



DIGITAL FORENSIC REPORT

CASE #001

Examiner: Muhammad David Fawwas Olfat

INFORMASI KASUS

Nama Kasus	Project Akhir CHFI
Nomor Kasus	01
Pemilik Evidene	JCloudy(tersangka)
Jumlah Evidene	10
Tanggal Awal Pemeriksaan	09 December 2024
Tanggal Akhir Pemeriksaan	15 December 2024

PENDAHULUAN

LATAR BELAKANG

Peserta MSIB diminta untuk melakukan investigasi terhadap image file Inewolf untuk mencari barang bukti terkait adanya dugaan perancangan pembunuhan. Project ini bertujuan memberikan pengalaman praktis sekaligus membekali peserta dengan keterampilan penting di bidang forensik digital.

TUJUAN

- What: Apa bukti yang ditemukan?
- Who: Siapa yang terlibat dalam aktivitas berdasarkan bukti?
- When: Kapan aktivitas tersebut terjadi?
- Where: Di mana bukti ditemukan dalam sistem (misalnya, lokasi file atau log)?
- Why: Mengapa bukti ini relevan terhadap dugaan perencanaan pembunuhan?
- How: Bagaimana bukti ini menunjukkan keterkaitan dengan perencanaan pembunuhan?

RUANG LINGKUP / DISCLAIMER

Pemeriksaan hanya dilakukan pada lingkup hard disk atau image file

METODOLOGI

Metodologi yang digunakan dalam proses Pemeriksaan Forensik Digital mengacu pada:

- NIJ: Electronic Crime Scene Investigation: A Guide for First Responders [2002]
- NIST: Guide to Integrating Forensic Techniques into Incident Response [2006]
- ACPO: Good Practice Guide for Computer Based Evidence [2007].

Metodologi ini terdiri dari 4 (empat) tahap, yaitu *Collection*, *Examination*, *Analysis*, dan *Report*.

COLLECTION

DATA INVESTIGASI

- AIRPORT INFORMATION

Listing Keyword search 9 - f0014920 × | Keyword search 10 - jim notebook × | Keyword search 11 - paul × /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop 46 Results

Table Thumbnail Summary

Page: Pages: Go to Page:

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2018-04-06 15:30:22 WIB	2018-04-06 15:30:22 WIB	2018-04-06 15:30:22 WIB	2018-03-27 16:18:58 WIB	176
[parent folder]				2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-27 16:18:58 WIB	256
.tmp.drivedownload				2018-04-06 15:30:04 WIB	2018-04-06 15:30:04 WIB	2018-04-06 15:30:04 WIB	2018-03-28 07:43:53 WIB	56
✓ Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
✓ Larry King.. Time to Repeal the 'Poorly Written' Sec				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
AIRPORT INFORMATION.docx	▼	1		2018-04-04 11:59:32 WIB	2018-04-04 11:59:40 WIB	2018-04-04 11:59:32 WIB	2018-03-30 09:29:57 WIB	172684
Cloudy thoughts (4apr).docx	▼	0		2018-04-05 09:39:30 WIB	2018-04-05 09:39:41 WIB	2018-04-05 09:39:30 WIB	2018-04-05 09:39:29 WIB	12547
Planning.docx	▼	1		2018-04-04 12:30:41 WIB	2018-04-04 12:30:49 WIB	2018-04-04 12:30:41 WIB	2018-03-30 09:16:48 WIB	14060
The Cloudy Manifesto.docx	▼	1		2018-04-02 08:35:27 WIB	2018-04-02 08:35:39 WIB	2018-04-02 08:35:27 WIB	2018-04-02 08:35:27 WIB	816313

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

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.

-----METADATA-----
Application-Name: Microsoft Office Word
Application-Version: 16.0000

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/AIRPORT INFORMATION.docx
Type: File System
MIME Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size: 172684
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2018-04-04 11:59:32 WIB
Accessed: 2018-04-04 11:59:32 WIB
Created: 2018-03-30 09:29:57 WIB
Changed: 2018-04-04 11:59:40 WIB
MD5: 297eec248647f33f887d72328ab56f3c
SHA-256: 1fb5577d8559562d97ac3023e0ca91cc6b8b55d2e5fabaa81160c109f0abf9b6
Hash Lookup Results: UNKNOWN
Internal ID: 34757

From The Sleuth Kit istat Tool:

- Cloudy thoughts (4apr)

This is a DirectoryTree window

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2018-04-06 15:30:22 WIB	2018-04-06 15:30:22 WIB	2018-03-27 16:18:58 WIB	2018-03-27 16:18:58 WIB	176
[parent folder]				2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-27 16:18:58 WIB	256
.tmp.drivedownload				2018-04-06 15:30:04 WIB	2018-04-06 15:30:04 WIB	2018-04-06 15:30:04 WIB	2018-03-28 07:43:53 WIB	56
Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
Larry King_ Time to Repeal the 'Poorly Written' Sec				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
AIRPORT INFORMATION.docx	▼	1		2018-04-04 11:59:32 WIB	2018-04-04 11:59:40 WIB	2018-04-04 11:59:32 WIB	2018-03-30 09:29:57 WIB	172684
Cloudy thoughts (4apr).docx	▼	0		2018-04-05 09:39:30 WIB	2018-04-05 09:39:41 WIB	2018-04-05 09:39:30 WIB	2018-04-05 09:39:29 WIB	12547
Planning.docx	▼	1		2018-04-04 12:30:41 WIB	2018-04-04 12:30:49 WIB	2018-04-04 12:30:41 WIB	2018-03-30 09:16:48 WIB	14060
The Cloudy Manifesto.docx	▼	1		2018-04-02 08:35:27 WIB	2018-04-02 08:35:39 WIB	2018-04-02 08:35:27 WIB	2018-04-02 08:35:27 WIB	816313

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

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!

-----METADATA-----

Application-Name: Microsoft Office Word
Application-Version: 16.0000
Author: jcloudy
Character Count: 986
Character-Count-With-Spaces: 1156
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
Creation-Date: 2018-04-05T02:32:00Z

Metadata	
Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Cloudy thoughts (4apr).docx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.wordprocessingml.document
Size:	12547
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-04-05 09:39:30 WIB
Accessed:	2018-04-05 09:39:30 WIB
Created:	2018-04-05 09:39:29 WIB
Changed:	2018-04-05 09:39:41 WIB
MD5:	f8c2bc733c109a88405dfd13b47d0690
SHA-256:	37cd60bccb8cf01fd36be13d89e5df64749bcc072133d3bad1ed0c430e436dfd
Hash Lookup Results:	UNKNOWN
Internal ID:	34766

From The Sleuth Kit iStat Tool:

- Planning

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop
This is a DirectoryTree window

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]				2018-04-06 15:30:22 WIB	2018-04-06 15:30:22 WIB	2018-04-06 15:30:22 WIB	2018-03-27 16:18:58 WIB	176
[parent folder]				2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-27 16:18:58 WIB	256
.tmp.drivedownload				2018-04-06 15:30:04 WIB	2018-04-06 15:30:04 WIB	2018-04-06 15:30:04 WIB	2018-03-28 07:43:53 WIB	56
Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
Larry King_- Time to Repeal the 'Poorly Written' Sec				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
AIRPORT INFORMATION.docx	▼	1		2018-04-04 11:59:32 WIB	2018-04-04 11:59:40 WIB	2018-04-04 11:59:32 WIB	2018-03-30 09:29:57 WIB	172684
Cloudy thoughts (4apr).docx	▼	0		2018-04-05 09:39:30 WIB	2018-04-05 09:39:41 WIB	2018-04-05 09:39:30 WIB	2018-04-05 09:39:29 WIB	12547
Planning.docx	▼	1		2018-04-04 12:30:41 WIB	2018-04-04 12:30:49 WIB	2018-04-04 12:30:41 WIB	2018-03-30 09:16:48 WIB	14060
The Cloudy Manifesto.docx	▼	1		2018-04-02 08:35:27 WIB	2018-04-02 08:35:39 WIB	2018-04-02 08:35:27 WIB	2018-04-02 08:35:27 WIB	816313

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

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

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Planning.docx
 Type: File System
 MIME Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document
 Size: 14060
 File Name Allocation: Allocated
 Metadata Allocation: Allocated
 Modified: 2018-04-04 12:30:41 WIB
 Accessed: 2018-04-04 12:30:41 WIB
 Created: 2018-03-30 09:16:48 WIB
 Changed: 2018-04-04 12:30:49 WIB
 MD5: 4ef414e469b7830faa2db429fe1321ee
 SHA-256: 0d87fa0cb21fd3cd3e2eab41149e611593f0c6a5224ed264cd5632692c126e12
 Hash Lookup Results: UNKNOWN
 Internal ID: 34804

From The Sleuth Kit istat Tool:

- The Cloudy Manifesto

/img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop
This is a DirectoryTree window

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Larry King_Time to Repeal the 'Poorly Written' Sec				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
AIRPORT INFORMATION.docx	▼	1		2018-04-04 11:59:32 WIB	2018-04-04 11:59:40 WIB	2018-04-04 11:59:32 WIB	2018-03-30 09:29:57 WIB	172684
Cloudy thoughts (4apr).docx	▼	0		2018-04-05 09:39:30 WIB	2018-04-05 09:39:41 WIB	2018-04-05 09:39:30 WIB	2018-04-05 09:39:29 WIB	12547
Planning.docx	▼	1		2018-04-04 12:30:41 WIB	2018-04-04 12:30:49 WIB	2018-04-04 12:30:41 WIB	2018-03-30 09:16:48 WIB	14060
The Cloudy Manifesto.docx	▼	1		2018-04-02 08:35:27 WIB	2018-04-02 08:35:39 WIB	2018-04-02 08:35:27 WIB	2018-04-02 08:35:27 WIB	816313
Planning.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~\$anning.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~\$RPORT INFORMATION.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's				2018-04-05 09:20:17 WIB	2018-04-05 09:20:17 WIB	2018-03-30 11:32:31 WIB	2018-03-30 11:32:25 WIB	286463

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

The Cloudy Manifesto

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 fellow man.

This may be the most absurd statement yet. This is like saying, when the speeding driver sees that everyone else is doing the speed limit, he will slow down. Well no, he's in a hurry and you are in his way. Just like when a shooter wants to do something...he does. The laws won't stop him, and neither will disarming yourself.

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!?

If only it were just a "pair" of sheep. Rather than thousands of sheep we really have. You want to protest the police that protect us, then you want to protest the guns that protect us. I don't think

Metadata

Name: /img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/The Cloudy Manifesto.docx

Type: File System

MIME Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document

Size: 816313

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2018-04-02 08:35:27 WIB

Accessed: 2018-04-02 08:35:27 WIB

Created: 2018-04-02 08:35:27 WIB

Changed: 2018-04-02 08:35:39 WIB

MD5: 14c07920ddc81fdbd489e61d60e5cf28

SHA-256: fee91c8baf9fb51574b11bfeed5a08b89e7bb90e874c07d95562c76380f2c65

Hash Lookup Results: UNKNOWN

Internal ID: 34811

From The Sleuth Kit istat Tool:

- Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop 46 Results

Table Thumbnail Summary

Page: Pages: ← → Go to Page: [] Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
The Cloudy Manifesto.docx		▼	1	2018-04-02 08:35:27 WIB	2018-04-02 08:35:39 WIB	2018-04-02 08:35:27 WIB	2018-04-02 08:35:27 WIB	816313
X Planning.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
X ~\$anning.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
id Amendment_files (207) ATION.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
X Cubs' Anthony Rizzo Praises Parkland Kids, Says It's				2018-04-05 09:20:17 WIB	2018-04-05 09:20:17 WIB	2018-03-30 11:32:31 WIB	2018-03-30 11:32:25 WIB	286463
X Larry King_ Time to Repeal the 'Poorly Written' Sec				2018-04-05 09:20:17 WIB	2018-04-05 09:20:17 WIB	2018-03-30 11:29:51 WIB	2018-03-30 11:29:48 WIB	289380
desktop.ini			1	2018-03-27 16:56:47 WIB	2018-03-27 16:56:47 WIB	2018-03-27 16:20:00 WIB	2018-03-27 16:20:00 WIB	282
BladeofGrass.jpg			1	2018-03-31 11:15:53 WIB	2018-04-02 08:12:46 WIB	2018-03-31 11:15:36 WIB	2018-03-31 11:15:53 WIB	201810

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

[Download Images](#)

Cubs' Anthony Rizzo: 'It's too Easy to Get a Gun'

53 [E](#) [G](#) [T](#)

Screenshot

by Warner Todd Huston 29 Mar 2018 322

29 Mar, 2018 29 Mar, 2018

Chicago Cubs first baseman Anthony Rizzo has made his strongest gun control statement yet, saying that he thinks laws need to be changed to make it harder for Americans to buy firearms.

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'.html
 Type: File System
 MIME Type: text/html
 Size: 286463
 File Name Allocation: Unallocated
 Metadata Allocation: Unallocated
 Modified: 2018-04-05 09:20:17 WIB
 Accessed: 2018-03-30 11:32:31 WIB
 Created: 2018-03-30 11:32:25 WIB
 Changed: 2018-04-05 09:20:17 WIB
 MD5: Not calculated
 SHA-256: Not calculated
 Hash Lookup Results: UNKNOWN
 Internal ID: 384980

From The Sleuth Kit iStat Tool:

- Larry King_ Time to Repeal the 'Poorly Written' Second Amendment

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop
This is a DirectoryTree window 46 Results

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
The Cloudy Manifesto.docx		1		2018-04-02 08:35:27 WIB	2018-04-02 08:35:39 WIB	2018-04-02 08:35:27 WIB	2018-04-02 08:35:27 WIB	816313
Planning.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~\$anning.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~\$RPORT INFORMATION.docx				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's				2018-04-05 09:20:17 WIB	2018-04-05 09:20:17 WIB	2018-03-30 11:32:31 WIB	2018-03-30 11:32:25 WIB	286463
Larry King_Time to Repeal the 'Poorly Written' Sec				2018-04-05 09:20:17 WIB	2018-04-05 09:20:17 WIB	2018-03-30 11:29:51 WIB	2018-03-30 11:29:48 WIB	289380
desktop.ini		1		2018-03-27 16:56:47 WIB	2018-03-27 16:56:47 WIB	2018-03-27 16:20:00 WIB	2018-03-27 16:20:00 WIB	282
BladeofGrass.jpg		1		2018-03-31 11:15:53 WIB	2018-04-02 08:12:46 WIB	2018-03-31 11:15:36 WIB	2018-03-31 11:15:53 WIB	201810

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

Download Images

Larry King: Time to Repeal the 'Poorly Written' Second Amendment

4017

Rich Fury/Getty Images

by AWR Hawkins 29 Mar 2018 2,936

29 Mar, 2018 29 Mar, 2018

Former CNN anchor-turned celebrity interviewer Larry King says he supports repealing the “poorly written” Second Amendment.

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Larry King_Time to Repeal the 'Poorly Written' Second Amendment.html
 Type: File System
 MIME Type: text/html
 Size: 289380
 File Name Allocation: Unallocated
 Metadata Allocation: Unallocated
 Modified: 2018-04-05 09:20:17 WIB
 Accessed: 2018-03-30 11:29:51 WIB
 Created: 2018-03-30 11:29:48 WIB
 Changed: 2018-04-05 09:20:17 WIB
 MD5: Not calculated
 SHA-256: Not calculated
 Hash Lookup Results: UNKNOWN
 Internal ID: 384978

From The Sleuth Kit iStat Tool:

- AMEN

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop

46 Results

Table Thumbnail Summary

Page: Pages: < > Go to Page: [] Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Sheep.jpg:Zone.Identifier			0	2018-03-30 10:32:40 WIB	2018-04-02 08:12:46 WIB	2018-03-30 10:32:34 WIB	2018-03-30 10:32:40 WIB	177
Box Sync.lnk			1	2018-03-28 07:53:57 WIB	2018-03-28 07:54:04 WIB	2018-03-28 07:53:57 WIB	2018-03-28 07:53:57 WIB	1606
Dropbox.lnk			1	2018-03-28 07:06:27 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:06:27 WIB	2018-03-28 07:06:27 WIB	1303
Google Drive.lnk			1	2018-03-28 07:43:22 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:43:22 WIB	2018-03-28 07:43:22 WIB	1766
AMEN.pdf		▼	0	2018-04-06 10:55:03 WIB	2018-04-06 10:55:13 WIB	2018-04-06 10:55:02 WIB	2018-04-06 10:55:00 WIB	371701
LeftUsesBoycotts.pdf		▼	0	2018-04-06 10:56:37 WIB	2018-04-06 10:56:43 WIB	2018-04-06 10:56:33 WIB	2018-04-06 10:56:31 WIB	1470817
SelfDefenseisMurder.pdf		▼	0	2018-04-05 12:48:42 WIB	2018-04-05 12:48:52 WIB	2018-04-05 12:48:41 WIB	2018-04-05 12:48:40 WIB	609290
UKknifeBan.pdf		▼	0	2018-04-05 12:51:45 WIB	2018-04-05 12:51:54 WIB	2018-04-05 12:51:42 WIB	2018-04-05 12:51:41 WIB	1051631
DarkWolf.pnp			1	2018-03-30 10:33:51 WIB	2018-03-30 08:12:46 WIB	2018-03-30 10:33:41 WIB	2018-03-30 10:33:50 WIB	603740

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

theblaze
www.theblaze.com

'You can't fight the government'? It's time to debunk this popular anti-gun talking point

Glenn Beck (<http://www.theblaze.com/glenn-beck>) 10 hours

A common anti-Second Amendment argument goes like this: The Founding Fathers thought that people needed guns to have a way to resist the government, but clearly nowadays, you can't use a rifle to prevent a tank from running over you. Guns are useless against the government, so we don't need them in the way the founders intended.

On today's show, Stu pointed out some practical facts that debunk this view of the argument. Yes, if the...

Page 1 / 1

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

Metadata

Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/AMEN.pdf
Type:	File System
MIME Type:	application/pdf
Size:	371701
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-04-06 10:55:03 WIB
Accessed:	2018-04-06 10:55:02 WIB
Created:	2018-04-06 10:55:00 WIB
Changed:	2018-04-06 10:55:13 WIB
MD5:	5c21578283b9c5cc058f4faa2d5365ee
SHA-256:	c92b417cb72aaa39e0e7ec891a593be41a0a5f44e0025747c93cdea9f4248170
Hash Lookup Results:	UNKNOWN
Internal ID:	34759

From The Sleuth Kit istat Tool:

- LeftUsesBoycotts

This is a DirectoryTree window

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Sheep.jpg:Zone.Identifier			0	2018-03-30 10:32:40 WIB	2018-04-02 08:12:46 WIB	2018-03-30 10:32:34 WIB	2018-03-30 10:32:40 WIB	177
Box Sync.lnk			1	2018-03-28 07:53:57 WIB	2018-03-28 07:54:04 WIB	2018-03-28 07:53:57 WIB	2018-03-28 07:53:57 WIB	1606
Dropbox.lnk			1	2018-03-28 07:06:27 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:06:27 WIB	2018-03-28 07:06:27 WIB	1303
Google Drive.lnk			1	2018-03-28 07:43:22 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:43:22 WIB	2018-03-28 07:43:22 WIB	1766
AMEN.pdf		▼	0	2018-04-06 10:55:03 WIB	2018-04-06 10:55:13 WIB	2018-04-06 10:55:02 WIB	2018-04-06 10:55:00 WIB	371701
LeftUsesBoycotts.pdf		▼	0	2018-04-06 10:56:37 WIB	2018-04-06 10:56:43 WIB	2018-04-06 10:56:33 WIB	2018-04-06 10:56:31 WIB	1470817
SelfDefenseisMurder.pdf		▼	0	2018-04-05 12:48:42 WIB	2018-04-05 12:48:52 WIB	2018-04-05 12:48:41 WIB	2018-04-05 12:48:40 WIB	609290
UKknifeBan.pdf		▼	0	2018-04-05 12:51:45 WIB	2018-04-05 12:51:54 WIB	2018-04-05 12:51:42 WIB	2018-04-05 12:51:41 WIB	1051631
DarkWolf.pptx			1	2018-02-20 10:22:51 WIB	2018-01-02 08:12:46 WIB	2018-02-20 10:22:41 WIB	2018-02-20 10:22:50 WIB	603740

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

Commentary: How the left bullies everyone who disagrees with them, and what you should do about it

7 hours

Page 1 / 4

Displays the binary contents of a file as hexadecimal, with bytes that are displayable as ASCII characters on the right.

Name: /img_LoneWolf.E01/vol_vo17/Users/jcloudy/Desktop/LeftUsesBoycotts.pdf

Type: File System

MIME Type: application/pdf

Size: 1470817

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2018-04-06 10:56:37 WIB

Accessed: 2018-04-06 10:56:33 WIB

Created: 2018-04-06 10:56:31 WIB

Changed: 2018-04-06 10:56:43 WIB

MDS: 1822aa3999e889942938c5f9bb4f2908

SHA-256: 2abe281c71d0da916533ab2fd057c375134bbba423dbf89f2e681c76235e7c6

Hash Lookup Results: UNKNOWN

Internal ID: 34800

From The Sleuth Kit iStat Tool:

- SelfDefenseisMurder

46 Results

This is a DirectoryTree window.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Sheep.jpg:Zone.Identifier			0	2018-03-30 10:32:40 WIB	2018-04-02 08:12:46 WIB	2018-03-30 10:32:34 WIB	2018-03-30 10:32:40 WIB	177
Box Sync.lnk			1	2018-03-28 07:53:57 WIB	2018-03-28 07:54:04 WIB	2018-03-28 07:53:57 WIB	2018-03-28 07:53:57 WIB	1606
Dropbox.lnk			1	2018-03-28 07:06:27 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:06:27 WIB	2018-03-28 07:06:27 WIB	1303
Google Drive.lnk			1	2018-03-28 07:43:22 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:43:22 WIB	2018-03-28 07:43:22 WIB	1766
AMEN.pdf		▼	0	2018-04-06 10:55:03 WIB	2018-04-06 10:55:13 WIB	2018-04-06 10:55:02 WIB	2018-04-06 10:55:00 WIB	371701
LeftUsesBoycotts.pdf		▼	0	2018-04-06 10:56:37 WIB	2018-04-06 10:56:43 WIB	2018-04-06 10:56:33 WIB	2018-04-06 10:56:31 WIB	1470817
SelfDefenseisMurder.pdf		▼	0	2018-04-05 12:48:42 WIB	2018-04-05 12:48:52 WIB	2018-04-05 12:48:41 WIB	2018-04-05 12:48:40 WIB	609290
UKknifeBan.pdf		▼	0	2018-04-05 12:51:45 WIB	2018-04-05 12:51:54 WIB	2018-04-05 12:51:42 WIB	2018-04-05 12:51:41 WIB	1051631
DarkWolf.pnp			1	2018-02-20 10:33:51 WIB	2018-02-20 10:33:46 WIB	2018-02-20 10:33:41 WIB	2018-02-20 10:33:50 WIB	603780

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



A 78-year-old man has been arrested on suspicion of murder after a suspected burglar was stabbed to death.

The man, named locally as Richard Osborn-Brooks, discovered two intruders in South Park Crescent, Hither Green, south-east London, at about 00:45 BST.

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/SelfDefenseisMurder.pdf

Type: File System

MIME Type: application/pdf

Size: 609290

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2018-04-05 12:48:42 WIB

Accessed: 2018-04-05 12:48:41 WIB

Created: 2018-04-05 12:48:40 WIB

Changed: 2018-04-05 12:48:52 WIB

MD5: 215dd901860ce43a480123f15a85a15e

SHA-256: 0b1a0528b5ece3cd43fde1df25b630470b3e6c8c6e464326d3b36196e3cf3dd8

Hash Lookup Results: UNKNOWN

Internal ID: 34809

- UKknifeBan

46 Result

Table [Thumbnail](#) [Summary](#)

Page: Pages: ← → Go to Page:

[Save Table as CSV](#)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
Sheep.jpg:Zone.Identifier			0	2018-03-30 10:32:40 WIB	2018-04-02 08:12:46 WIB	2018-03-30 10:32:34 WIB	2018-03-30 10:32:40 WIB	177
Box Sync.lnk			1	2018-03-28 07:53:57 WIB	2018-03-28 07:54:04 WIB	2018-03-28 07:53:57 WIB	2018-03-28 07:53:57 WIB	1606
Dropbox.lnk			1	2018-03-28 07:06:27 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:06:27 WIB	2018-03-28 07:06:27 WIB	1303
Google Drive.lnk			1	2018-03-28 07:43:22 WIB	2018-03-28 07:43:53 WIB	2018-03-28 07:43:22 WIB	2018-03-28 07:43:22 WIB	1766
AMEN.pdf	▼		0	2018-04-06 10:55:03 WIB	2018-04-06 10:55:13 WIB	2018-04-06 10:55:02 WIB	2018-04-06 10:55:00 WIB	371701
LeftUsesBoycotts.pdf	▼		0	2018-04-06 10:56:37 WIB	2018-04-06 10:56:43 WIB	2018-04-06 10:56:33 WIB	2018-04-06 10:56:31 WIB	1470817
SelfDefenseisMurder.pdf	▼		0	2018-04-05 12:48:42 WIB	2018-04-05 12:48:52 WIB	2018-04-05 12:48:41 WIB	2018-04-05 12:48:40 WIB	609290
UKknifeBan.pdf	▼		0	2018-04-05 12:51:45 WIB	2018-04-05 12:51:54 WIB	2018-04-05 12:51:42 WIB	2018-04-05 12:51:41 WIB	1051631
DarkWolf.png			1	2018-04-07 10:32:41 WIB	2018-04-07 10:32:41 WIB	2018-04-07 10:32:41 WIB	2018-04-07 10:32:40 WIB	602710

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

1 of 5 100%

Top doctor: Ban deadly blades from our kitchens

ONE of Scotland's leading doctors has called for a ban on "killer" kitchen knives.

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/UKknifeBan.pdf

Type: File System

MIME Type: application/pdf

Size: 1051631

File Name Allocation: Allocated

Metadata Allocation: Allocated

Modified: 2018-04-05 12:51:45 WIB

Accessed: 2018-04-05 12:51:42 WIB

Created: 2018-04-05 12:51:41 WIB

Changed: 2018-04-05 12:51:54 WIB

MDS: 3e79634bf0f7c45c0b7b40ff965e84b9

SHA-256: 3d316b3cf208b985f85c23a4116c30de75ae4ecabc879e5e2932a5d51686e130

Hash Lookup Results: UNKNOWN

Internal ID: 34813

From The Sleuth Kit istat Tool:

- Operation 2nd Hand Smoke

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop 46 Result

Table Thumbnail Summary

Page: Pages: ← → Go to Page: [] Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
UKkniteBan.pdt	Y		U	2018-04-05 12:51:45 WIB	2018-04-05 12:51:54 WIB	2018-04-05 12:51:42 WIB	2018-04-05 12:51:41 WIB	1051631
DarkWolf.png		1		2018-03-30 10:33:51 WIB	2018-04-02 08:12:46 WIB	2018-03-30 10:33:41 WIB	2018-03-30 10:33:50 WIB	603749
DarkWolf.png:Zone.Identifier		0		2018-03-30 10:33:51 WIB	2018-04-02 08:12:46 WIB	2018-03-30 10:33:41 WIB	2018-03-30 10:33:50 WIB	161
Huckleberry.png		1		2018-03-31 11:23:25 WIB	2018-04-02 08:12:46 WIB	2018-03-31 11:23:16 WIB	2018-03-31 11:23:25 WIB	306471
Huckleberry.png:Zone.Identifier		0		2018-03-31 11:23:25 WIB	2018-04-02 08:12:46 WIB	2018-03-31 11:23:16 WIB	2018-03-31 11:23:25 WIB	217
Operation 2nd Hand Smoke.pptx	V	1		2018-04-04 12:11:27 WIB	2018-04-04 12:11:53 WIB	2018-04-04 12:11:27 WIB	2018-04-04 11:56:19 WIB	4408968
~WRL2465.tmp				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~WRL3075.tmp				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0
~WRL3075.tmp				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0

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

Strings Extracted Text Translation

Page: 1 of 1 Page ← → Matches on page: - of - Match ← → 100% ⚡ ⌂ Reset Text Source: File Text

OPERATION 2ND HAND SMOKE

Event: 1230 – 1400
Flight:

Park

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx
Type: File System
MIME Type: application/vnd.openxmlformats-officedocument.presentationml.presentation
Size: 4408968
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2018-04-04 12:11:27 WIB
Accessed: 2018-04-04 12:11:27 WIB
Created: 2018-04-04 11:56:19 WIB
Changed: 2018-04-04 12:11:53 WIB
MD5: b301fbf4104fb64b566b076c12a5d113
SHA-256: 7b08d680f342f3d28a79c2a324bfd0576586958992cd738319aec3cc5d1e129
Hash Lookup Results: UNKNOWN
Internal ID: 34802

From The Sleuth Kit iStat Tool:

AutoSave off Operation 2nd Hand Sm... • Saved to this PC Search

File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help

Clipboard Slides

Font Paragraph Drawing Editing Add-ins

Event: 1230 – 1400 Flight:

RESISTANCE CALENDAR ADD EVENT

SAT APR 7 Town Hall For Our Lives Sterling, VA

LOCATION 21030 Wharf Rd, Sterling, VA, 20165

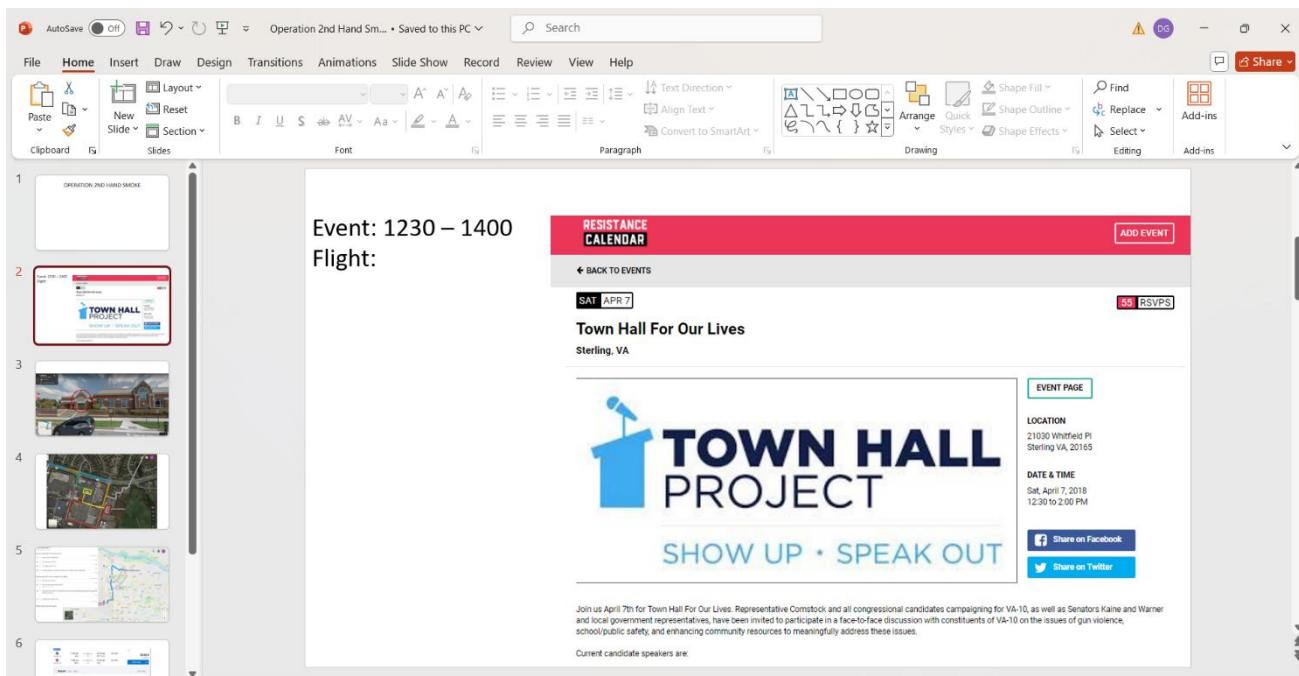
DATE & TIME Sat, April 7, 2018 12:30 to 2:00 PM

Share on Facebook Share on Twitter

SHOW UP • SPEAK OUT

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:



AutoSave off Operation 2nd Hand Sm... • Saved to this PC Search

File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help

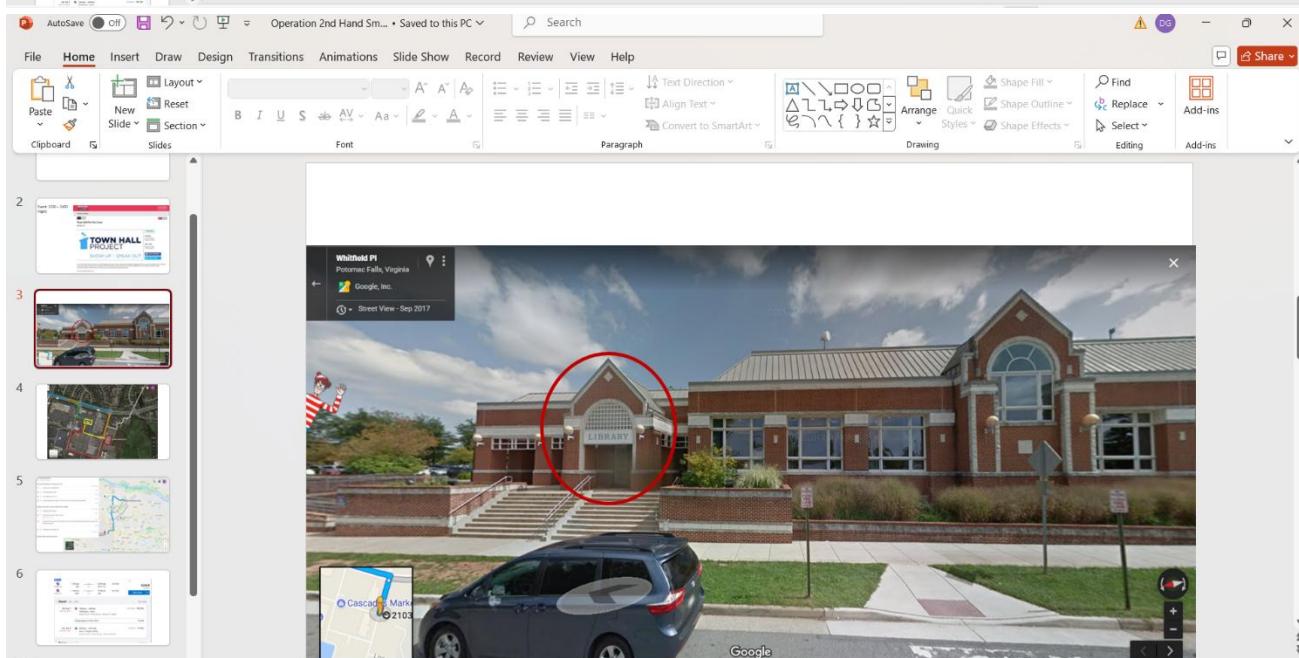
Clipboard Slides

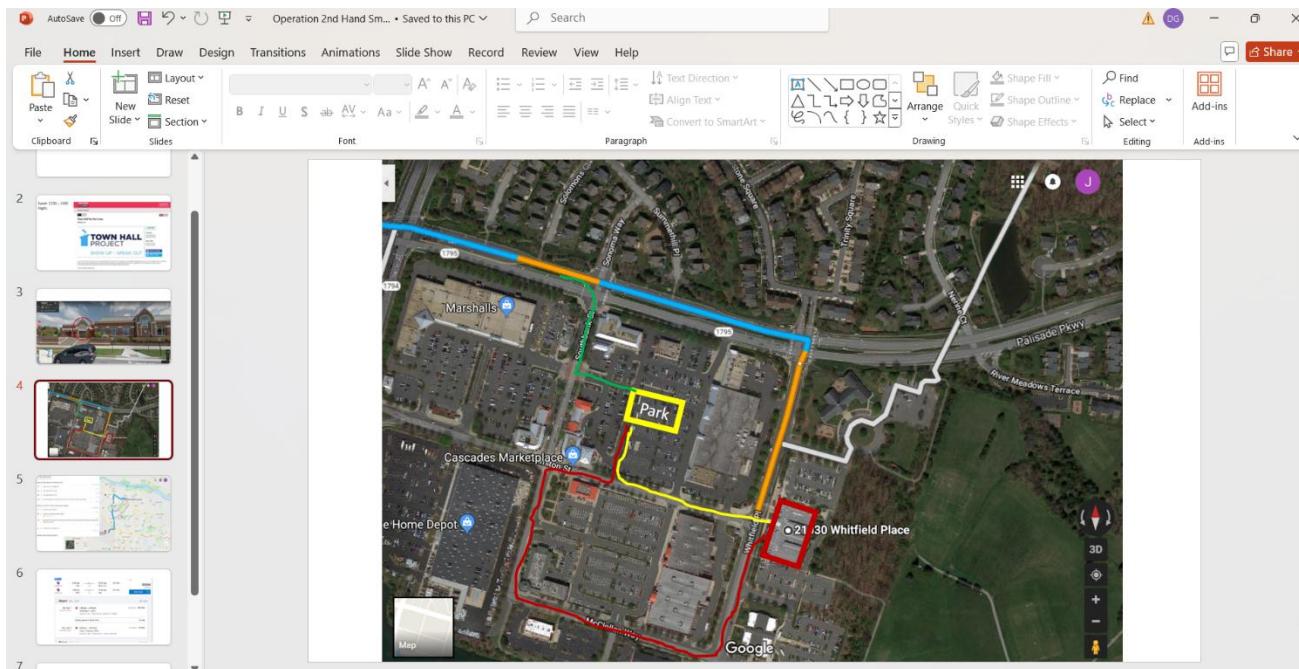
Font Paragraph Drawing Editing Add-ins

Whitfield PI Potomac Falls, Virginia Google, Inc. Street View - Sep 2017

LIBRARY

Google





This screenshot shows a Microsoft Word document with driving directions. The first section, titled '21030 Whitfield Pl Potomac Falls, VA 20165', provides instructions to get on VA-28 S from VA-1795 and VA-7 W. The second section, 'Continue on VA-28 S. Drive to Saarinen Cir in Dulles', continues the route to Dulles International Airport. The third section, 'Dulles International Airport', shows a detailed map of the airport area. The map includes labels for 'International Airport', 'Steven F. Udvar-Hazy Center', 'Dulles Access Rd', 'Reston', 'Herndon', 'Hannington', 'Floris', 'Lake Fairfax Park', 'Great Falls', 'Shady Oak', 'Seneca', 'Lowes Island', 'Volcano Island Waterpark', and 'Sterling'. It also shows various roads like 'VA-28', 'VA-7', 'VA-1795', 'VA-190', and 'VA-112'. A compass rose and a scale bar are included.

AutoSave (Off) Search

File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help

Paste New Slide Section Slides

Font Paragraph Drawing Editing Add-ins

2 Paste (Ctrl+V)
Add content on the Clipboard to your document.

3

4

5

6

Flight	Time	Airline	From	To	Duration
1:20 pm	Korean Air	IAD	ICN	DPS (+2)	22h 50m
1:20 am	Korean Air	DPS	ICN	IAD	22h 00m

\$2424 KAYAK

View Deal

7

Flight	Time	Airline	From	To	Duration
1:20 pm — 4:50 pm	Korean Air 94	IAD	Seoul	Washington	14h 30m
6:05 pm — 12:10 am	Korean Air 629	DPS	Bali	Denpasar	7h 05m

AutoSave (Off) Search

File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help

Paste New Slide Section Slides

Font Paragraph Drawing Editing Add-ins

3

4

5

6

Check-in	Check-out	Rooms	Adults	Children
Apr 8	Apr 20	1 room	1 adult	0 children

6 people are viewing this hotel

SAVE \$11 Expedia \$58 View Deal >

SAVE \$11 Hotels.com \$58 View Deal >

SAVE \$11 Orbitz \$58 View Deal >

Booking.com \$62 Travelocity \$58 View all 8 deals >

Certificate of Excellence

Traveler (589)

Room & Suite (230)

Pool & Beach (202)

All photos (936)

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

- Brother Chat

This is a DirectoryTree window
Table Thumbnail Summary

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Fla
[current folder]				2018-04-04 12:31:54 WIB	2018-04-04 12:31:54 WIB	2018-03-28 07:43:22 WIB	2018-03-28 07:43:22 WIB	56	Allocated	Allc
[parent folder]				2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-28 07:53:56 WIB	2018-03-27 16:18:58 WIB	256	Allocated	Allc
.tmp.drivedownload				2018-04-04 12:32:04 WIB	2018-04-04 12:32:04 WIB	2018-04-02 08:36:28 WIB	2018-04-01 03:09:54 WIB	48	Allocated	Allc
The Cloudy Manifesto.docx	▼	1		2018-04-02 08:35:27 WIB	2018-04-02 08:36:35 WIB	2018-04-02 08:36:28 WIB	2018-04-02 08:36:28 WIB	816313	Allocated	Allc
Brother Chat.gdoc	▼	0		2018-04-06 14:20:00 WIB	2018-04-06 14:21:28 WIB	2018-04-06 14:20:00 WIB	2018-04-01 03:09:54 WIB	178	Allocated	Allc
desktop.ini		0		2018-03-28 07:43:36 WIB	2018-03-28 07:43:36 WIB	2018-03-28 07:43:36 WIB	2018-03-28 07:43:22 WIB	174	Allocated	Allc
Operation 2nd Hand Smoke.pptx	▼	1		2018-04-04 12:11:27 WIB	2018-04-04 12:32:04 WIB	2018-04-04 12:31:54 WIB	2018-04-04 12:31:54 WIB	4408968	Allocated	Allc

Save Table as CSV

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% Reset Text Source: File Text

{"url": "https://docs.google.com/open?id=1GOv7MwOXM-7Vkoy4kjE3Q5bMDB5lWA0tB57a3u2hqeA", "doc_id": "1GOv7MwOXM-7Vkoy4kjE3Q5bMDB5lWA0tB57a3u2hqeA", "email": "jimcloudy1@gmail.com"}

METADATA

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Google Drive/Brother Chat.gdoc
Type: File System
MIME Type: text/plain
Size: 178
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2018-04-06 14:20:00 WIB
Accessed: 2018-04-06 14:20:00 WIB
Created: 2018-04-01 03:09:54 WIB
Changed: 2018-04-06 14:21:28 WIB
MD5: 9eb42bf9159828639cc2f30214050e0f
SHA-256: 09b278b3c798bdcc3e77ec5a10a3096b9b6c766e14e84655d54511ae5912da19
Hash Lookup Results: UNKNOWN
Internal ID: 36017

From The Sleuth Kit istat Tool:

- Jim's Notebook

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/OneDrive/Documents

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	K
[current folder]				2018-03-27 16:50:14 WIB	2018-03-27 16:50:14 WIB	2018-03-27 16:50:14 WIB	2018-03-27 16:50:14 WIB	280	Allocated	Allocated	u
[parent folder]				2018-04-05 09:21:38 WIB	2018-04-05 09:21:38 WIB	2018-04-05 09:21:38 WIB	2018-03-27 16:21:44 WIB	56	Allocated	Allocated	u
Jim's Notebook.url		0		2018-04-06 11:03:46 WIB	2018-04-06 13:14:39 WIB	2018-04-06 13:14:39 WIB	2018-03-27 16:50:14 WIB	120	Allocated	Allocated	u

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: - of - Match 100% ⌂ ⌃ Reset Text Source: File Text

[InternetShortcut]
URL=https://onedrive.live.com/redir.aspx?cid=b5e4e0f22924dca&resid=B5E4E06F22924DCA!110&type=3

-----METADATA-----

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/OneDrive/Documents/Jim's Notebook.url
Type: File System
MIME Type: text/plain
Size: 120
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2018-04-06 11:03:46 WIB
Accessed: 2018-04-06 13:14:39 WIB
Created: 2018-03-27 16:50:14 WIB
Changed: 2018-04-06 13:14:39 WIB
MD5: 840fb715c63dc194fea68033a1c77844
SHA-256: 34130062b0dc3268b775fecc08d5316b3fc037c68df201049f4507c05785cf1f
Hash Lookup Results: UNKNOWN
Internal ID: 36111

From The Sleuth Kit istat Tool:

• 000044.idb

paul								67 Results
Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time	
000044.idb			0	ibilBrother ChatHey, «Paul» its me. Just thought this	paul	2018-04-06 14:20:02 WIB	2018-04-06 14:20:02 WIB	
000238.idb			0	lawyer floAGideal]],s for «Paul» M-4 and Michael Fl\ pre paul		2018-04-06 11:07:40 WIB	2018-04-06 11:07:40 WIB	
000265.idb			0	&e"A>=]~)sue lm-dTEmp%NA(«Paul» J ask% fEJl judEo paul		2018-04-06 19:37:12 WIB	2018-04-06 19:37:12 WIB	
89e6ac2f397707d8_blobs.bin			0	KEY_LOCMACHV ScanRemove%0< paul<JAMAICADUCT_ paul		2018-04-06 12:49:03 WIB	2018-03-27 16:36:48 WIB	
Adios Script Pro.otf			0	(c) 2009 by Alejandro «Paul». All rights reserved.Adios	paul	2018-03-27 17:49:08 WIB	2018-03-27 17:47:43 WIB	
Alphabet.xml			1	VÉRITABLE CHEF-D'ŒUVRE ! «Paul» : "Une chaîne sp	paul	2017-09-29 21:43:12 WIB	2017-09-29 21:43:12 WIB	
Alphabet.xml			1	VÉRITABLE CHEF-D'ŒUVRE ! «Paul» : "Une chaîne sp	paul	2017-09-29 21:43:12 WIB	2017-09-29 21:43:12 WIB	
Cloudy thoughts (4apr).docx			0	remain in the cloud and «Paul» will have the only other	paul	2018-04-05 09:39:30 WIB	2018-04-05 09:39:30 WIB	

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

Strings	Extracted Text	Translation
Page: 2 of 3 Page		
Matches on page: 1 of 1 Match		
100% Reset		
Text Source: Search Results		
Hey, Paul its me. Just thought this would be easier and safer honestly. WTF, Jim. This is wierd. What are you researching that would bring th feds to your door? Why would anyone care what you research, there are thousands of people researching guns and gun control now days. Why would you stand out? im not saying I would stand out, I m just condemed. I just read somewhere about a family who s mom researched a crock pot and the dad researched a backpack and boom...feds at the door. So obviously they are watching everyone s history. I dont want to get visited by the cops. They want find any terrorism stuff, but I have a little garden they might be interested in once they arrive. So you are worried they will come by just to check and find a real reason to get you...ok Exactly, man. I just think that chatting on here will be simpler anyway. I promise not to get mad...lol. You k Xe%(an actual chat fun top H right? swit .8aved. A Dl.u fl f " Hev. 2		

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/Google Drive/Brother Chat.gdoc
Type: File System
MIME Type: text/plain
Size: 178
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2018-04-06 14:20:00 WIB
Accessed: 2018-04-06 14:20:00 WIB
Created: 2018-04-01 03:09:54 WIB
Changed: 2018-04-06 14:21:28 WIB
MD5: 9eb42bf9159828639cc2f30214050e0f
SHA-256: 09b278b3c798bddc3e77ec5a10a3096b9b6c766e14e84655d54511ae5912da19
Hash Lookup Results: UNKNOWN
Internal ID: 36017

From The Sleuth Kit istat Tool:

- 00000003.bin

This is a DirectoryTree window

Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time
0			0	"onenotesuccess"]=""«My notebook» opened successfull. my notebook	my notebook	0000-00-00 00:00:00	0000-00-00 00:00:00
00000003.bin			0	LightYou start with «My Notebook» - everything lives	my notebook	2018-04-05 15:35:33 WIB	2018-03-27 16:50:22
IEAWSDC.DLL			0	Microsoft\FrontPage\Pages\{My Notebook\}\Documen	my notebook	2018-03-27 16:36:15 WIB	2018-03-27 16:36:15
f_0014fd			0	inf\My Documents\{My Notebook\}\My Templates\{M..	my notebook	2018-03-27 16:42:27 WIB	2018-03-27 16:41:57
f_002b7f			0	OneNoteoneneoteappname«My notebook» opened succ	my notebook	2018-03-31 04:17:35 WIB	2018-03-31 04:17:35
f_002b86			0	OneNoteoneneoteappname«My notebook» opened succ	my notebook	2018-04-06 11:07:45 WIB	2018-04-06 11:07:45
nv3deng.chm			0	L_PageTitleLabel~ghShare <my notebook>L_TellMeTry.	my notebook	2018-04-06 11:07:45 WIB	2018-04-06 11:07:45
nvmnbls.dll			0	additional displays on «my notebook» computer?	my notebook	2016-12-29 20:15:27 WIB	2018-03-27 16:21:04
				when «mv notebook» is uninstalledAfter «mv notebook mv notebook	my notebook	2016-12-29 20:16:13 WIB	2018-03-27 16:21:04

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: 1 of 7 Match 100% Text Source: Search Results

```
"O6(
Cloud Thoughts
This might be a better way to keep my thoughts organized, as I can keep a running tab instead of creating new documents every time. I'm still nervous and worried that this wont go as planned, but I'm really looking forward to what could be a fresh start in Bali. This wont be an easy transition, but I hope everyone can understand why I must do this for my country.
2. Get organized
You start with "My Notebook" - everything lives in here
IHDR
sRGB
gAMA
pHYs
IDATx^
5 RD
S!
%
?<<
*=82
"8\9
HF
HF
uc
```

Metadata

Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/LocalState/AppData/Local/OneNote/16.0/cache/00000003.bin
Type:	File System
MIME Type:	application/octet-stream
Size:	110592
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-04-05 15:35:33 WIB
Accessed:	2018-03-27 16:50:22 WIB
Created:	2018-03-27 16:50:22 WIB
Changed:	2018-04-05 15:35:33 WIB
MD5:	91a3b1ebc0b2ae450b96e2fec74f3665
SHA-256:	4b5714b1cd1323e4c03e8b2eb42bc9bf239711c6bd0e082068604a8de425a888
Hash Lookup Results:	UNKNOWN
Internal ID:	29985

- f_0017c1

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache 7625 Results

This is a DirectoryTree window.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
...				2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	75419	Unallocated	Unallocated
f_0017bc				2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	75419	Unallocated	Unallocated
f_0017c0				2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	30766	Unallocated	Unallocated
f_0017c1				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	17073	Unallocated	Unallocated
f_0017c2				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	19226	Unallocated	Unallocated
f_0017c3				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18955	Unallocated	Unallocated
f_0017c4				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18939	Unallocated	Unallocated
f_0017c5				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18959	Unallocated	Unallocated
f_0017c6				2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	18959	Unallocated	Unallocated

Save Table as CSV

Page: 1 of 1 Pages: Go to Page: Save Table as CSV

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

0° 130% Tags Menu

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c1
Type: File System
MIME Type: image/jpeg
Size: 17073
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 2018-03-31 11:44:27 WIB
Accessed: 2018-03-31 11:44:27 WIB
Created: 2018-03-31 11:44:27 WIB
Changed: 2018-03-31 11:44:27 WIB
MD5: c70a5efd5f023576dfbb8797d8ba06b1
SHA-256: 31e1c3d2d915b7bce4d048f3c987b16896b7e1e4bccdecf525f175a80e9d00df
Hash Lookup Results: UNKNOWN
Internal ID: 15848

From The Sleuth Kit iStat Tool:

• f_0017c2

/img_LoneWolf.E01/vol_voi7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache											7625 Results
Table Thumbnail Summary Page: 1 of 1 Pages: Go to Page: <input type="text"/>											Save Table as CSV
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	
f_0017c2				2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	75419	Unallocated	Unallocated	
f_0017c0				2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	30766	Unallocated	Unallocated	
f_0017c1				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	17073	Unallocated	Unallocated	
f_0017c2				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	19226	Unallocated	Unallocated	
f_0017c3				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18955	Unallocated	Unallocated	
f_0017c4				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18939	Unallocated	Unallocated	
f_0017c5				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18959	Unallocated	Unallocated	
f_0017c6				2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	18959	Unallocated	Unallocated	

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

0° 130% Reset Tags Menu



Metadata

Name: /img_LoneWolf.E01/vol_voi7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c2
 Type: File System
 MIME Type: image/jpeg
 Size: 19226
 File Name Allocation: Unallocated
 Metadata Allocation: Unallocated
 Modified: 2018-03-31 11:44:27 WIB
 Accessed: 2018-03-31 11:44:27 WIB
 Created: 2018-03-31 11:44:27 WIB
 Changed: 2018-03-31 11:44:27 WIB
 MD5: 8bd95702f8e6f758e44c34bb42834299
 SHA-256: e6cffa5ddc8fac93fb1eb2b50d7523a0c360c8c61c558e654224a11fc5f5917
 Hash Lookup Results: UNKNOWN
 Internal ID: 15850

From The Sleuth Kit istat Tool:

- f_0017c4

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache 7625 Results

This is a DirectoryTree window

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
...				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	23012	Unallocated	Unallocated
✗ f_0017bc				2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	2018-03-31 11:44:14 WIB	75419	Unallocated	Unallocated
✗ f_0017c0				2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	2018-03-31 11:44:26 WIB	30766	Unallocated	Unallocated
✗ f_0017c1	▼			2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	17073	Unallocated	Unallocated
✗ f_0017c2				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	19226	Unallocated	Unallocated
✗ f_0017c3	▼			2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18955	Unallocated	Unallocated
✗ f_0017c4	▼			2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18939	Unallocated	Unallocated
✗ f_0017c5				2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	2018-03-31 11:44:27 WIB	18959	Unallocated	Unallocated
✗ f_0017c6				2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	2018-03-31 11:44:28 WIB	18959	Unallocated	Unallocated

Save Table as CSV

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

0° C C 130% ⌂ ⌂ Reset Tags Menu

Metadata

Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c4
Type: File System
MIME Type: image/jpeg
Size: 18939
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 2018-03-31 11:44:27 WIB
Accessed: 2018-03-31 11:44:27 WIB
Created: 2018-03-31 11:44:27 WIB
Changed: 2018-03-31 11:44:27 WIB
MD5: cde4c1ff31c6071605ef593f714a9de
SHA-256: 0ef7617d58d590677ae27ab5a1b30f0c98c33921553feda7bb4f4cf684c83348
Hash Lookup Results: UNKNOWN
Internal ID: 15854

From The Sleuth Kit iStat Tool:

- f0014920

Source Name	S	C	O	Keyword Preview	Keyword	Modified Time	Access Time	Change Time	File Path
f0014920.jpg			0	«f0014920».jpg	f0014920	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	/img_LoneWolf.E01/vol_vol7/\$CarvedFiles/1/f0014920.j
f0014920.png			0	«f0014920».png	f0014920	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	/img_LoneWolf.E01/vol_vol7/\$CarvedFiles/2/f0014920.p

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

0° C 99% | Reset Tags Menu



Metadata

Name:	/img_LoneWolf.E01/vol_vol7/\$CarvedFiles/1/f0014920.jpg
Type:	Carved
MIME Type:	image/jpeg
Size:	25024
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	0000-00-00 00:00:00
Accessed:	0000-00-00 00:00:00
Created:	0000-00-00 00:00:00
Changed:	0000-00-00 00:00:00
MD5:	43dfb947b72e8920256ec7927fe5f35b
SHA-256:	db9efaf4f671f6b25db5c14279132a3ac86fc206cc3fbebe44e9837d7701509ebb
Hash Lookup Results:	UNKNOWN
Internal ID:	412968

- f_001786 karena difile tidak terlihat pada autopsy saya extract file tersebut ke directory windows

Listing Keyword search 9 - f0014920 x | Keyword search 10 - jim notebook x | Keyword search 11 - paul x

This is a DirectoryTree window J:\users\jcloudy\AppData\Local\Google\Chrome\User Data\Default\Cache 7625 Results

Table Thumbnail Summary

Page: 1 of 1 Pages: ← → Go to Page: Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
				2010-03-31 11:42:20 WIB	2010-03-31 11:42:20 WIB	2010-03-31 11:42:20 WIB	2010-03-31 11:42:20 WIB	55000	Unallocated	Unallocated
✓_001786				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	44694	Unallocated	Unallocated
✓_f_00177f				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	50598	Unallocated	Unallocated
✓_f_001780				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	52511	Unallocated	Unallocated
✓_f_001781				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	56576	Unallocated	Unallocated
✓_f_001782	▼			2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	36461	Unallocated	Unallocated
✓_f_001783				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	42301	Unallocated	Unallocated
✓_f_001784				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	45327	Unallocated	Unallocated
✓_f_001785				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	25681	Unallocated	Unallocated
✓_f_001786				2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	2018-03-31 11:42:26 WIB	1	Unallocated	Unallocated

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

0° C C 130% ⌂ ⌂ Reset Tags Menu



Metadata	
Name:	/img_LoneWolf.E01/vol_vo17/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001786
Type:	File System
MIME Type:	image/png
Size:	25681
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2018-03-31 11:42:26 WIB
Accessed:	2018-03-31 11:42:26 WIB
Created:	2018-03-31 11:42:26 WIB
Changed:	2018-03-31 11:42:26 WIB
MD5:	df1624bf6b3f66b6b4061725d44327b8
SHA-256:	3b763c9849e3224e95b1b09caf5b63b491372946ccfac64296e52f87f14ce451
Hash Lookup Results:	UNKNOWN
Internal ID:	15776

From The Sleuth Kit Forensic Tool

• web artefak

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Keyword search 1 - Brother Chat... x

2402 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History	3			https://www.google.com/search?rlz=1C1CHB8_enUS/..._new nokia dual sim	2018-03-30 06:04:14 WIB	https://www.google.com/search?rlz=1C1CHB8_enUS/..._new nokia dual sim	In 5.7 ammo For Sa
History	0			https://www.nokia.com/en_int/phones/nokia-216-dual-~	2018-03-30 06:04:27 WIB	https://www.nokia.com/en_int/phones/nokia-216-dual-~ Nokia 216 Dual SIM	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Sort=5&PageSize=5	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Sort=5&PageSize=5 In 5.7 ammo For Sa	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In 5.7 ammo For Sa
History	3			https://mail.google.com/mail/u/0/#inbox/16270030a00	2018-04-01 03:07:23 WIB	https://mail.google.com/mail/u/0/#inbox/16270030a00 Computer - jimcloudy	In 5.7 ammo For Sa
History	3			https://www.google.com/search?q=ls+there+a+map+~	2018-03-30 06:13:25 WIB	https://www.google.com/search?q=ls+there+a+map+~ Is there a map of gu	In 5.7 ammo For Sa
History	3			https://maps.google.com/maps?q=ls+there+a+map+o.	2018-03-30 06:13:20 WIB	https://maps.google.com/maps?q=ls+there+a+map+o. National Rifle Assoc	In 5.7 ammo For Sa

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

Result: 292 of 2534 Result ← → Web History

Visit Details

Title: fn 5.7 ammo For Sale - Buy fn 5.7 ammo Online at GunBroker.com

Username: Default

Date Accessed: 2018-03-30 06:05:21 WIB

Domain: gunbroker.com

URL: https://www.gunbroker.com/All/search?Keywords=fn+5.7+ammo&Sort=5&PageSize=24

Referrer URL: https://www.gunbroker.com/All/search?Keywords=fn+5.7+ammo&Sort=5&PageSize=24

Program Name: Google Chrome

Source

Host: LoneWolf.E01_1 Host

Data Source: LoneWolf.E01

File: /img_LoneWolf.E01/vol_vo17/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/History

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Keyword search 1 - Brother Chat... x

2402 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History	3			https://www.google.com/search?rlz=1C1CHB8_enUS/..._new nokia dual sim	2018-03-30 06:04:14 WIB	https://www.google.com/search?rlz=1C1CHB8_enUS/..._new nokia dual sim	In 5.7 ammo For Sa
History	0			https://www.nokia.com/en_int/phones/nokia-216-dual-~	2018-03-30 06:04:27 WIB	https://www.nokia.com/en_int/phones/nokia-216-dual-~ Nokia 216 Dual SIM	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Sort=5&PageSize=5	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Sort=5&PageSize=5 In 5.7 ammo For Sa	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In 5.7 ammo For Sa
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In 5.7 ammo For Sa
History	3			https://mail.google.com/mail/u/0/#inbox/16270030a00	2018-04-01 03:07:23 WIB	https://mail.google.com/mail/u/0/#inbox/16270030a00 Computer - jimcloudy	In 5.7 ammo For Sa
History	3			https://www.google.com/search?q=ls+there+a+map+~	2018-03-30 06:13:25 WIB	https://www.google.com/search?q=ls+there+a+map+~ Is there a map of gu	In 5.7 ammo For Sa
History	3			https://maps.google.com/maps?q=ls+there+a+map+o.	2018-03-30 06:13:20 WIB	https://maps.google.com/maps?q=ls+there+a+map+o. National Rifle Assoc	In 5.7 ammo For Sa

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

Result: 295 of 2534 Result ← → Web History

Visit Details

Title: Computer - jimcloudy1@gmail.com - Gmail

Username: Default

Date Accessed: 2018-04-01 03:07:23 WIB

Domain: google.com

URL: https://mail.google.com/mail/u/0/#inbox/16270030a00a0b0

Referrer URL: https://mail.google.com/mail/u/0/#inbox/16270030a00a0b0

Program Name: Google Chrome

Source

Host: LoneWolf.E01_1 Host

Data Source: LoneWolf.E01

File: /img_LoneWolf.E01/vol_vo17/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/History

Case Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Keyword search 1 - Brother Chat... x 2402 Results

Web History Table Thumbnail Summary

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History	0			https://catalog.data.gov/dataset/?tags=911	2018-03-30 06:21:12 WIB	https://catalog.data.gov/dataset/?tags=911	Datasets - Data.gov
History	3			https://www.google.com/search?q=which+state+has+l...	2018-03-30 06:21:44 WIB	https://www.google.com/search?q=which+state+has+l...	which state has the l...
History	0			http://wqad.com/2016/06/15/the-10-states-with-the-w...	2018-03-30 06:21:51 WIB	http://wqad.com/2016/06/15/the-10-states-with-the-w...	The 10 States with t...
History	3			https://mail.google.com/mail/u/0/#inbox	2018-04-05 13:08:54 WIB	https://mail.google.com/mail/u/0/#inbox	Inbox (7) - jimcloud
History	3			https://mail.google.com/mail/u/0/#inbox/16270030...	2018-04-01 03:07:23 WIB	https://mail.google.com/mail/u/0/#inbox/16270030...	Computer - jimcloud
History	0			https://washington.org/DC-guide-to/washington-dc-air	2018-03-09:25:32 WIB	https://washington.org/DC-guide-to/washington-dc-air	Guide to Washingt...
History	3			https://docs.google.com/document?usp=drive_sync&...	2018-04-01 03:09:33 WIB	https://docs.google.com/document?usp=drive_sync&...	Google Docs
History	3			https://docs.google.com/document/?usp=drive_sync&...	2018-04-01 03:09:33 WIB	https://docs.google.com/document/?usp=drive_sync&...	Google Docs
History	3			https://docs.google.com/document/u/0/?usp=drive_sy...	2018-04-01 03:09:33 WIB	https://docs.google.com/document/u/0/?usp=drive_sy...	Google Docs

Save Table as CSV

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

Result: 327 of 2534 Result ← → Web History

Visit Details

Title: Guide to Washington, DC-Area Airports | Washington.org
 Username: Default
 Date Accessed: 2018-03-30 09:25:32 WIB
 Domain: washington.org
 URL: https://washington.org/DC-guide-to/washington-dc-airports
 Referrer URL: https://washington.org/DC-guide-to/washington-dc-airports
 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/UserData/Default/History

Analysis Results

- Encryption Suspected (3)
- EXIF Metadata (7)
- Extension Mismatch Detected (299)
- Interesting Items (9)
- Keyword Hits (46260)

Case Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing Keyword search 1 - Brother Chat... x 2402 Results

Web History Table Thumbnail Summary

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-31 11:32:34 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In .5/ ammo For Sal...
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-31 11:32:31 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In .57 ammo For Sal...
History	0			https://www.gunbroker.com/All/search?Keywords=fn%...	2018-03-31 11:32:34 WIB	https://www.gunbroker.com/All/search?Keywords=fn%...	In .57 ammo For Sal...
History	0			https://www.gunbroker.com/All/search?PageSize=24&...	2018-03-31 11:34:15 WIB	https://www.gunbroker.com/All/search?PageSize=24&...	9mm ammo For Sal...
History	0			https://www.gunbroker.com/All/search?Keywords=9m...	2018-03-31 11:34:15 WIB	https://www.gunbroker.com/All/search?Keywords=9m...	9mm ammo For Sal...
History	0			https://www.gunbroker.com/All/search?Keywords=9m...	2018-03-31 11:34:15 WIB	https://www.gunbroker.com/All/search?Keywords=9m...	9mm ammo For Sal...
History	0			https://www.gunbroker.com/All/search?Keywords=9m...	2018-03-31 11:34:15 WIB	https://www.gunbroker.com/All/search?Keywords=9m...	9mm ammo For Sal...
History	0			https://www.gunbroker.com/Pistol-Ammunition/search...	2018-03-31 11:34:22 WIB	https://www.gunbroker.com/Pistol-Ammunition/search...	Pistol Ammo - Hanc...
History	0			https://www.gunbroker.com/Pistol-Ammunition/search...	2018-03-31 11:34:23 WIB	https://www.gunbroker.com/Pistol-Ammunition/search...	Pistol Ammo - Hanc...

Save Table as CSV

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

Result: 574 of 2534 Result ← → Web History

Visit Details

Title: 9mm ammo For Sale - Buy 9mm ammo Online at GunBroker.com
 Username: Default
 Date Accessed: 2018-03-31 11:34:15 WIB
 Domain: gunbroker.com
 URL: https://www.gunbroker.com/All/search?PageSize=24&Sort=5
 Referrer URL: https://www.gunbroker.com/All/search?PageSize=24&Sort=5
 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/UserData/Default/History

Analysis Results

- Encryption Suspected (3)
- EXIF Metadata (7)
- Extension Mismatch Detected (299)
- Interesting Items (9)
- Keyword Hits (46260)

Web History							2402 Results	
Table				Thumbnail	Summary			Save Table as CSV
Source Name	S	C	O	△ URL	Date Accessed	Referrer URL	Title	
History			0	https://weather.com/	2018-04-06 15:25:20 WIB	https://weather.com/	National a	
History			0	https://weather.com/	2018-04-06 15:25:20 WIB	https://weather.com/	National a	
History			0	https://weather.com/	2018-04-06 15:25:20 WIB	https://weather.com/	National a	
History			0	https://weather.com/	2018-04-06 15:25:20 WIB	https://weather.com/	National a	
History			0	https://weather.com/weather/5day/l/IAD:9:US	2018-04-06 15:25:53 WIB	https://weather.com/weather/5day/l/IAD:9:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/IAD:9:US	2018-04-06 15:25:53 WIB	https://weather.com/weather/5day/l/IAD:9:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/IAD:9:US	2018-04-06 15:25:53 WIB	https://weather.com/weather/5day/l/IAD:9:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/IAD:9:US	2018-04-06 15:25:53 WIB	https://weather.com/weather/5day/l/IAD:9:US	5-Day We.	

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 1494 of 2534	Result	◀ ▶							Web History
Visit Details									
Title: 5-Day Weather Forecast for Washington Dulles International Airport - The Weather Channel Weather.com									
Username: Default									
Date Accessed: 2018-04-06 15:25:53 WIB									
Domain: weather.com									
URL: https://weather.com/weather/5day/l/IAD:9:US									
Referrer URL: https://weather.com/weather/5day/l/IAD:9:US									
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									

Web History							2402 Results	
Table				Thumbnail	Summary			Save Table as CSV
Source Name	S	C	O	△ URL	Date Accessed	Referrer URL	Title	
History			0	https://weather.com/weather/5day/l/IAD:9:US	2018-04-06 15:25:53 WIB	https://weather.com/weather/5day/l/IAD:9:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/IAD:9:US	2018-04-06 15:25:53 WIB	https://weather.com/weather/5day/l/IAD:9:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/IAD:9:US	2018-04-06 15:25:53 WIB	https://weather.com/weather/5day/l/IAD:9:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/USVA0949:1:US	2018-04-06 15:25:25 WIB	https://weather.com/weather/5day/l/USVA0949:1:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/USVA0949:1:US	2018-04-06 15:25:25 WIB	https://weather.com/weather/5day/l/USVA0949:1:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/USVA0949:1:US	2018-04-06 15:25:25 WIB	https://weather.com/weather/5day/l/USVA0949:1:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/USVA0949:1:US	2018-04-06 15:25:25 WIB	https://weather.com/weather/5day/l/USVA0949:1:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/USVA0949:1:US	2018-04-06 15:25:25 WIB	https://weather.com/weather/5day/l/USVA0949:1:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/USVA0949:1:US	2018-04-06 15:25:25 WIB	https://weather.com/weather/5day/l/USVA0949:1:US	5-Day We.	
History			0	https://weather.com/weather/5day/l/USVA0949:1:US	2018-04-06 15:25:25 WIB	https://weather.com/weather/5day/l/USVA0949:1:US	5-Day We.	

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 632 of 2534	Result	◀ ▶							Web History
Visit Details									
Title: 5-Day Weather Forecast for Huntington, VA - The Weather Channel Weather.com									
Username: Default									
Date Accessed: 2018-04-06 15:25:25 WIB									
Domain: weather.com									
URL: https://weather.com/weather/5day/l/USVA0949:1:US									
Referrer URL: https://weather.com/weather/5day/l/USVA0949:1:US									
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									

Web History 2402 Results

Table Thumbnail Summary Save Table as CSV

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History			3	https://www.google.com/search?q=cloud+storage+sol...	2018-03-28 06:42:35 WIB	https://www.google.com/search?q=cloud+storage+sol...	cloud stor...
History			3	https://www.google.com/search?q=concealable+tactic...	2018-03-31 11:36:31 WIB	https://www.google.com/search?q=concealable+tactic...	concealab...
History			3	https://www.google.com/search?q=concealable+tactic...	2018-03-31 11:37:14 WIB	https://www.google.com/search?q=concealable+tactic...	concealab...
History			3	https://www.google.com/search?q=concealable+tactic...	2018-03-31 11:36:57 WIB	https://www.google.com/search?q=concealable+tactic...	concealab...
History			3	https://www.google.com/search?q=do+indonesian+ba...	2018-04-05 12:58:57 WIB	https://www.google.com/search?q=do+indonesian+ba...	do indone...
History			3	https://www.google.com/search?q=do+the+cops+trac...	2018-04-01 03:03:23 WIB	https://www.google.com/search?q=do+the+cops+trac...	do the cop...
History			3	https://www.google.com/search?q=do+the+cops+trac...	2018-04-01 03:03:23 WIB	https://www.google.com/search?q=do+the+cops+trac...	do the cop...
History			3	https://www.google.com/search?q=doh+hamad+intern...	2018-04-01 02:57:09 WIB	https://www.google.com/search?q=doh+hamad+intern...	doh hama...
History			3	https://www.google.com/search?q=dropbox&rlz=1C1...	2018-04-02 08:40:05 WIB	https://www.google.com/search?q=dropbox&rlz=1C1...	dropbox -

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

Result: 1755 of 2534 Result ← →

Web History

Visit Details

Title: do indonesian banks cooperate with us government - Google Search
 Username: Default
 Date Accessed: 2018-04-05 12:58:57 WIB
 Domain: google.com
 URL: https://www.google.com/search?q=do+indonesian+banks+cooperate+with+us+government&rlz=1C1CHBF_enUS790US790&oq=do+indonesian+banks+cooperate+with+us+gov...
 Referrer URL: https://www.google.com/search?q=do+indonesian+banks+cooperate+with+us+government&rlz=1C1CHBF_enUS790US790&oq=do+indonesian+banks+cooperate+with+us+gov...
 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

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History			3	https://www.google.com/search?q=fairfax+democrate...	2018-04-03 13:14:42 WIB	https://www.google.com/search?q=fairfax+democrate...	fairfax der...
History			3	https://www.google.com/search?q=federal+governme...	2018-04-02 07:58:35 WIB	https://www.google.com/search?q=federal+governme...	federal go...
History			3	https://www.google.com/search?q=federal+governme...	2018-04-02 07:58:35 WIB	https://www.google.com/search?q=federal+governme...	federal go...
History			3	https://www.google.com/search?q=flights+to+indones...	2018-04-01 02:52:52 WIB	https://www.google.com/search?q=flights+to+indones...	flights to i...
History			3	https://www.google.com/search?q=fnp90&rlz=1C1CH...	2018-03-28 08:01:11 WIB	https://www.google.com/search?q=fnp90&rlz=1C1CH...	fnp90 - Go...
History			3	https://www.google.com/search?q=foldable+kel+tec&...	2018-03-31 11:43:13 WIB	https://www.google.com/search?q=foldable+kel+tec&...	foldable k...
History			3	https://www.google.com/search?q=foxnews&rlz=1C1C...	2018-04-03 13:02:02 WIB	https://www.google.com/search?q=foxnews&rlz=1C1C...	foxnews -
History			3	https://www.google.com/search?q=get+onedrive+to+...	2018-04-05 08:59:43 WIB	https://www.google.com/search?q=get+onedrive+to+...	get onedri...
History			3	https://www.google.com/search?q=niaccinio+iurassic+...	2018-04-05 15:25:00 WIB	https://www.google.com/search?q=niaccinio+iurassic+...	niaccinio i...

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

Result: 157 of 2534 Result ← →

Web History

Visit Details

Title: fnp90 - Google Search
 Username: Default
 Date Accessed: 2018-03-28 08:01:11 WIB
 Domain: google.com
 URL: https://www.google.com/search?q=fnp90&rlz=1C1CHBF_enUS790US790&oq=fnp90&aqs=chrome..69i57j0l5.3301j0j7&sourceid=chrome&ie=UTF-8
 Referrer URL: https://www.google.com/search?q=fnp90&rlz=1C1CHBF_enUS790US790&oq=fnp90&aqs=chrome..69i57j0l5.3301j0j7&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

Web History 2402 Results

Table Thumbnail Summary Save Table as CSV

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History			3	https://www.google.com/search?q=gun+control+great..	2018-04-05 12:41:14 WIB	https://www.google.com/search?q=gun+control+great.. gun contr	
History			3	https://www.google.com/search?q=gun+control+great..	2018-04-05 12:41:17 WIB	https://www.google.com/search?q=gun+control+great.. gun contr	
History			3	https://www.google.com/search?q=gun+control+in+in..	2018-04-05 12:51:54 WIB	https://www.google.com/search?q=gun+control+in+in.. gun contro	
History			3	https://www.google.com/search?q=gunbroker&rlz=1C...	2018-03-31 11:44:13 WIB	https://www.google.com/search?q=gunbroker&rlz=1C... gunbroker	
History		History	3	https://www.google.com/search?q=gunstore+near+me..	2018-04-01 00:48:18 WIB	https://www.google.com/search?q=gunstore+near+me.. gunstore n	
History			3	https://www.google.com/search?q=hotels+in+bali&rlz..	2018-04-03 13:04:29 WIB	https://www.google.com/search?q=hotels+in+bali&rlz.. hotels in b	
History			3	https://www.google.com/search?q=how+come+when...	2018-04-01 04:49:45 WIB	https://www.google.com/search?q=how+come+when... how come	
History			3	https://www.google.com/search?q=how+do+i+set+go..	2018-04-05 08:51:32 WIB	https://www.google.com/search?q=how+do+i+set+go.. how do i s	
History			3	https://www.nooble.com/search?n=how+far+would+...	2018-04-01 02:48:03 WIB	https://www.nooble.com/search?n=how+far+would+... how far wi	

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

Result: 1742 of 2534 Result ← → Web History

Visit Details

Title: gun control in indonesia - Google Search
 Username: Default
 Date Accessed: 2018-04-05 12:51:54 WIB
 Domain: google.com
 URL: https://www.google.com/search?q=gun+control+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=gun+control+in+indonesia&aqs=chrome..69i57.4917j0j7&sourceid=chrome&ie
 Referrer URL: https://www.google.com/search?q=gun+control+in+indonesia&rlz=1C1CHBF_enUS790US790&oq=gun+control+in+indonesia&aqs=chrome..69i57.4917j0j7&sourceid=chrome&ie
 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

EXAMINATION

TOOLS

- AUTOSPY
- HashMyFiles

IMAGING

LoneWolf.E01	05/02/2021 15:40	E01 File	1.535.844 ...
LoneWolf.E02	05/02/2021 15:34	E02 File	1.535.849 ...
LoneWolf.E03	05/02/2021 15:24	E03 File	1.535.889 ...
LoneWolf.E04	05/02/2021 15:32	E04 File	1.535.901 ...
LoneWolf.E05	05/02/2021 15:28	E05 File	1.535.819 ...
LoneWolf.E06	05/02/2021 15:55	E06 File	1.535.940 ...
LoneWolf.E07	05/02/2021 15:57	E07 File	1.535.908 ...
LoneWolf.E08	05/02/2021 15:58	E08 File	1.535.863 ...
LoneWolf.E09	05/02/2021 15:57	E09 File	941.019 KB

HASHING

HashMyFiles			
HashMyFiles File Edit View Options Help			
Add Files		MD5	SHA1
LoneWolf.E01		b1fbb5a40ce1fd4a1ac8663117ea5ac0	88c6d994a14c053c456f272e25051f92e8736d...
LoneWolf.E02		c11769a15d69379aa84e69f6006d5c87	f7c8c742b5012abdd4ae1dd97ae7db5c18fd4...
LoneWolf.E03		312fd2876c454ece1744b9303e35f4b0	dde1e067af98a1e4b8c294c1042f034b9391e5...
LoneWolf.E04		1669162c8bae6414d1412bc7f122b532	2770c68dad294119f8843b88170eaf56de0351...
LoneWolf.E05		148908037b3b05a21745c2777d1d3df4	aa26d655b832bd8a8cf61adeccea227c157c...
LoneWolf.E06		49e5b354f938568ac25acd088f1f76af	be538b686711d6f31d3b9fb605b5a85067db...
LoneWolf.E07		48fa361db68328405d70c510e590069d	22ff8463cc1b887ff66207bbc7daafc9ad689323
LoneWolf.E08		fe4ca92e5b90e07179b68b282da97d20	844aeaba7d66baa0d555c1bc46184c2277bbd...
LoneWolf.E09		3c2494c42d9816c0789cc3c0861f1d1a	c1e8c0bf16b96b003e88925f0a07faf12986ade4

ANALYSIS

- **Bukti pertama**

Telah ditemukan adanya Identitas asli dari tersangka yang dikenal dengan nama "lenowolf" atau "jcloudy" terungkap melalui email yang terdaftar pada akun jimcloudy1@gmail.com dan jimcloudy@outlook.com di platform Outlook. Selain itu, ditemukan juga percakapan dalam chat dengan saudara laki-lakinya yang memanggilnya dengan nama "Jim". Hal ini diperkuat oleh nama pengguna Windows yang terdaftar sebagai jcloudy, yang tampaknya merupakan singkatan dari nama asli, Jim Cloudy.

- **Bukti Kedua**

Telah ditemukan bukti berupa file berjudul "The Cloudy Manifesto" di dalam sistem komputer tersangka, yang menunjukkan penolakan Jim terhadap

pembatasan senjata. Dalam file ini, Jim mengungkapkan keyakinannya bahwa melucuti senjata warga hanya akan membuat masyarakat lebih rentan terhadap ancaman, baik dari penjahat, pemerintah, maupun pihak asing. Jim berpendapat bahwa kepemilikan senjata adalah hak dasar setiap individu untuk melindungi diri dan kebebasan mereka. Selain itu, dalam file tersebut, Jim menyatakan niatnya untuk melanggar hukum dan melakukan pembunuhan massal, dengan tujuan untuk menjadi orang pertama yang menyerukan pembebasan senjata.

Pendapat Jim didukung oleh tiga file lain yang saya temukan, yaitu Amen.pdf, SelfDefenseisMurder.pdf, dan LeftUsesBoycotts.pdf:

- Amen.pdf menekankan bahwa meskipun senjata tidak dapat mengalahkan teknologi militer canggih, kepemilikan senjata penting untuk melawan tirani pemerintah dan mempertahankan kebebasan.
- SelfDefenseisMurder.pdf menunjukkan bahwa pembelaan diri dengan senjata tajam adalah hak yang sah untuk melindungi diri dari ancaman kriminal.
- LeftUsesBoycotts.pdf mengungkapkan bagaimana kelompok kiri menggunakan tekanan sosial dan ekonomi untuk mengubah kebijakan terkait hak kepemilikan senjata.
- Sebagai kontra terhadap argumen Jim, terdapat file yang dihapus, seperti [Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'](#) dan [Larry King: Time to Repeal the 'Poorly Written' Second Amendment](#), yang mendukung pembatasan senjata untuk mengurangi ancaman kekerasan. Ditambah dengan UkknifeBan.pdf, yang mengusulkan pelarangan pisau dapur berujung runcing untuk mengurangi penusukan fatal.

Bukti ini menunjukkan pandangan berbeda terkait pembatasan senjata. Jim menentang pembatasan karena ia percaya bahwa hak kepemilikan senjata adalah hak dasar untuk melindungi diri dan kebebasan. Ia melihat senjata sebagai sarana untuk mempertahankan kebebasan dan melawan tirani, serta menyatakan bahwa melucuti senjata akan membuat masyarakat lebih rentan terhadap ancaman.

- **Bukti Ketiga**

Telah ditemukan bukti berupa file "planning.docx" di dalam sistem komputer tersangka, yang menunjukkan bahwa Jim merencanakan serangan tersebut secara rinci. Dalam dokumen tersebut, Jim menetapkan bahwa lokasi target harus memiliki rute pelarian yang baik, dekat dengan bandara, dan berada di zona bebas senjata. Perlengkapan yang akan dibawa juga dijelaskan secara terperinci, termasuk senjata yang dibeli dari pasar gelap melalui dua alamat di Virginia

(Norther VA Gun Works 7518 Fullerton Rd K, Springfield, VA 22153 dan NOVA 412 W Broad Street Falls Church, VA 22046), beserta amunisinya (1000 ammo i9mm dan Kel-Tec Sub 2000 9mm). Selain itu, Jim juga berencana untuk membawa sejumlah uang tunai, Velcro, dan sarung tangan lateks. Setelah selesai melaksanakan aksi, Cloudy berencana untuk melarikan diri ke Indonesia atau Vietnam pada hari yang sama dengan tiket penerbangan.

- **Bukti Ke Empat**

Telah ditemukan bukti berupa file "AIRPORT INFORMATION.docx" di dalam sistem komputer tersangka, yang berisi informasi terkait bandara. Dalam file tersebut, tercatat bahwa "Ronald Reagan Airport" dikenal memiliki catatan terbaik untuk keberangkatan tepat waktu, sementara "Dulles Airport" menyediakan penerbangan ke Indonesia. Selain itu, file ini juga mencantumkan jarak tempuh dari "Fairfax County Democratic Committee" yang berlokasi di 8500 Executive Park Ave, Fairfax, VA 22031, ke "Dulles Airport", yang hanya memerlukan waktu sekitar 22 menit. Data ini tampaknya digunakan sebagai bagian dari perencanaan perjalanan atau rute pelarian.

- **Bukti Ke Lima**

Telah ditemukan bukti berupa file "Operation 2nd Hand Smoke.pptx" di dalam sistem komputer tersangka. Dalam file presentasi tersebut, terdapat beberapa bukti gambar penting yang mengindikasikan adanya perencanaan pembunuhan, termasuk informasi tentang acara yang menjadi target, lokasi dan waktu acara, rute pelarian setelah aksi, rute menuju bandara, maskapai yang akan digunakan, serta hotel tempat pelaku akan menginap.

Berikut adalah detail yang ditemukan dalam file tersebut:

- Pada slide kedua, terdapat informasi tentang lokasi target di 21030 Whitfield Pl, Sterling, VA 20165, dengan waktu acara yang direncanakan pada Sabtu, 7 April 2018, dari pukul 12:30 hingga 14:00. Acara ini membahas isu-isu terkait kekerasan senjata, yang kemungkinan besar memicu ketidaksukaan tersangka Jim terhadap pembatasan kepemilikan senjata.
- Pada slide ketiga, terdapat gambar gedung target yang ditandai dengan lingkaran merah, dengan detail lokasi yang sama seperti pada slide kedua.
- Pada slide keempat, terdapat denah rute, mulai dari parkir menuju lokasi target yang ditandai dengan warna kuning, rute pelarian setelah aksi yang ditandai dengan warna merah, dan rute menuju bandara yang ditandai dengan warna hijau.

- Pada slide kelima, terdapat peta yang menunjukkan rute dari lokasi aksi menuju Bandara Dulles.
 - Pada slide keenam, terdapat informasi mengenai maskapai yang akan digunakan, yaitu Korea Air, dengan penerbangan dari Washington menuju Indonesia.
 - Pada slide ketujuh, terdapat gambar hotel tujuan pelaku yang terletak di Bali, Indonesia, yang akan digunakan setelah tiba di tujuan.
- **Bukti Ke Enam**

Telah ditemukan bukti berupa file “Cloudy thoughts (4apr).docx” di dalam sistem komputer tersangka. Dalam dokumen tersebut, tersangka Jim mengungkapkan perasaan gugup dan cemas terkait dengan rencana yang telah disiapkan. Ia khawatir tentang cuaca yang dapat mempengaruhi penerbangan yang direncanakan. Meskipun demikian, Jim bertekad untuk melaksanakan rencana tersebut meskipun menyadari adanya risiko yang terlibat.

Jim juga menyimpan berbagai informasi penting, seperti file “AIRPORT INFORMATION,” “Planning Operation 2nd Hand Smoke,” dan “The Cloudy Manifesto,” di beberapa layanan cloud (Bos Sync, OneDrive, GoogleDrive, dan DropBox). Hal ini dilakukan agar pemikirannya tetap dapat diakses, dengan harapan bahwa keluarganya akan mengerti tindakannya. Dalam dokumen ini, Jim juga menyebutkan nama Paul, yang menurutnya memiliki satu-satunya kunci yang diperlukan. Jim memandang tindakan yang direncanakan sebagai sebuah pengorbanan demi kebebasan.
 - **Bukti ke Tujuh**

Melalui artefak pencarian web yang ditemukan, dapat dipastikan bahwa rencana yang disiapkan oleh tersangka Jim Cloudy telah dipersiapkan dengan matang. Beberapa riwayat pencarian di peramban Google Chrome menunjukkan bahwa Jim mencari peta zona bebas senjata, informasi tentang Indonesia, serta ramalan cuaca untuk Washington dan Virginia. Pencarian cuaca ini menunjukkan perhatian Jim terhadap faktor yang dapat mempengaruhi keterlambatan penerbangan yang direncanakan. Selain itu, terdapat banyak pencarian terkait Virginia, yang mengindikasikan bahwa Jim Cloudy berdomisili di wilayah tersebut.
 - **Bukti Ke Delapan**

Melalui artefak pencarian web, ditemukan bahwa Jim melakukan pembelian senjata dan amunisi melalui situs “gunbroker.com”. Pembelian tersebut meliputi satu senjata FNP90 dan dua jenis amunisi, yaitu i9mm ammo 1000 dan FN 5.7 ammo.

- **Bukti Ke Sembilan**

Saya menemukan beberapa foto yang relevan terkait rencana yang telah dipersiapkan. Foto-foto ini menunjukkan senjata, tempat latihan menembak, dan logo toko senjata yang telah dihapus.

- File "f_0017c1", "f_0017c2", "f_0014920", dan "f_001786" berisi foto-foto senjata.
- File "f_00183d" menunjukkan foto tempat latihan menembak.
- File "f_0017c4" adalah logo toko senjata.

- **Bukti Ke Sepuluh**

ditemukan dua file berjudul Brother Chat.gdoc (Google Dokumen) dan Jim's Notebook (OneDrive). Namun, setelah mencoba mengakses kedua tautan dari dokumen tersebut, file-file tersebut sudah tidak tersedia. Selanjutnya, saya melakukan pencarian melalui Autopsy dengan menggunakan kata kunci "paul" dan "my notebook". Dari hasil pencarian tersebut, saya berhasil menemukan potongan percakapan dan catatan milik Jim yang tersimpan dalam file "000044.ldb" dan "00000003.bin".

- Percakapan dalam file "000044.ldb" menunjukkan ketegangan antara Jim dan Paul mengenai keamanan dalam melakukan riset terkait senjata dan kontrol senjata. Jim mengungkapkan kekhawatirannya tentang kemungkinan pengawasan oleh pihak berwenang. Paul memperingatkan bahwa orang-orang bisa menjadi target pengawasan hanya karena pencarian online, mengacu pada kasus keluarga yang mendapat kunjungan dari pihak berwenang setelah mencari informasi tentang barang-barang yang tidak mencurigakan.
- Catatan dalam file "00000003.bin" menunjukkan kecemasan dan keraguan Jim terkait keberhasilan rencananya. Namun, ia juga menyiratkan optimisme tentang "awal yang baru" di Bali, yang tampaknya merupakan tujuan akhirnya setelah melaksanakan rencananya.

KESIMPULAN

Kesimpulan Berdasarkan Hasil Analisis Forensik Digital

- What: Apa bukti yang ditemukan?
- Where: Di mana bukti ditemukan dalam sistem (misalnya, lokasi file atau log)?

Berdasarkan hasil analisis forensik digital terhadap komputer milik tersangka Jim Cloudy, ditemukan beberapa bukti berikut:

Filename	Lokasi
The Cloudy Manifesto	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/The Cloudy Manifesto
AIRPORT INFORMATION	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/AIRPORT INFORMATION.docx
AMEN	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/AMEN.pdf
Cloudy thoughts (4apr)	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Cloudy thoughts (4apr).docx
LeftUsesBoycotts	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/LeftUses Boycotts.pdf
Operation 2nd Hand Smoke	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx
Planning	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Planning.docx
SelfDefenseisMurder	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/SelfDefenseisMurder.pdf
UKknifeBan	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/SelfDefenseisMurder.pdf
00000003.bin	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Packages/Microsoft.Office.OneNote_8wekyb3d8bbwe/LocalState/AppData/Local/OneNote/16.0/cache/00000003.bin

000044.ldb	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/IndexedDB/https_docs.google.com_0.indexeddb.logedb/000044.ldb
Brother Chat.gdoc	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Google Drive/Brother Chat.gdoc
Cubs' Anthony Rizzo Praised Parkland Kids, Says 'It's too Easy to Get a Gun'	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Cubs' Anthony Rizzo Praised Parkland Kids, Says 'It's too Easy to Get a Gun'.html
Jim's Notebook	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/OneDrive/Documents/Jim's Notebook.url
Larry King_ Time to Repeal the 'Poorly Written' Second Amendment	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Larry King_ Time to Repeal the 'Poorly Written' Second Amendment.html
f_0017c1	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c1
f_0017c2	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c2
f_00183d	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_00183d
f_001786	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001786

f0014920	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001786
f_0017c4	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c4
situs "gunbroker.com"	www.gunbroker.com

- Who: Siapa yang terlibat dalam aktivitas berdasarkan bukti?
 - Berdasarkan analisa di atas, terdapat dua orang yang terlibat, yaitu Jim Cloudy sebagai tersangka utama dan Paul yang menjadi opsional untuk pemeriksaan. Hal ini didasarkan pada penyebutan nama Paul dalam file "Cloudy Thoughts (4apr).docx" dan percakapan antara Paul dan Jim yang ditemukan dalam file "000044 ldb".
- When: Kapan aktivitas tersebut terjadi?
 - Berdasarkan file "Operation 2nd Hand Smoke.pptx" Jim melakukan aktifitas tersebut pada **(Sat, April 7, 2018 12:30 to 2:00 PM)** berlokasi di **(21030 Whitfield Pl Sterling VA, 20165)**.
- Why: Mengapa bukti ini relevan terhadap dugaan perencanaan pembunuhan?

Bukti ini relevan karena mengungkapkan beberapa fakta penting:

1. **Identitas dan Motivasi:**
 - File *The Cloudy Manifesto* mengungkap pandangan ideologis Jim yang menentang pembatasan senjata dan tujuan untuk menjadi orang pertama yang menyerukan pembebasan senjata walaupun melanggar hukum.
2. **Rencana Pembunuhan Terperinci:**
 - File *planning.docx* dan *Operation 2nd Hand Smoke.pptx* merinci lokasi target, persiapan senjata, rute pelarian, dan jadwal aksi.
3. **Persiapan Senjata:**
 - Bukti pembelian senjata **FN P90** dan amunisi melalui situs *gunbroker.com* menunjukkan kesiapan fisik Jim untuk melakukan aksi kekerasan.
4. **Rencana Pelarian:**
 - File *AIRPORT INFORMATION.docx* menunjukkan persiapan rute penerbangan dari Washington menuju Indonesia atau Vietnam, yang menegaskan niat melarikan diri setelah melakukan aksi.

5. Keterlibatan Paul:

- Percakapan dalam file *000044.Idb* menunjukkan Paul sebagai pihak yang mungkin mengetahui atau berhubungan dengan rencana ini.
- How: Bagaimana bukti ini menunjukkan keterkaitan dengan perencanaan pembunuhan?

Bukti menunjukkan keterkaitan melalui langkah-langkah sistematis berikut:

1. **Pandangan Ideologis** : Motivasi tindakan kekerasan berdasarkan file manifesto.
2. **Rencana Aksi** : Dokumen *planning.docx* dan *Operation 2nd Hand Smoke.pptx* memberikan rincian aksi serangan.
3. **Persiapan Senjata** Pembelian FN P90 dan amunisi.
4. **Rencana Pelarian** : File bandara dan rute pelarian menunjukkan persiapan pasca-serangan.
5. **Komunikasi** : Bukti keterlibatan pihak lain (Paul) yang membantu atau mengetahui rencana tersebut.

Kesimpulan Akhir

Berdasarkan analisis forensik digital terhadap komputer milik tersangka Jim Cloudy, ditemukan sejumlah bukti yang menguatkan dugaan perencanaan pembunuhan, termasuk dokumen manifesto yang berisi pandangan ideologisnya terkait penolakan terhadap pembatasan senjata, serta rencana terperinci dalam file "Planning.docx" dan "Operation 2nd Hand Smoke.pptx" yang mencakup lokasi target, persiapan senjata, dan rute pelarian menuju bandara. Bukti tambahan seperti file "AIRPORT INFORMATION.docx" menunjukkan rencana pelarian ke luar negeri, sementara jejak aktivitas di situs "gunbroker.com" mengonfirmasi pembelian senjata dan amunisi yang mendukung eksekusi serangan. Percakapan dalam file "000044.Idb" dan menyebutkan nama Paul dalam "Cloudy Thoughts (4apr).docx" mengindikasikan adanya keterlibatan pihak lain. Secara keseluruhan, bukti-bukti tersebut menunjukkan bahwa Jim Cloudy telah mempersiapkan serangkaian langkah yang matang, dari perencanaan hingga pelarian, dengan motivasi ideologis untuk melakukan aksi kekerasan yang mengakibatkan hilangnya nyawa.

REKOMENDASI (OPTIONAL)

Berdasarkan kesimpulan Pemeriksaan Forensik Digital maka dapat direkomendasikan, sebagai berikut:

1. Pemeriksaan Lanjutan terhadap Paul

Perlu dilakukan pemeriksaan lebih mendalam terhadap individu bernama Paul yang disebut dalam file "Cloudy Thoughts (4apr).docx" dan percakapan dalam file "000044.Idb" untuk mengetahui sejauh mana keterlibatannya dalam perencanaan tindakan tersebut.

PENGESAHAN

Mengetahui ATASAN (Optional)

KETUA TIM/PEMERIKSA

LAMPIRAN

Berikut Link folder yang berisi bukti-bukti :

<https://drive.google.com/drive/folders/1F7WHfgSCKagN9VTfqej-SvSj04rd-WV2?usp=sharing>

Source Name	S	C	O	URL	Date Accessed	Referrer URL	Title
History	0			https://weather.com/	2018-04-06 15:25:20 WIB	https://weather.com/	National and Local
History	3			https://www.google.com/search?q=best+new+phone&...	2018-03-30 06:03:48 WIB	https://www.google.com/search?q=best+new+phone&...	best new phone - G...
History	3			https://www.google.com/search?rlz=1C1CHBF_enUS79_...	2018-03-30 06:04:06 WIB	https://www.google.com/search?rlz=1C1CHBF_enUS79_...	new nokia - Google
History	3			https://www.google.com/search?rlz=1C1CHBF_enUS79_...	2018-03-30 06:04:14 WIB	https://www.google.com/search?rlz=1C1CHBF_enUS79_...	new nokia dual sim
History	0			https://www.nokia.com/en_int/phones/nokia-216-dual...	2018-03-30 06:04:27 WIB	https://www.nokia.com/en_int/phones/nokia-216-dual...	Nokia 216 Dual SIM
History	0			https://www.gunbroker.com/All/search?Sort=-5&Page5...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Sort=-5&Page5...	In 5 7 ammo For Sal...
History	0			https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn...	In 5 7 ammo For Sal...
History	0			https://www.gunbroker.com/All/search?fn...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?fn...	In 5 7 ammo For Sal...
History	0			https://www.gunbroker.com/All/search?Keywords=fn...	2018-03-30 06:05:21 WIB	https://www.gunbroker.com/All/search?Keywords=fn...	In 5 7 ammo For Sal...

Table [Thumbnail](#) [Summary](#)

[Save Table as CSV](#)

Source Name	S	C	O	△ URL	Date Accessed	Referrer URL	Title
History			3	https://www.google.com/search?q=cloud+storage+sol...	2018-03-28 06:42:35 WIB	https://www.google.com/search?q=cloud+storage+sol...	cloud stor...
History			3	https://www.google.com/search?q=concealable+tactic...	2018-03-31 11:36:31 WIB	https://www.google.com/search?q=concealable+tactic...	concealab...
History			3	https://www.google.com/search?q=concealable+tactic...	2018-03-31 11:37:14 WIB	https://www.google.com/search?q=concealable+tactic...	concealab...
History			3	https://www.google.com/search?q=concealable+tactic...	2018-03-31 11:36:57 WIB	https://www.google.com/search?q=concealable+tactic...	concealab...
History		History	3	https://www.google.com/search?q=do+indonesian+ba...	2018-04-05 12:58:57 WIB	https://www.google.com/search?q=do+indonesian+ba...	do indone...
History			3	https://www.google.com/search?q=do+the+cops+trac...	2018-04-01 03:03:23 WIB	https://www.google.com/search?q=do+the+cops+trac...	do the cop...
History			3	https://www.google.com/search?q=do+the+cops+trac...	2018-04-01 03:03:23 WIB	https://www.google.com/search?q=do+the+cops+trac...	do the cop...
History			3	https://www.google.com/search?q=doh+hamad+intern...	2018-04-01 02:57:09 WIB	https://www.google.com/search?q=doh+hamad+intern...	doh hama...
History			3	https://www.google.com/search?q=dronbox&rlz=1C1...	2018-04-02 08:40:05 WIB	https://www.google.com/search?q=dronbox&rlz=1C1...	dronbox -

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

Result: 585 of 2534 Result [◀](#) [▶](#)

Web History

Visit Details

Title: concealable tactical rifles - Google Search
 Username: Default
 Date Accessed: 2018-03-31 11:36:31 WIB
 Domain: google.com
 URL: https://www.google.com/search?q=concealable+tactical+rifles&rlz=1C1CHBF_enUS790US790&oq=concealable+tactical+rifles&aqs=chrome..69i57j0l4.5853j0j7&sourceid=chrc
 Referrer URL: https://www.google.com/search?q=concealable+tactical+rifles&rlz=1C1CHBF_enUS790US790&oq=concealable+tactical+rifles&aqs=chrome..69i57j0l4.5853j0j7&sourceid=chrc
 Program Name: Google Chrome

Source

Host: LoneWolf.E01_1 Host
 Data Source: LoneWolf.E01
 File: /img/LoneWolf_E01/vol1/vol17/1User/Cloud/AppData/Local/Google/Chrome/User Data/Default/History