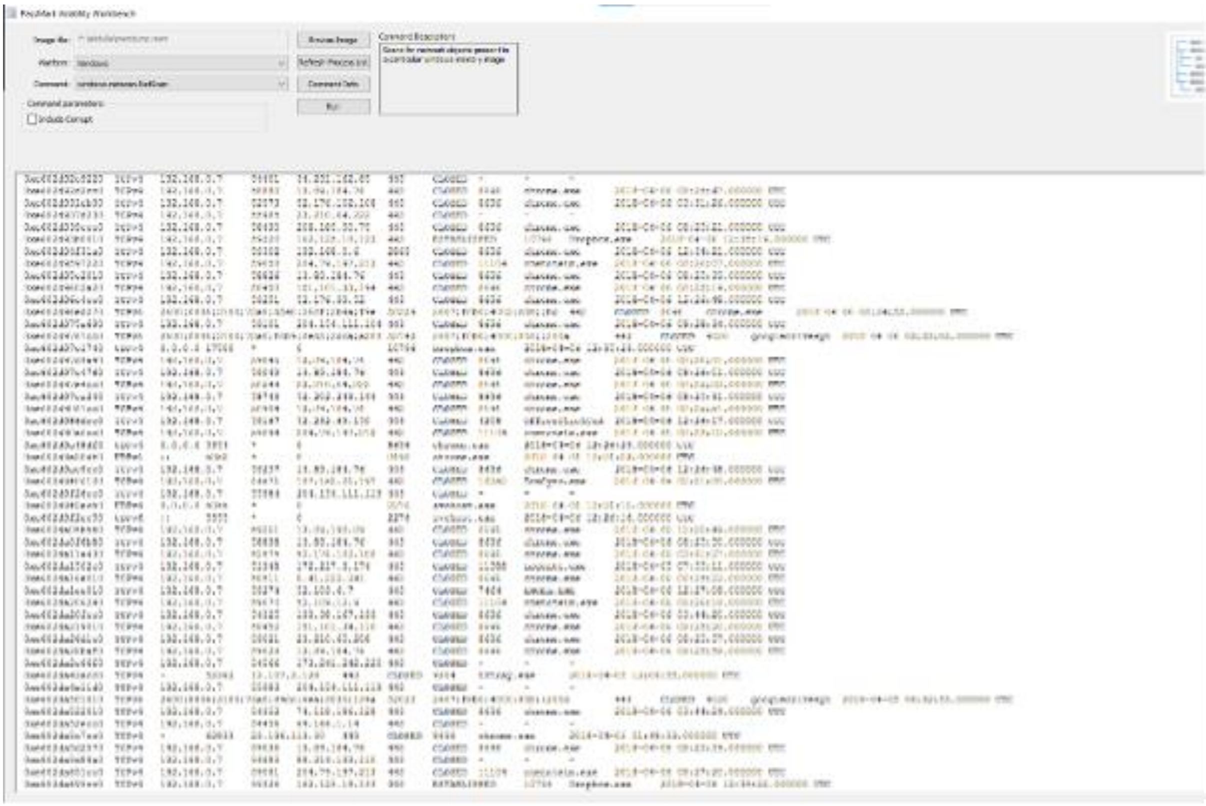
Scans for network objects present in a particular windows memory image.

```
[illegible]
```



Scans for network objects present in a particular windows memory image.

```
[illegible]
```



PassMark Volatility Workbench

Image file: [illegible]

Platform: Windows

Command: windows.netscan.NetScan

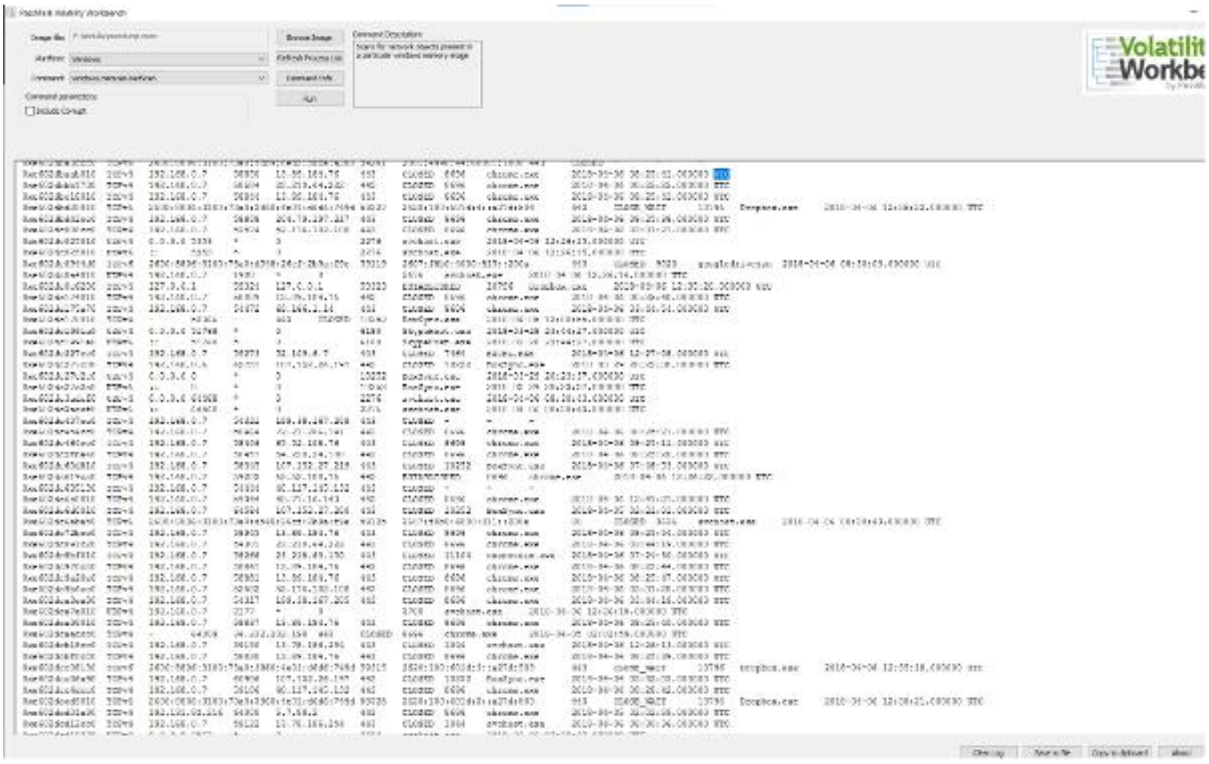
Command Description

Scans for network objects present in a particular windows memory image

Command parameters:

□ Include Corrupt

```
[illegible]
```



PassMark Volatility Workbench

Image file: [illegible]

Platform: Windows

Command: windows.netscan.NetScan

Command Description

Scans for network objects present in a particular windows memory image

Command parameters:

□ Include Corrupt

```
[illegible]
```

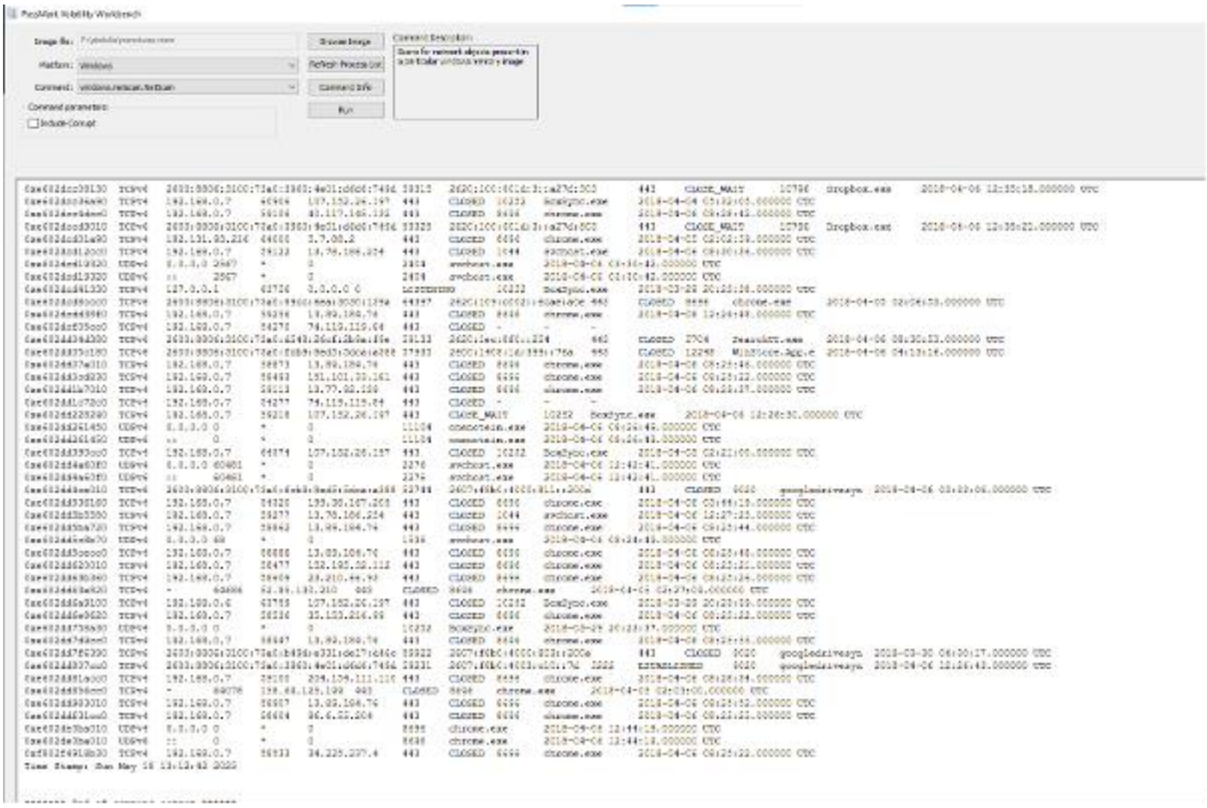


Image file: [illegible]

Platform: Windows

Command: windows.netscan.NetScan

Command parameters:

□ Include-Corrupt

Command Description: Scans for network objects present in a particular windows memory image

```
0xe682dcc38130  TCPv6  2603:8806:3100:73a0:3363:4e01:d6d6:7496 33315  2620:100:6014:3::a27d:503     443  CLOSE_WAIT  10796  Dropbox.exe     2018-04-06 12:35:18.000000 UTC
0xe682dcc36a90  TCPv4  192.168.0.7     46966  107.152.26.197  443  CLOSED  10232  ScnSync.exe     2018-04-04 05:32:05.000000 UTC
0xe682dce5dee0  TCPv4  192.168.0.7     58186  40.117.146.132  443  CLOSED  8488   chrome.exe      2018-04-06 08:28:42.000000 UTC
0xe682dcdd3010  TCPv6  2603:8806:3100:73a0:3363:4e01:d6d6:7496 33325  2620:100:6014:3::a27d:503     443  CLOSE_WAIT  10796  Dropbox.exe     2018-04-06 12:35:22.000000 UTC
0xe682dcd31a90  TCPv4  192.131.93.216  44000  3.7.00.2        443  CLOSED  6656   chrome.exe      2018-04-05 02:02:28.000000 UTC
0xe682dd812000  TCPv4  192.168.0.7     29132  13.78.188.224   443  CLOSED  1044   svchost.exe     2018-04-06 08:30:24.000000 UTC
0xe682dde41320  UDPv4  0.0.0.0 2667    *      0               2404  svchost.exe     2018-04-06 03:36:43.000000 UTC
0xe682dcd13320  UDPv6  ::      2667    *      0               2404  svchost.exe     2018-04-06 03:30:42.000000 UTC
0xe682dcd81330  TCPv4  127.0.0.1       43726  0.0.0.0 0       LISTENING      10232  ScnSync.exe     2018-03-28 20:22:26.000000 UTC
0xe682dd890000  TCPv6  2603:8806:3100:73a0:8960:8ea:3030:1298 44397  2620:107:c002::60ae:a0e 443   CLOSED  8888   chrome.exe      2018-04-02 02:56:53.000000 UTC
0xe682dee48880  TCPv4  192.168.0.7     59298  13.89.184.74    443  CLOSED  8488   chrome.exe      2018-04-08 12:26:48.000000 UTC
0xe682dcf35ce0  TCPv4  192.168.0.7     54278  74.119.119.64   443  CLOSED  -      -       -
0xe682dd34d300  TCPv6  2603:8806:3100:73a0:d243:26cf:2b0a:f6e 28133  2620:1ec:8f0::224        443   CLOSED  2704   SearchUI.exe    2018-04-06 08:30:23.000000 UTC
0xe682dd35d180  TCPv6  2603:8806:3100:73a0:f889:9ed3:3006:e888 37933  2600:1408:16/333::76a    443   CLOSED  12248  WinStore.App.e  2018-04-06 04:13:16.000000 UTC
0xe682dd37a010  TCPv4  192.168.0.7     38873  13.89.184.74    443  CLOSED  8888   chrome.exe      2018-04-08 08:25:46.000000 UTC
0xe682dd3cd230  TCPv4  192.168.0.7     56493  151.101.32.161  443  CLOSED  6656   chrome.exe      2018-04-06 08:23:22.000000 UTC
0xe682dd1b7010  TCPv4  192.168.0.7     28113  13.77.92.120    443  CLOSED  6656   chrome.exe      2018-04-06 08:22:27.000000 UTC
0xe682dd1c7200  TCPv4  192.168.0.7     24277  74.119.119.84   443  CLOSED  -      -       -
0xe682dd228280  TCPv4  192.168.0.7     39218  107.152.26.197  443  CLOSE_WAIT     10252  ScnSync.exe     2018-04-06 12:28:30.000000 UTC
0xe682dd261450  UDPv4  0.0.0.0 0       *      0               11104  onenotein.exe   2018-04-06 06:26:46.000000 UTC
0xe682dd261450  UDPv6  ::      0       *      0               11104  onenotein.exe   2018-04-06 06:26:43.000000 UTC
0xe682dd393cc0  TCPv4  192.168.0.7     64874  107.152.26.197  443  CLOSED  10232  ScnSync.exe     2018-04-05 02:21:06.000000 UTC
0xe682dd4a63f0  UDPv4  0.0.0.0 60481   *      0               2276  svchost.exe     2018-04-06 12:42:41.000000 UTC
0xe682dd4a63f0  UDPv6  ::      60481   *      0               2276  svchost.exe     2018-04-06 12:42:41.000000 UTC
0xe682dd8ee010  TCPv6  2603:8806:3100:73a0:feb8:9ed5:1eea:a288 52744  2607:f8b0:4000:811::200e       443  CLOSED  9020   googledrivesyn  2018-04-06 03:22:06.000000 UTC
0xe682dd338180  TCPv4  192.168.0.7     34320  135.38.167.203  443  CLOSED  6656   chrome.exe      2018-04-08 03:44:18.000000 UTC
0xe682dd3b5580  TCPv4  192.168.0.7     28277  13.78.186.224   443  CLOSED  1044   svchost.exe     2018-04-06 12:27:23.000000 UTC
0xe682dd5ba720  TCPv4  192.168.0.7     39862  13.89.184.74    443  CLOSED  8444   chrome.exe      2018-04-06 08:23:44.000000 UTC
0xe682dd6e8e70  UDPv4  0.0.0.0 68      *      0               1536  svchost.exe     2018-04-06 08:24:45.000000 UTC
0xe682dd5ecc00  TCPv4  192.168.0.7     56688  13.89.184.74    443  CLOSED  6656   chrome.exe      2018-04-08 08:25:48.000000 UTC
0xe682dd620010  TCPv4  192.168.0.7     28477  152.195.32.112  443  CLOSED  6656   chrome.exe      2018-04-06 08:22:21.000000 UTC
0xe682dd680840  TCPv4  192.168.0.7     28409  23.210.44.93    443  CLOSED  8444   chrome.exe      2018-04-06 08:23:24.000000 UTC
0xe682dd63e920  TCPv4  -       62886   52.84.132.210  443    CLOSED  8696   chrome.exe      2018-04-04 02:27:08.000000 UTC
0xe682dd6a3100  TCPv4  192.168.0.6     43785  107.152.26.197  443  CLOSED  10232  ScnSync.exe     2018-03-28 20:23:10.000000 UTC
0xe682dd6e3620  TCPv4  192.168.0.7     28336  35.153.214.89   443  CLOSED  6656   chrome.exe      2018-04-06 08:22:22.000000 UTC
0xe682dd738830  UDPv4  0.0.0.0 0       *      0               10232  ScnSync.exe     2018-03-28 20:22:37.000000 UTC
0xe682dd748ee0  TCPv4  192.168.0.7     38447  13.89.184.74    443  CLOSED  8444   chrome.exe      2018-04-08 08:25:55.000000 UTC
0xe682dd786330  TCPv6  2603:8806:3100:73a0:b49d:e331:de17:c46c 55922  2607:f8b0:4000:803::200e       443  CLOSED  9020   googledrivesyn  2018-03-30 06:30:17.000000 UTC
0xe682dd837ea0  TCPv6  2603:8806:3100:73a0:3363:4e01:d6d6:7496 28231  2607:f8b0:4003:c10::7d  2222   ESTABLISHED     9020   googledrivesyn  2018-04-06 12:26:43.000000 UTC
0xe682dd81a000  TCPv4  192.168.0.7     28188  204.154.111.118 443  CLOSED  6656   chrome.exe      2018-04-06 08:28:24.000000 UTC
0xe682dd896ee0  TCPv4  -       59078   198.64.125.190  443   CLOSED  8696   chrome.exe      2018-04-02 02:03:00.000000 UTC
0xe682dd903010  TCPv4  192.168.0.7     56667  13.89.184.76    443  CLOSED  6656   chrome.exe      2018-04-06 08:23:52.000000 UTC
0xe682ddf31ee0  TCPv4  192.168.0.7     56684  96.6.22.204     443  CLOSED  6656   chrome.exe      2018-04-06 08:22:22.000000 UTC
0xe682de3ba010  UDPv4  0.0.0.0 0       *      0               8696  chrome.exe      2018-04-08 12:44:18.000000 UTC
0xe682de3ba010  UDPv6  ::      0       *      0               8696  chrome.exe      2018-04-08 12:44:18.000000 UTC
0xf682f4918b30  TCPv4  192.168.0.7     56933  34.225.237.4    443  CLOSED  6656   chrome.exe      2018-04-06 08:25:22.000000 UTC
Time Stamp: Sun May 18 13:12:43 2025


****** End of command output ******
```

References:

ASEAN, 2021. *Summary of Indonesian Extradition Act*. [pdf] ASEAN. Available at: https://asean.org/wp-content/uploads/2021/01/SummaryofIndonesianExtraditionAct.pdf [accessed 24 May 2025].

Dictionary.com, n.d. *Molon labe*. [online] Available at: https://www.dictionary.com/e/slang/molon-labe/ [Accessed 24 May 2025].

Merriam-Webster, n.d. *Rugged individualism*. [online] Available at: https://www.merriam-webster.com/dictionary/rugged%20individualism [Accessed 24 May 2025].

Office of Justice Programs, 2015. *Developing a Strategy to Prevent and Counter Violent Extremism in the United States*. [pdf] National Institute of Justice. Available at: https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf [Accessed 24 May 2025]

Wondershare Recoverit, n.d. *Is PowerShell a Malicious Tool?* [online] Available at: https://recoverit.wondershare.com/windows-computer-tips/windows-powershell-virus.html [Accessed 24 May 2025].