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 lonewolf 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:

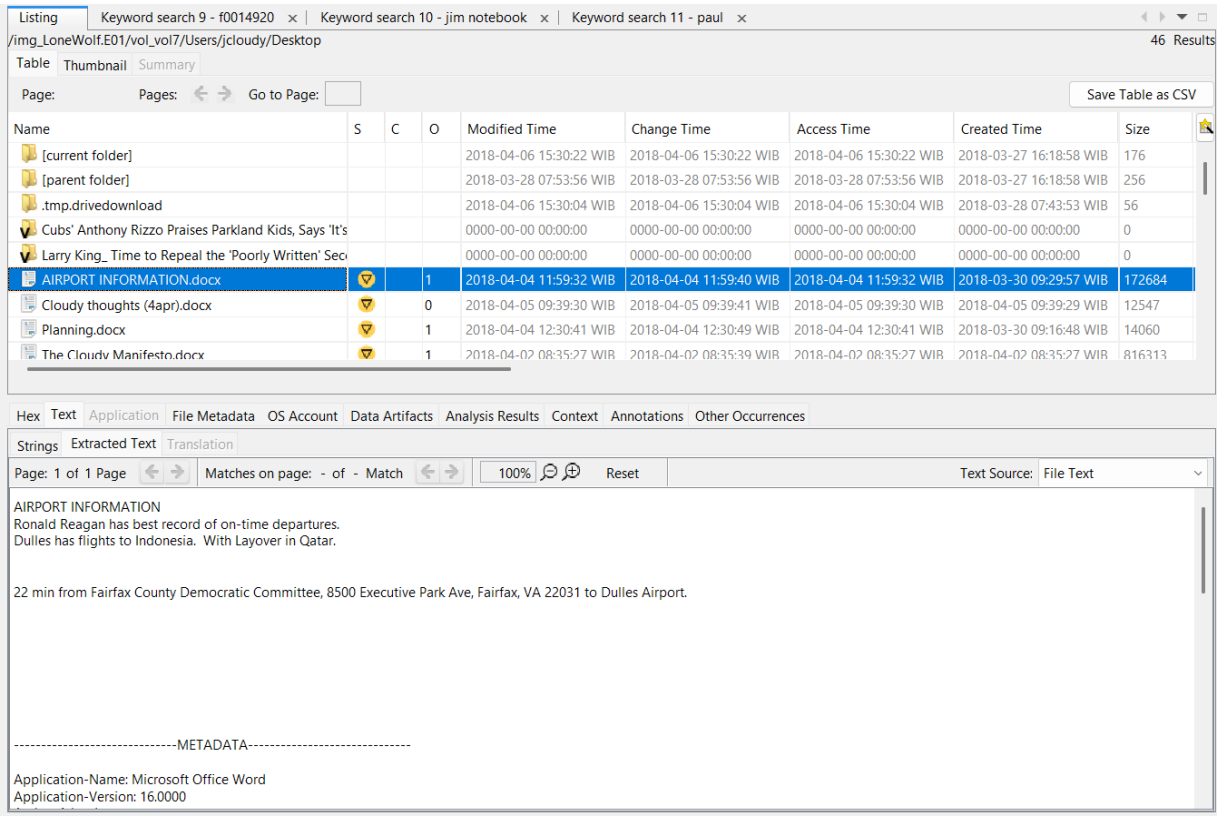
- NIJ: Electronic Crime Scene Investigation: A Guidee for First Responders [2002]
- NIST: Guide to Integrating Forensic Techniques into Incident Response [2006]
- ACPO: Good Practice Guide for Computer Based Evidence [2007].

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

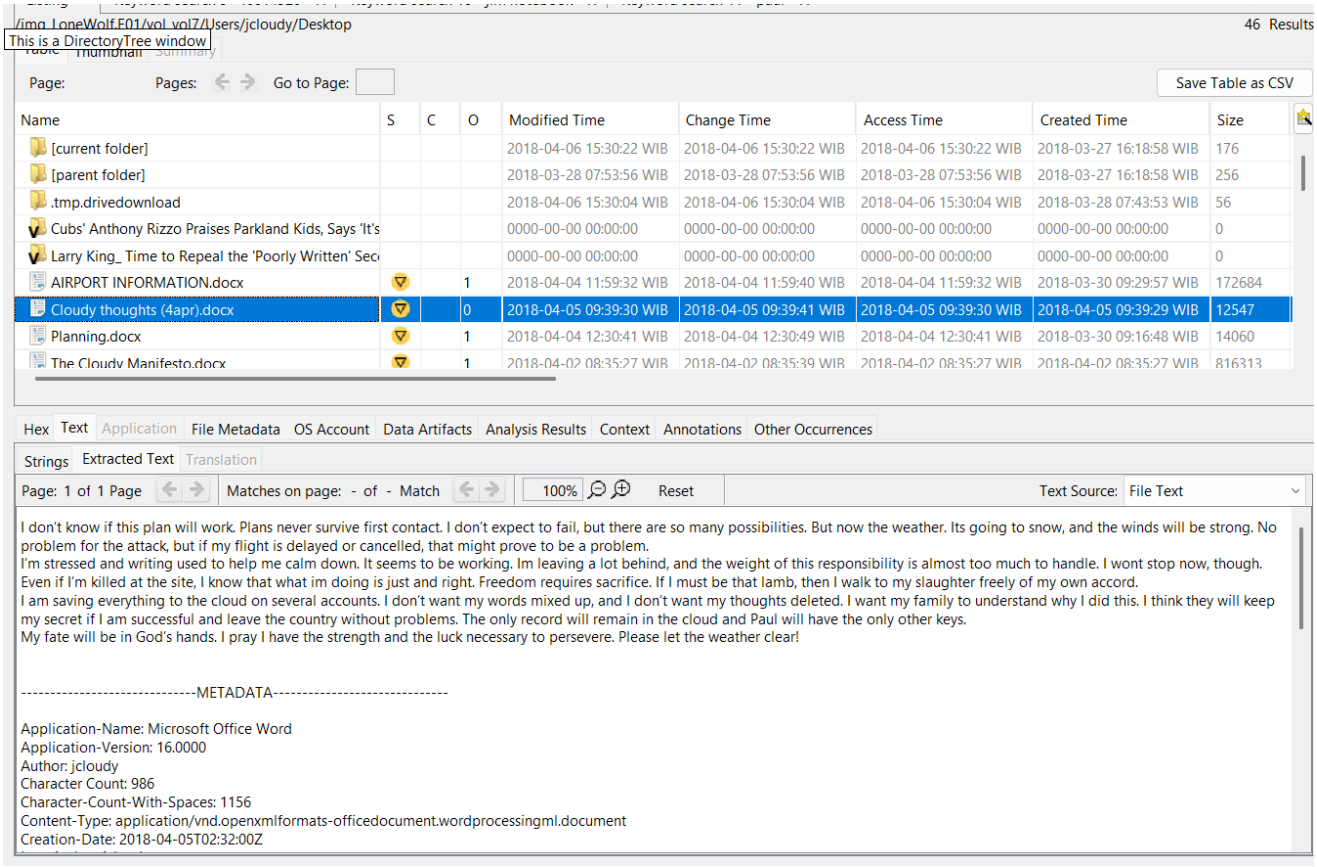
COLLECTION

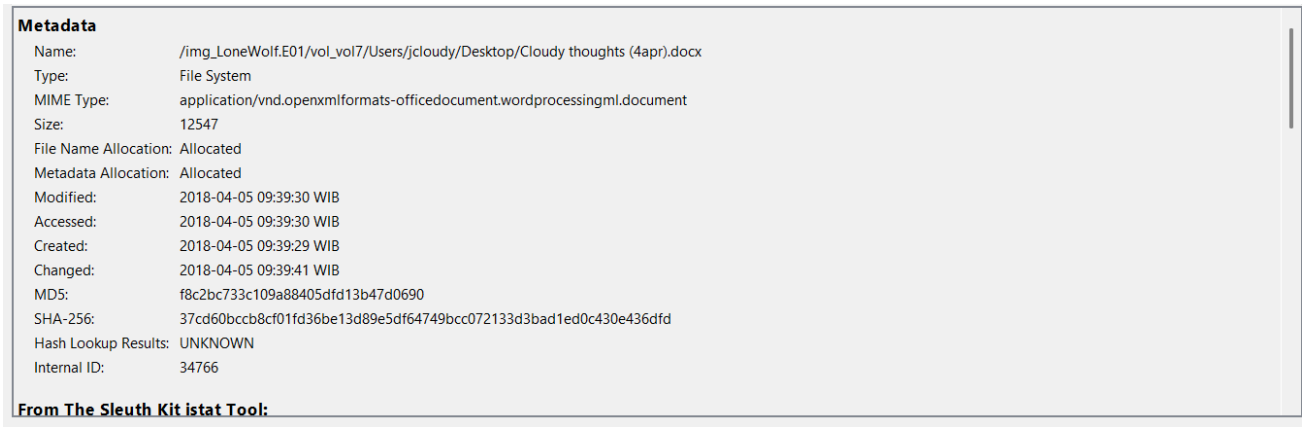
DATA INVESTIGASI

- AIRPORT INFORMATION

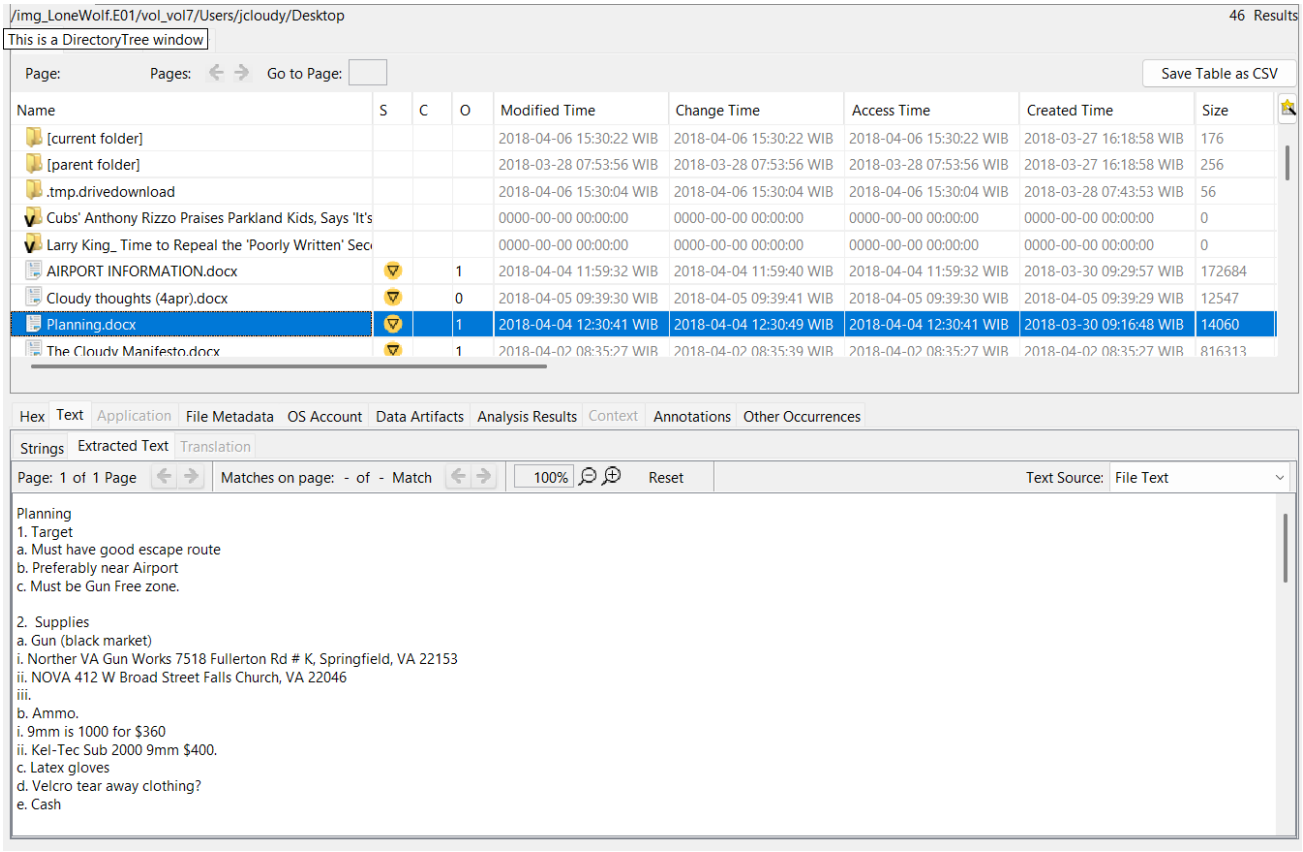


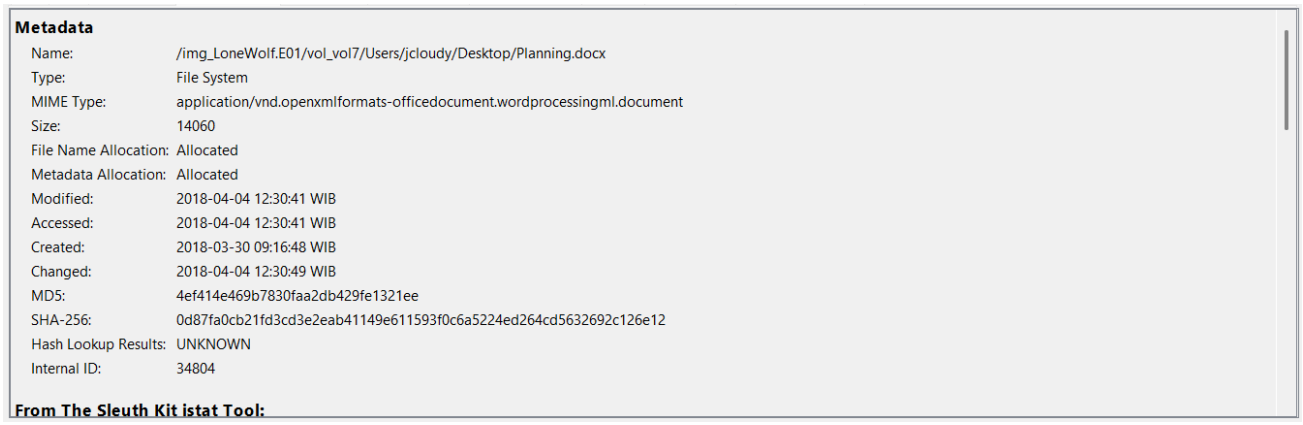
- Cloudy thoughts (4apr)



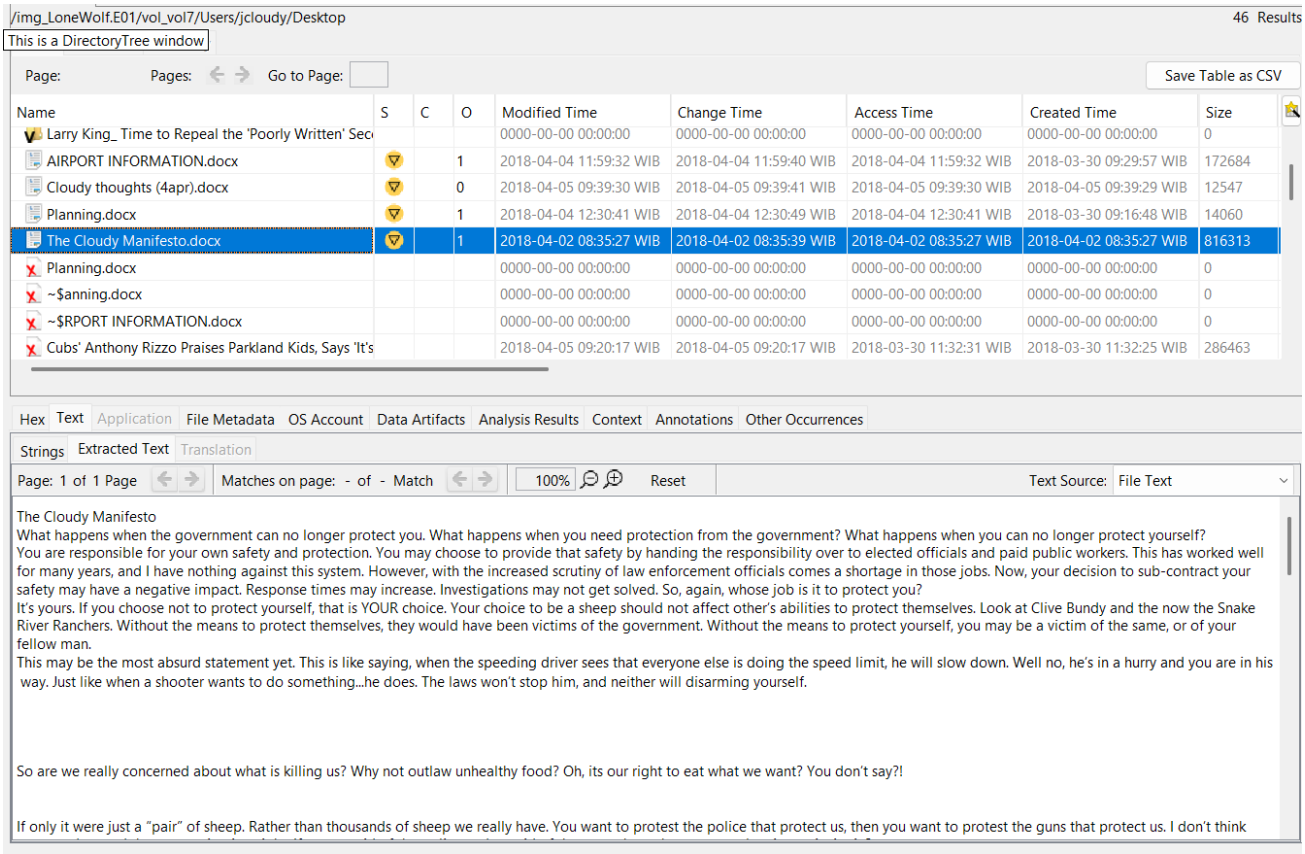


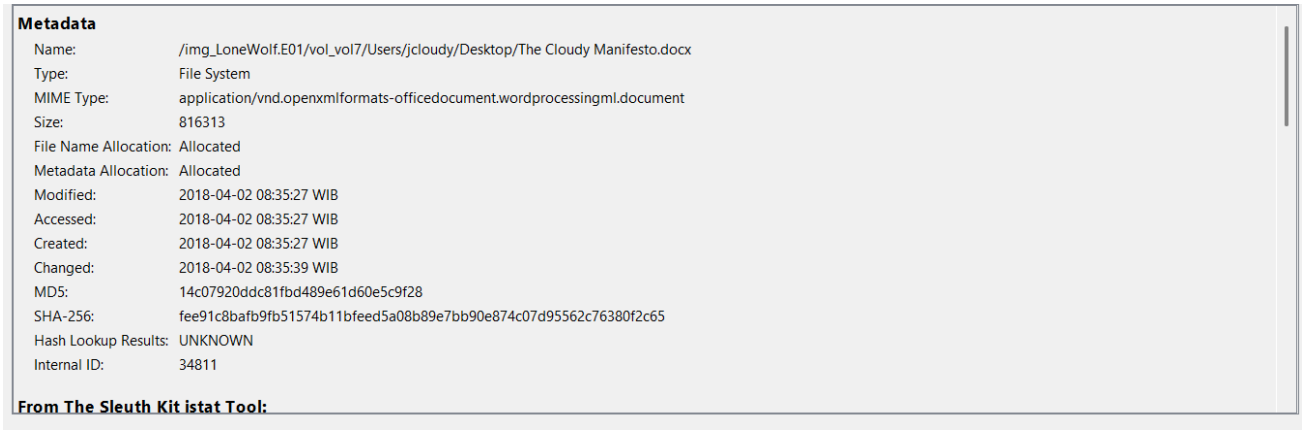
- Planning



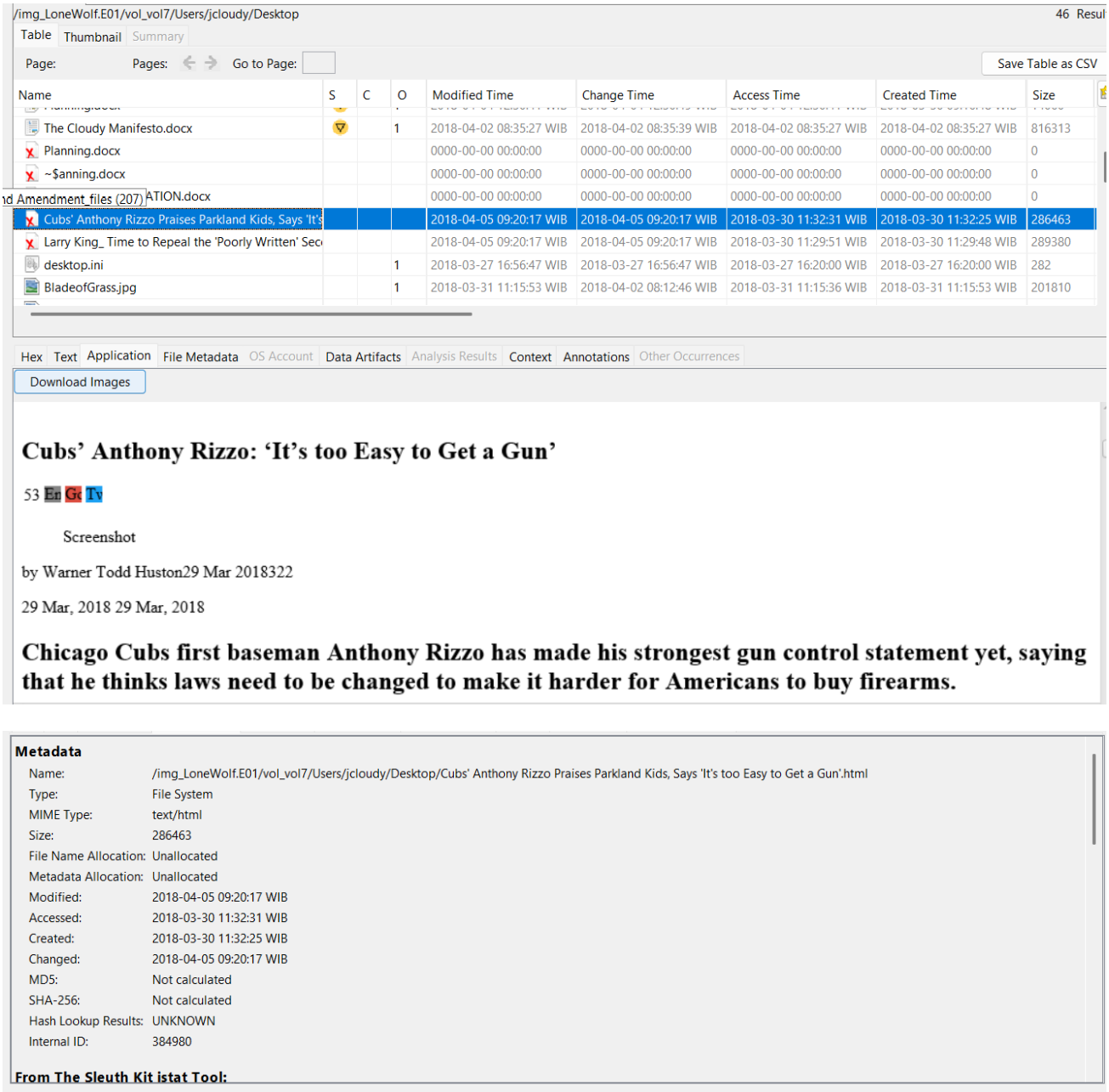


- The Cloudy Manifesto

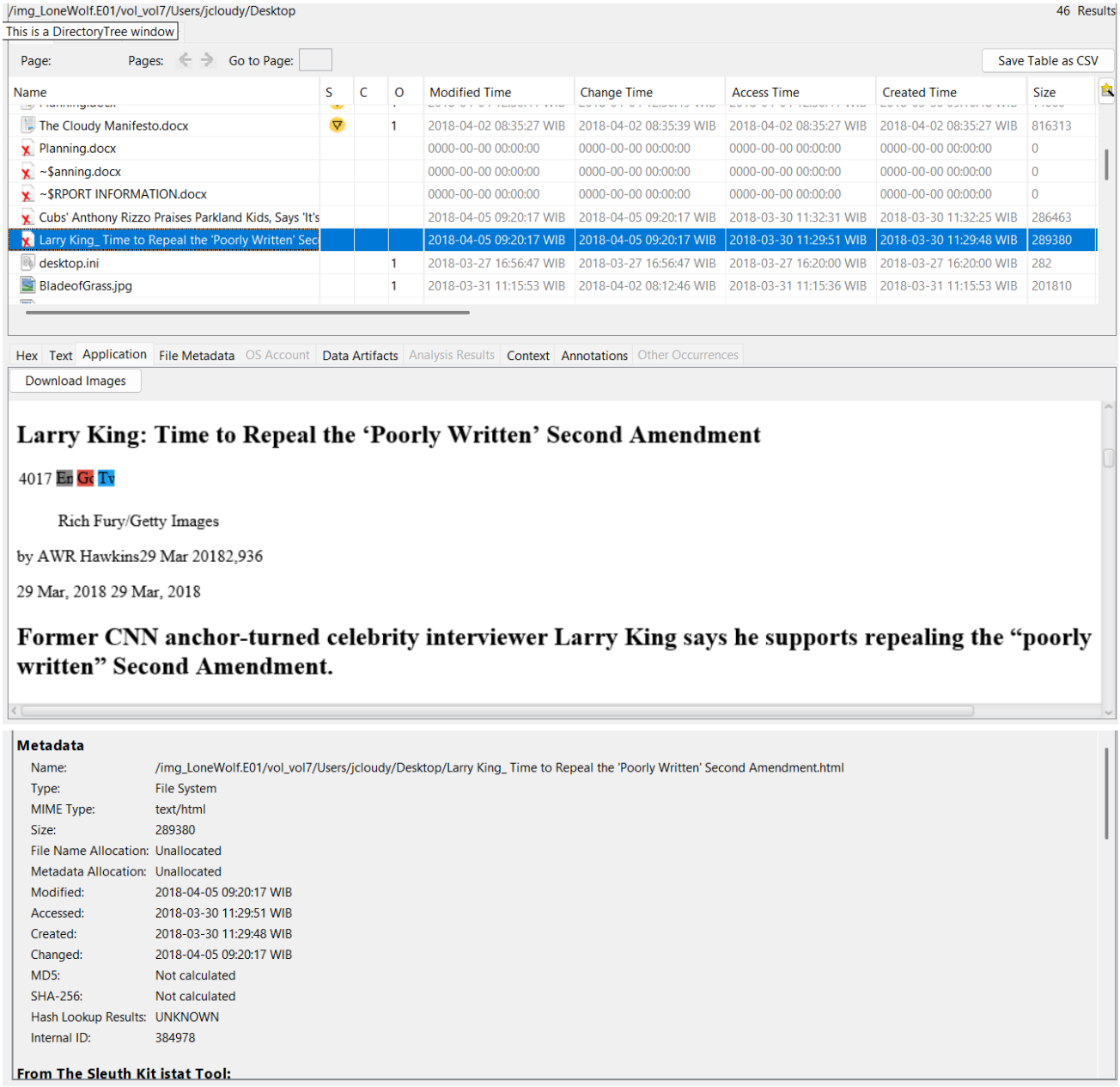




- Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'

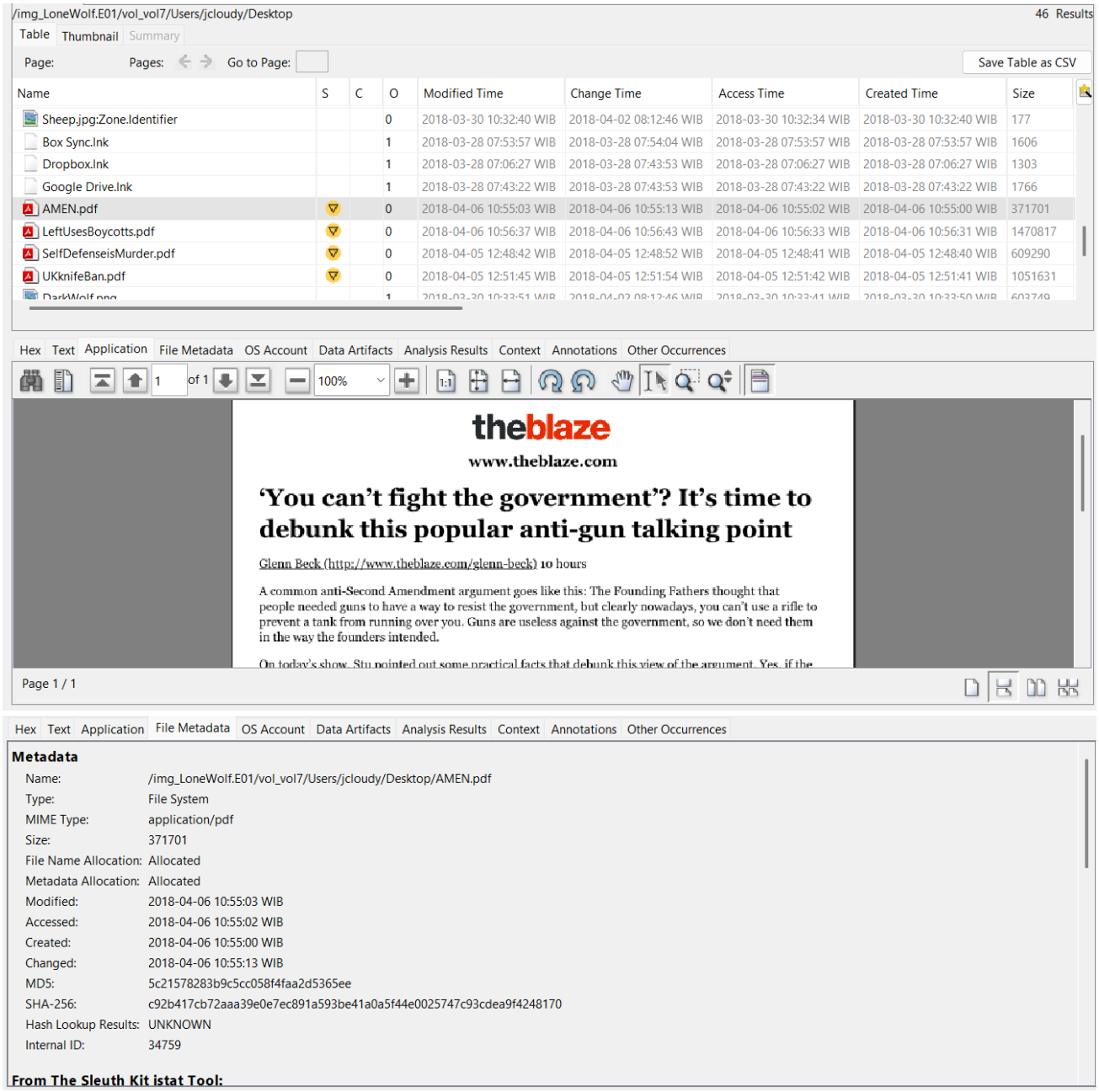


- Larry King_ Time to Repeal the 'Poorly Written' Second Amendment

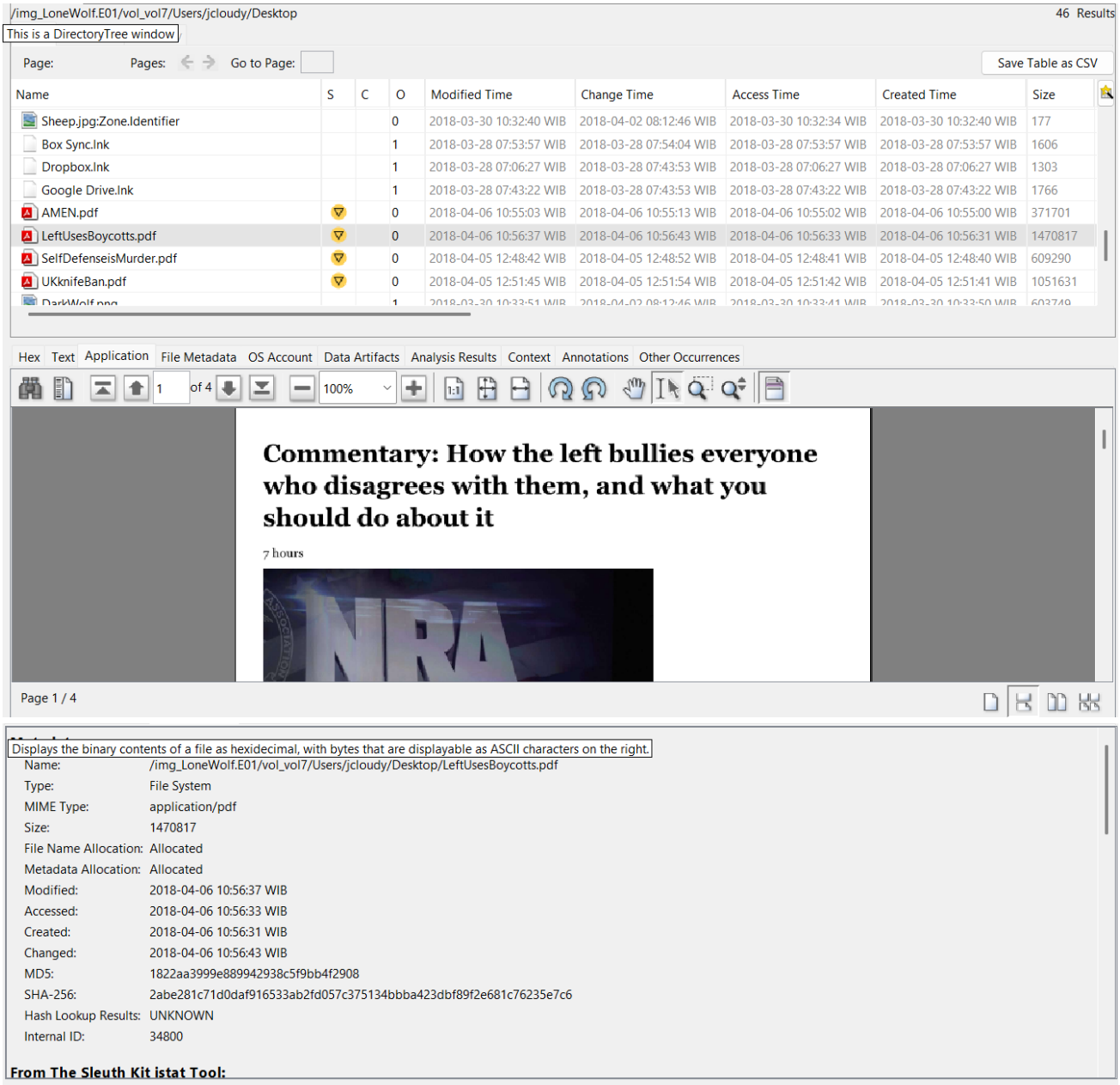


- AMEN

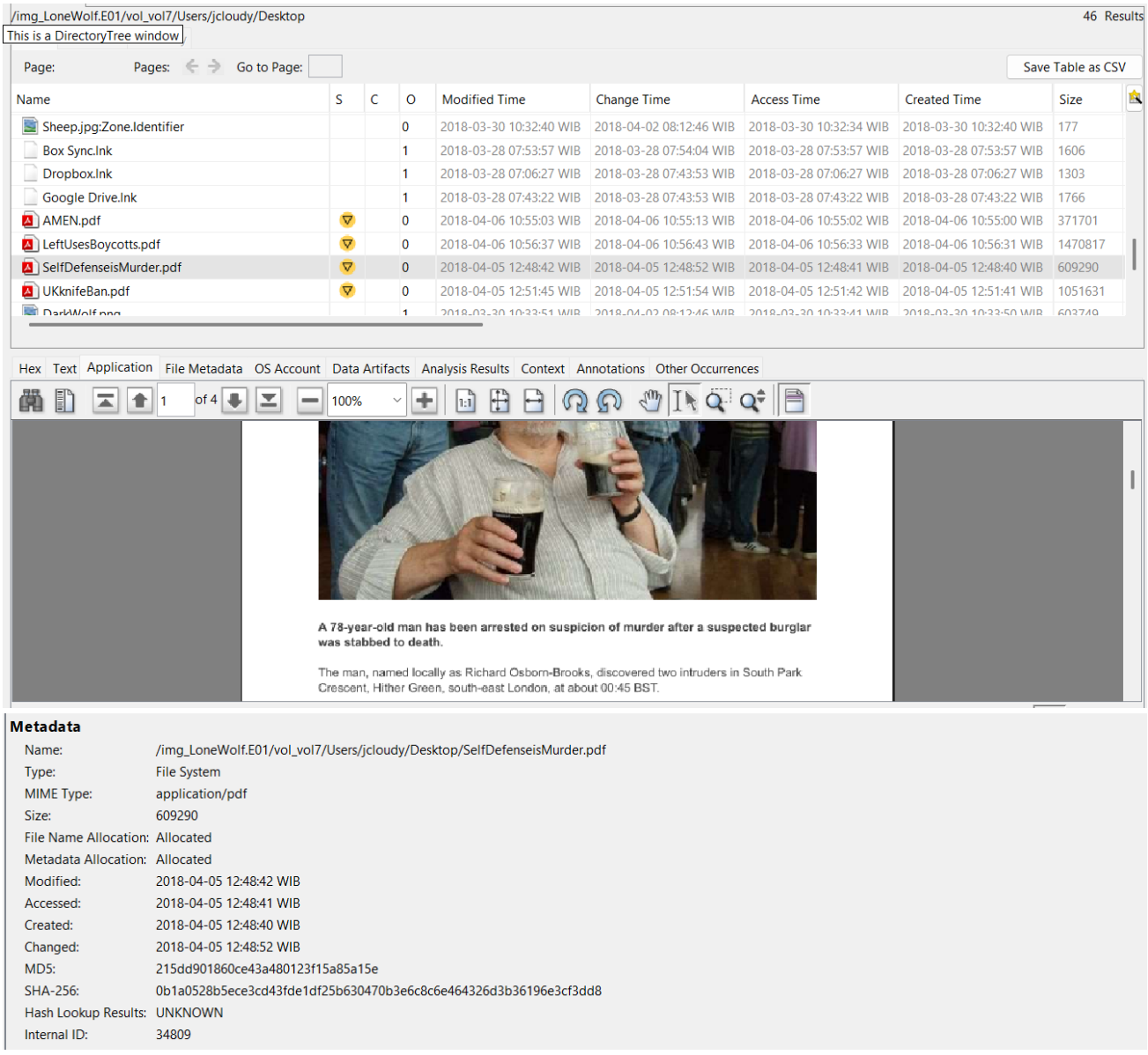
09 DECEMBER 2024 DIGITAL FORENSIC



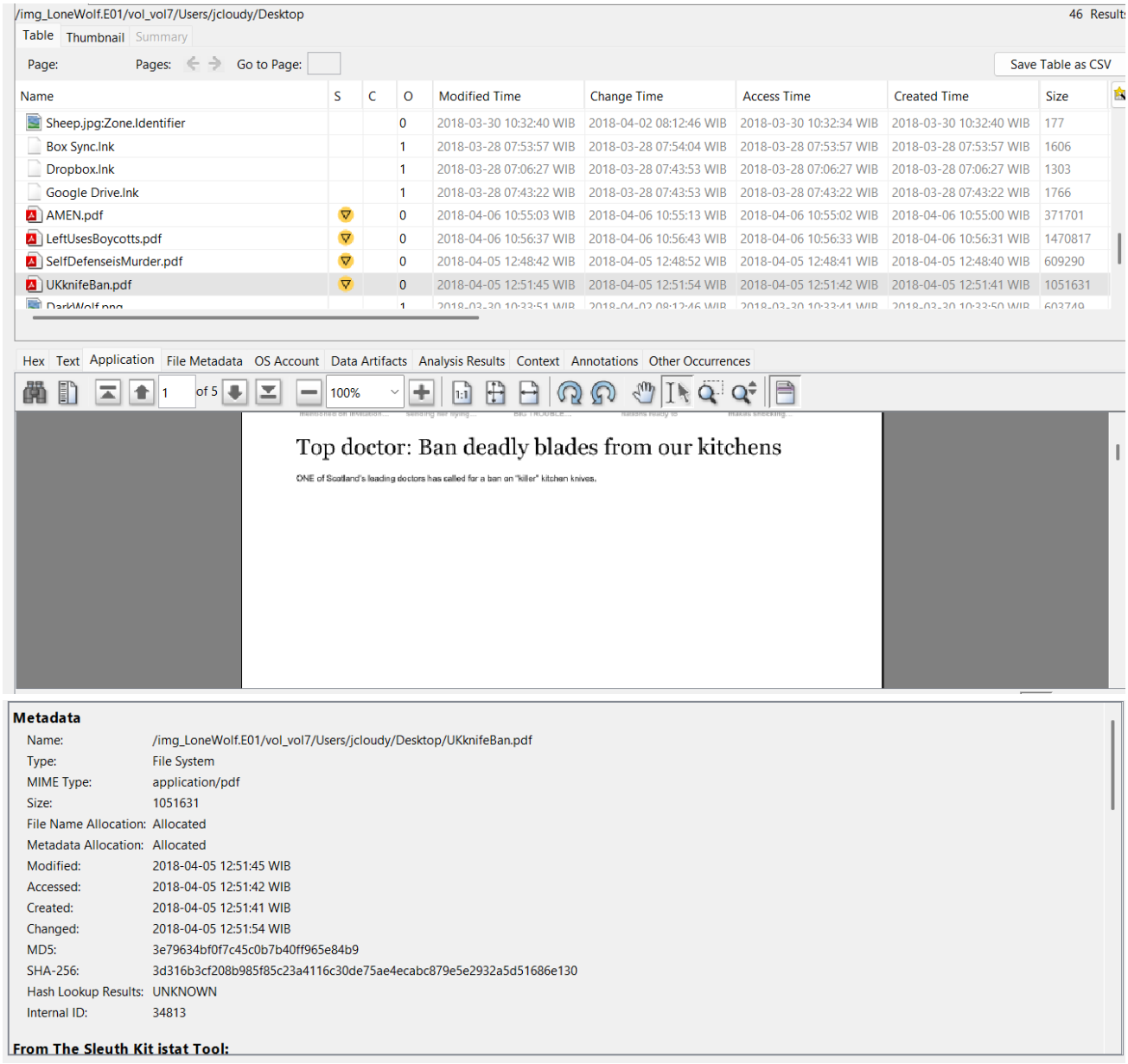
- LeftUsesBoycotts



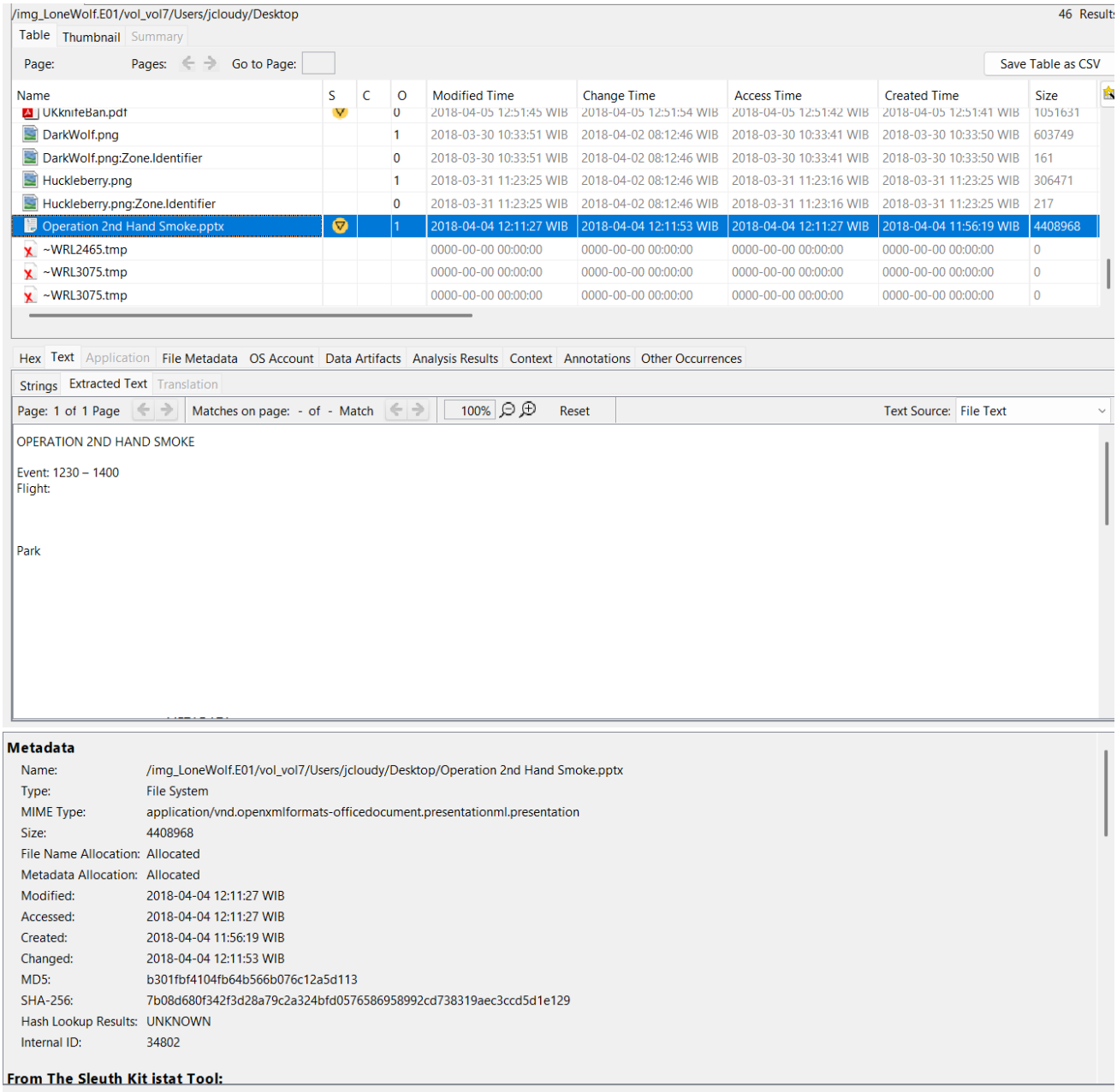
- SelfDefenseisMurder


/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop
46 Results
This is a DirectoryTree window
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
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
1
of 4
100%
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



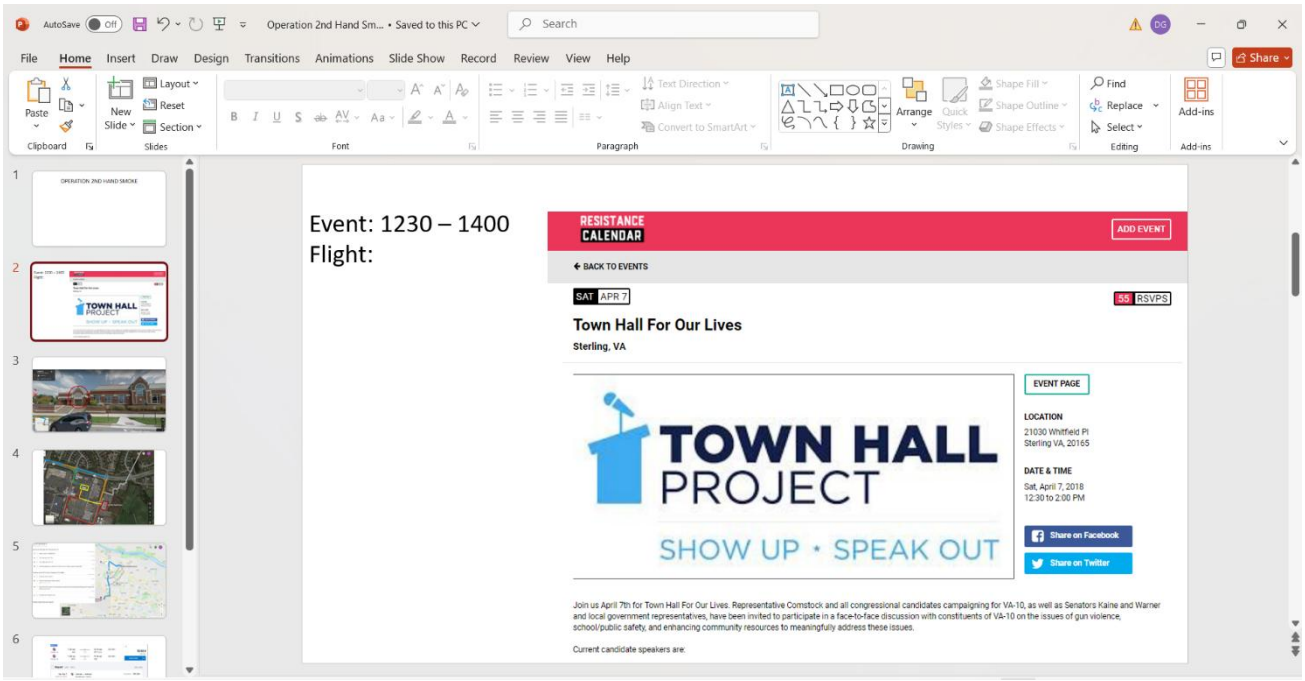
- Operation 2nd Hand Smoke

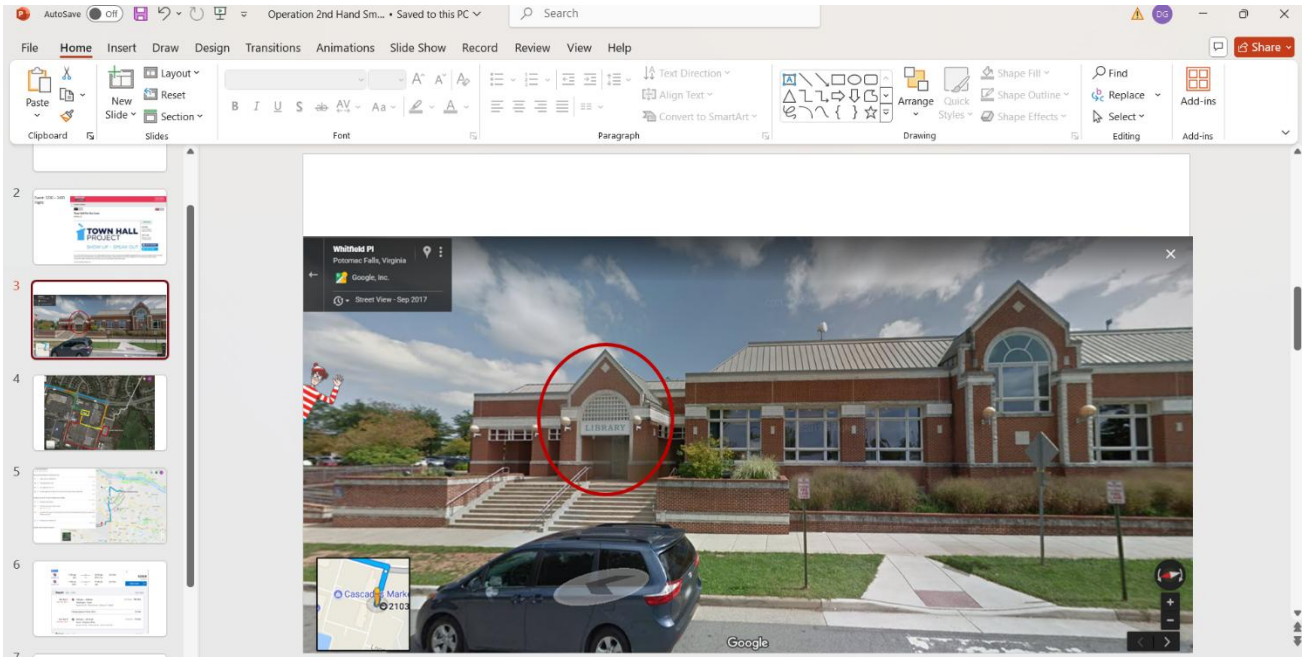


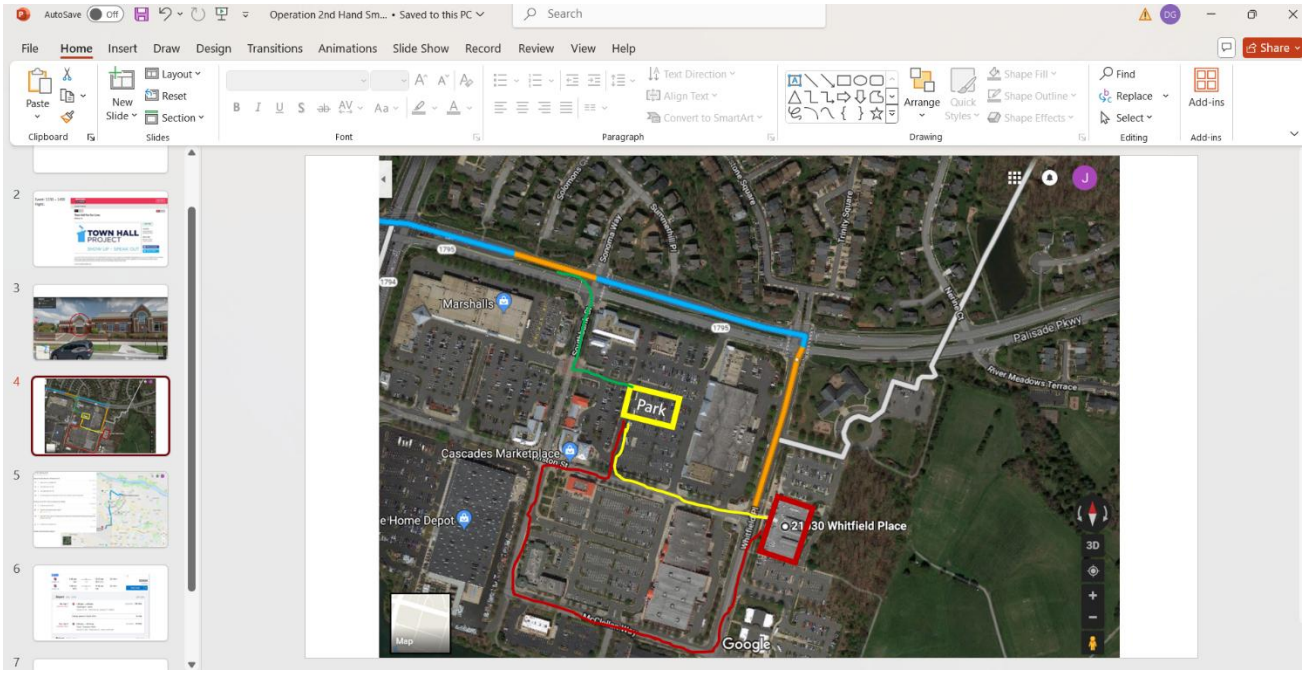
Metadata

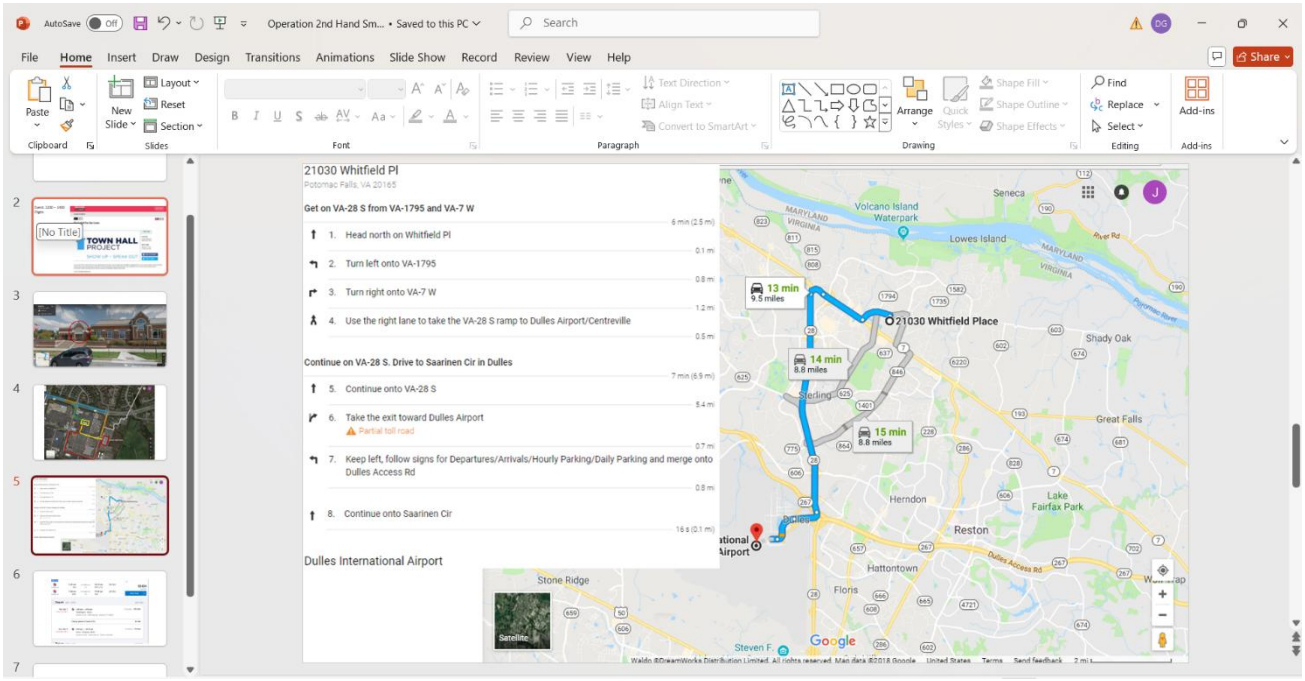
Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Operation 2nd Hand Smoke.pptx
Type:	File System
MIME Type:	application/vnd.openxmlformats-officedocument.presentationml.presentation
Size:	4408968
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2018-04-04 12:11:27 WIB
Accessed:	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:	7b08d680f342f3d28a79c2a324bfd0576586958992cd738319aec3ccd5d1e129
Hash Lookup Results:	UNKNOWN
Internal ID:	34802

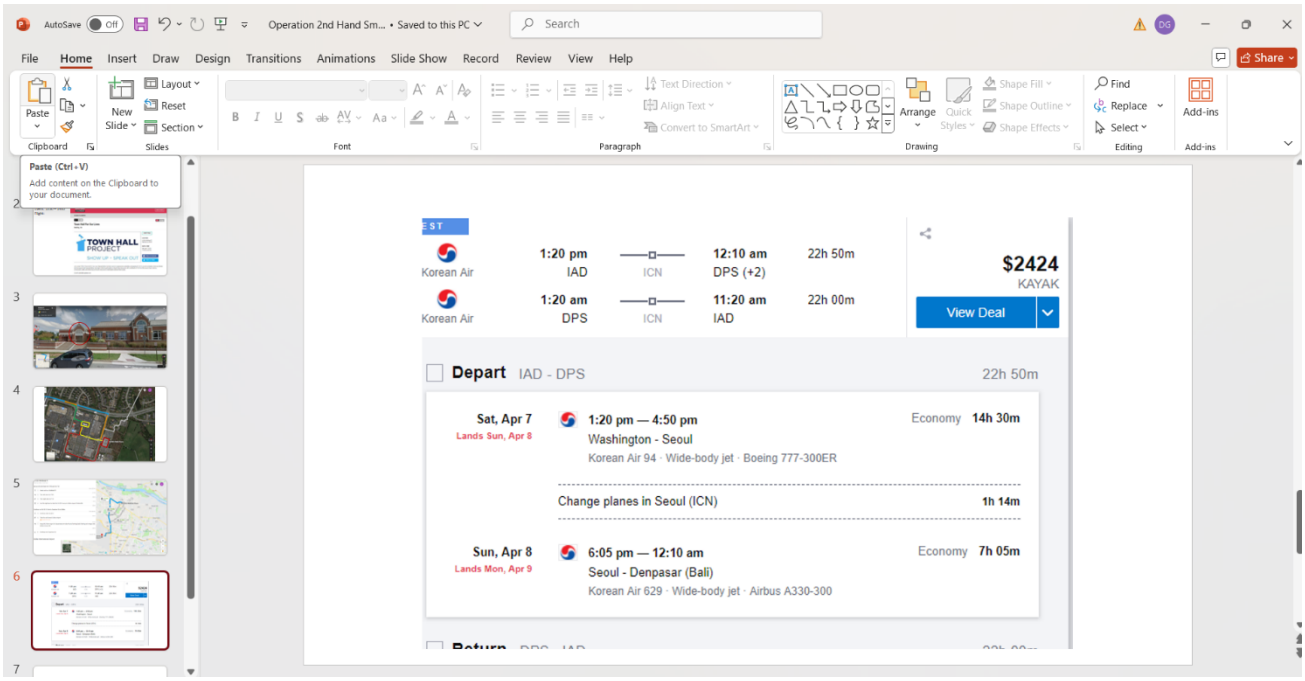
From The Sleuth Kit istat Tool:

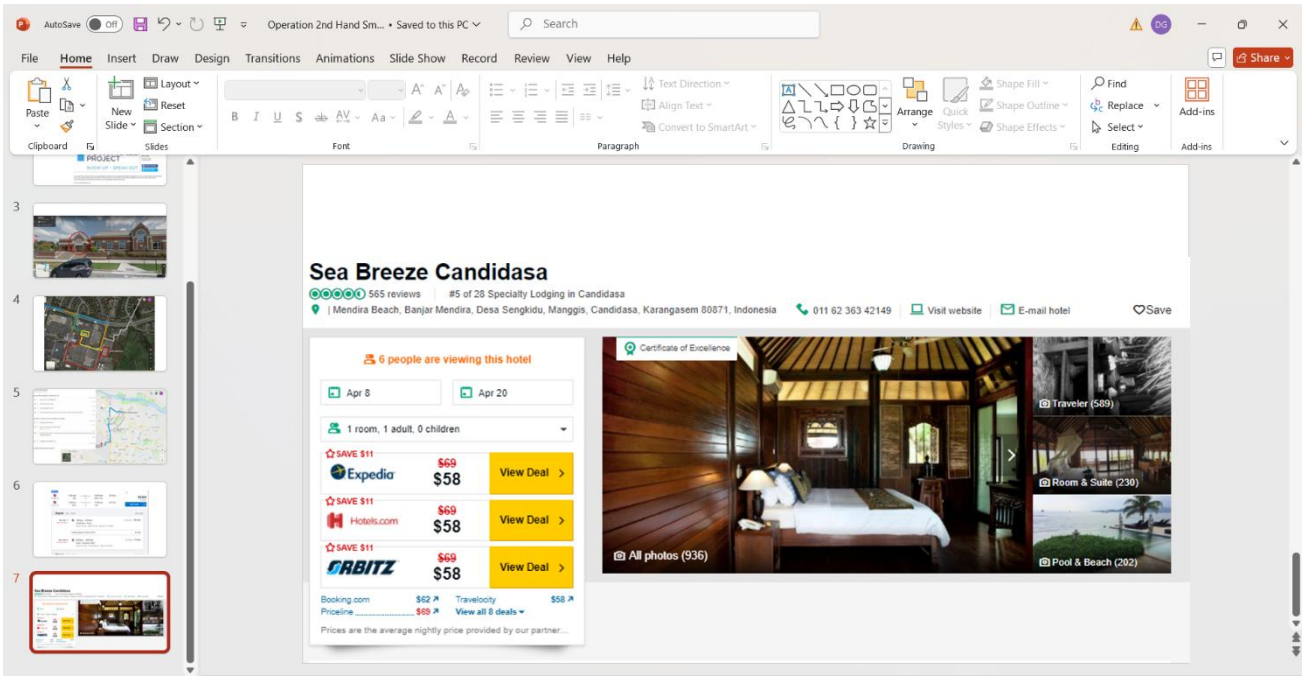

Operation 2nd Hand Sm... • Saved to this PC
Search
File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help
Share
Paste New Slide Layout Reset Section
Clipboard Slides Font Paragraph Drawing Editing Add-ins
Event: 1230 – 1400
Flight:
RESISTANCE CALENDAR
ADD EVENT
BACK TO EVENTS
SAT APR 7
55 RSVPS
Town Hall For Our Lives
Sterling, VA
TOWN HALL PROJECT
SHOW UP • SPEAK OUT
EVENT PAGE
LOCATION
21030 Whitfield Pl
Sterling VA, 20165
DATE & TIME
Sat, April 7, 2018
12:30 to 2:00 PM
Share on Facebook
Share on Twitter
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:


Operation 2nd Hand Sm... • Saved to this PC
Search
File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help
Share
Paste New Slide Layout Reset Section
Clipboard Slides Font Paragraph Drawing Editing Add-ins
Whitfield Pl
Potomac Falls, Virginia
Google, Inc.
Street View - Sep 2017
LIBRARY
Google

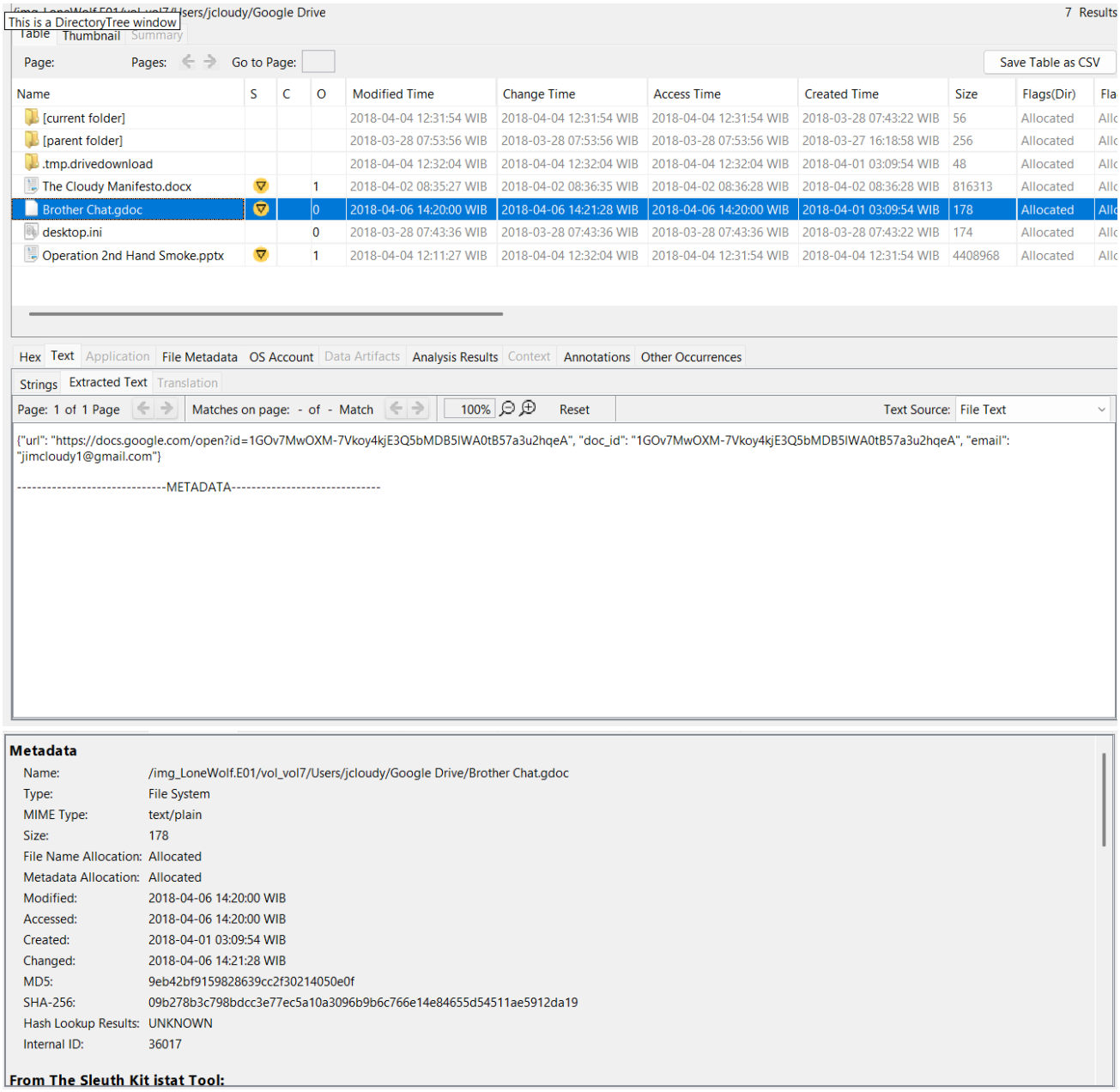

Operation 2nd Hand Sm... • Saved to this PC
Search
File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help
Share
Marshalls
Park
Cascades Marketplace
Home Depot
21030 Whitfield Place
Palisade Pkwy
River Meadows Terrace
Google


Operation 2nd Hand Sm... • Saved to this PC
Search
File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help
Share
21030 Whitfield Pl
Potomac Falls, VA 20165
Get on VA-28 S from VA-1795 and VA-7 W
1. Head north on Whitfield Pl
2. Turn left onto VA-1795
3. Turn right onto VA-7 W
4. Use the right lane to take the VA-28 S ramp to Dulles Airport/Centreville
Continue on VA-28 S. Drive to Saarinen Cir in Dulles
5. Continue onto VA-28 S
6. Take the exit toward Dulles Airport
Partial toll road
7. Keep left, follow signs for Departures/Arrivals/Hourly Parking/Daily Parking and merge onto Dulles Access Rd
8. Continue onto Saarinen Cir
Dulles International Airport
13 min
9.5 miles
14 min
8.6 miles
15 min
8.8 miles
21030 Whitfield Place
Volcano Island Waterpark
Lowes Island
Seneca
Shady Oak
Great Falls
Herndon
Reston
Hattontown
Floris
Stone Ridge
Lake Fairfax Park
Google

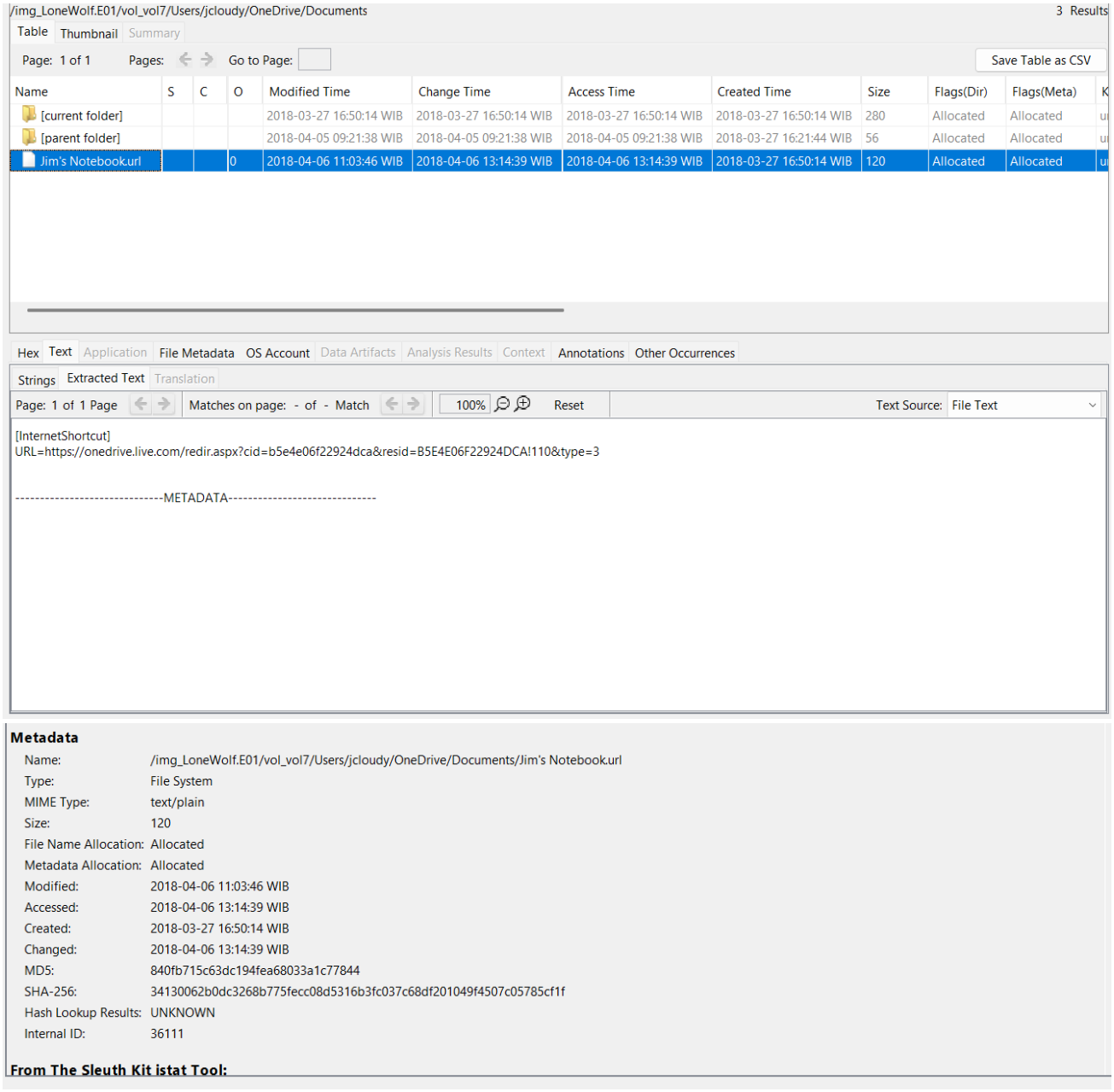

Operation 2nd Hand Sm... • Saved to this PC
Search
File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help
Share
Paste (Ctrl+V)
Add content on the Clipboard to your document.
Korean Air 1:20 pm IAD — ICN 12:10 am DPS (+2) 22h 50m
Korean Air 1:20 am DPS — ICN 11:20 am IAD 22h 00m
$2424
KAYAK
View Deal
Depart IAD - DPS 22h 50m
Sat, Apr 7
Lands Sun, Apr 8
1:20 pm — 4:50 pm
Washington - Seoul
Korean Air 94 · Wide-body jet · Boeing 777-300ER
Economy 14h 30m
Change planes in Seoul (ICN) 1h 14m
Sun, Apr 8
Lands Mon, Apr 9
6:05 pm — 12:10 am
Seoul - Denpasar (Bali)
Korean Air 629 · Wide-body jet · Airbus A330-300
Economy 7h 05m


Operation 2nd Hand Sm... • Saved to this PC
Search
File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help
Share
Sea Breeze Candidasa
565 reviews
#5 of 28 Specialty Lodging in Candidasa
Mendira Beach, Banjar Mendira, Desa Sengkidu, Manggis, Candidasa, Karangasem 80871, Indonesia
011 62 363 42149
Visit website
E-mail hotel
Save
6 people are viewing this hotel
Apr 8
Apr 20
1 room, 1 adult, 0 children
SAVE $11 Expedia $69 $58 View Deal
SAVE $11 Hotels.com $69 $58 View Deal
SAVE $11 ORBITZ $69 $58 View Deal
Booking.com $62
Priceline $69
Travelocity $58
View all 8 deals
Prices are the average nightly price provided by our partner...
Certificate of Excellence
All photos (936)
Traveler (589)
Room & Suite (230)
Pool & Beach (202)

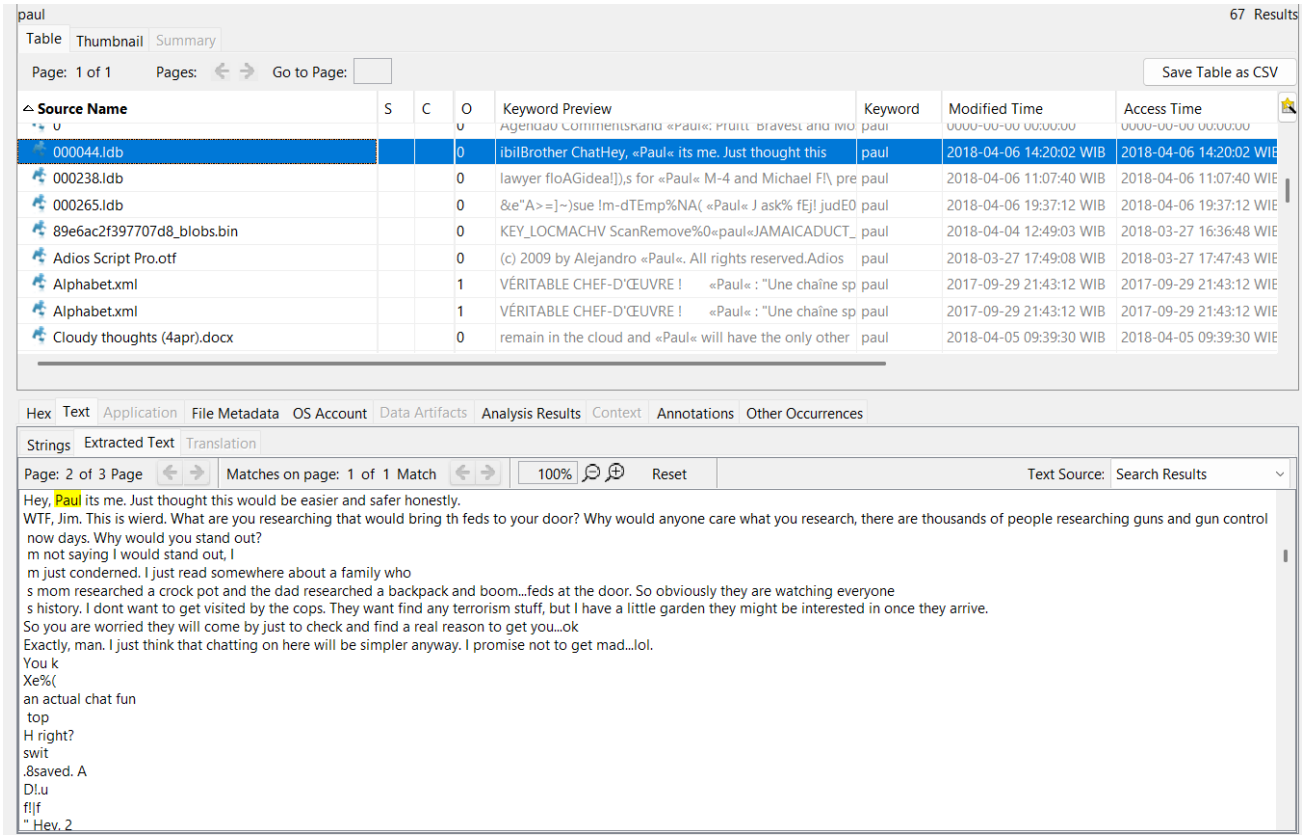
- Brother Chat



- Jim’s Notebook

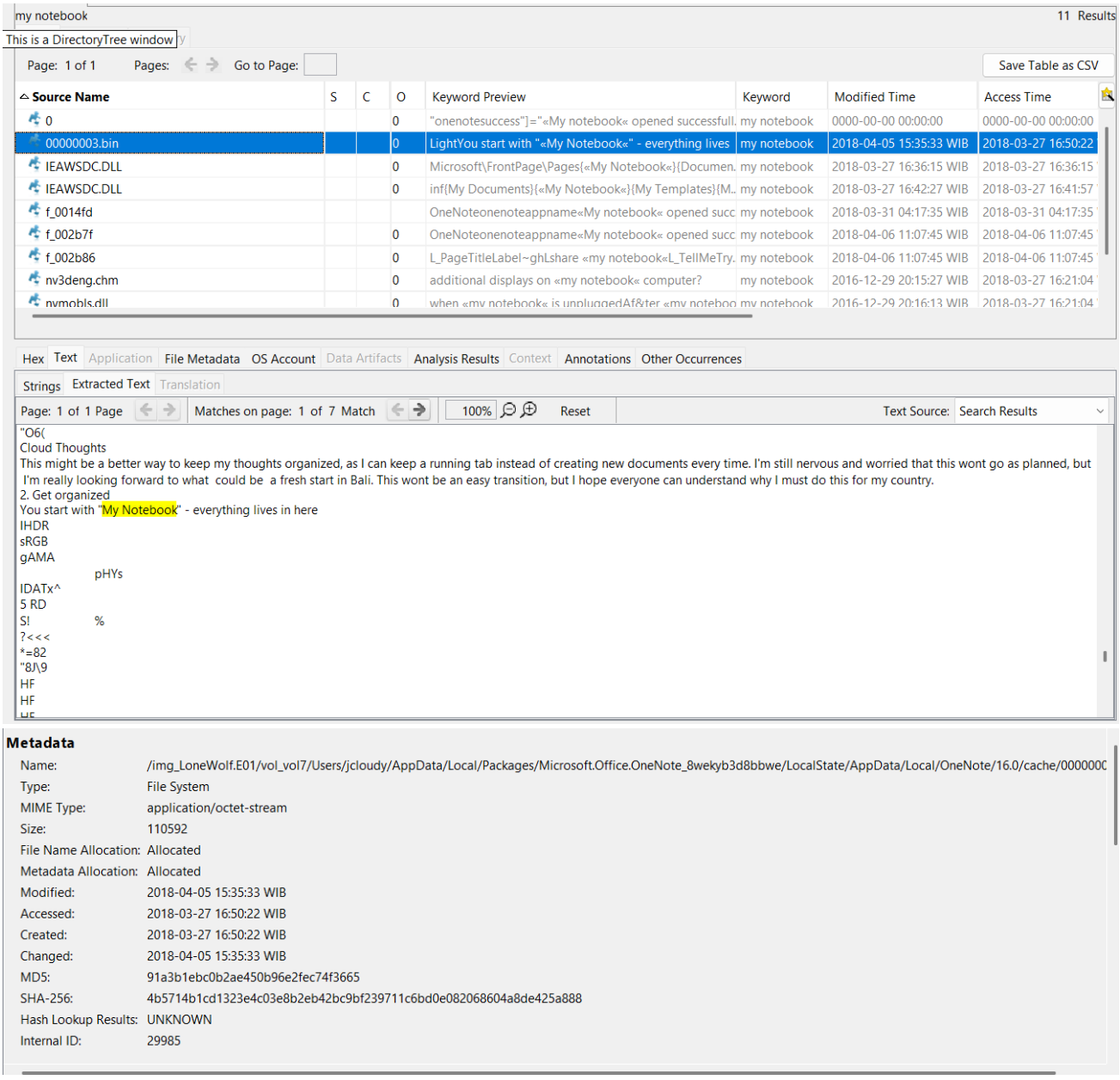


- 000044.idb

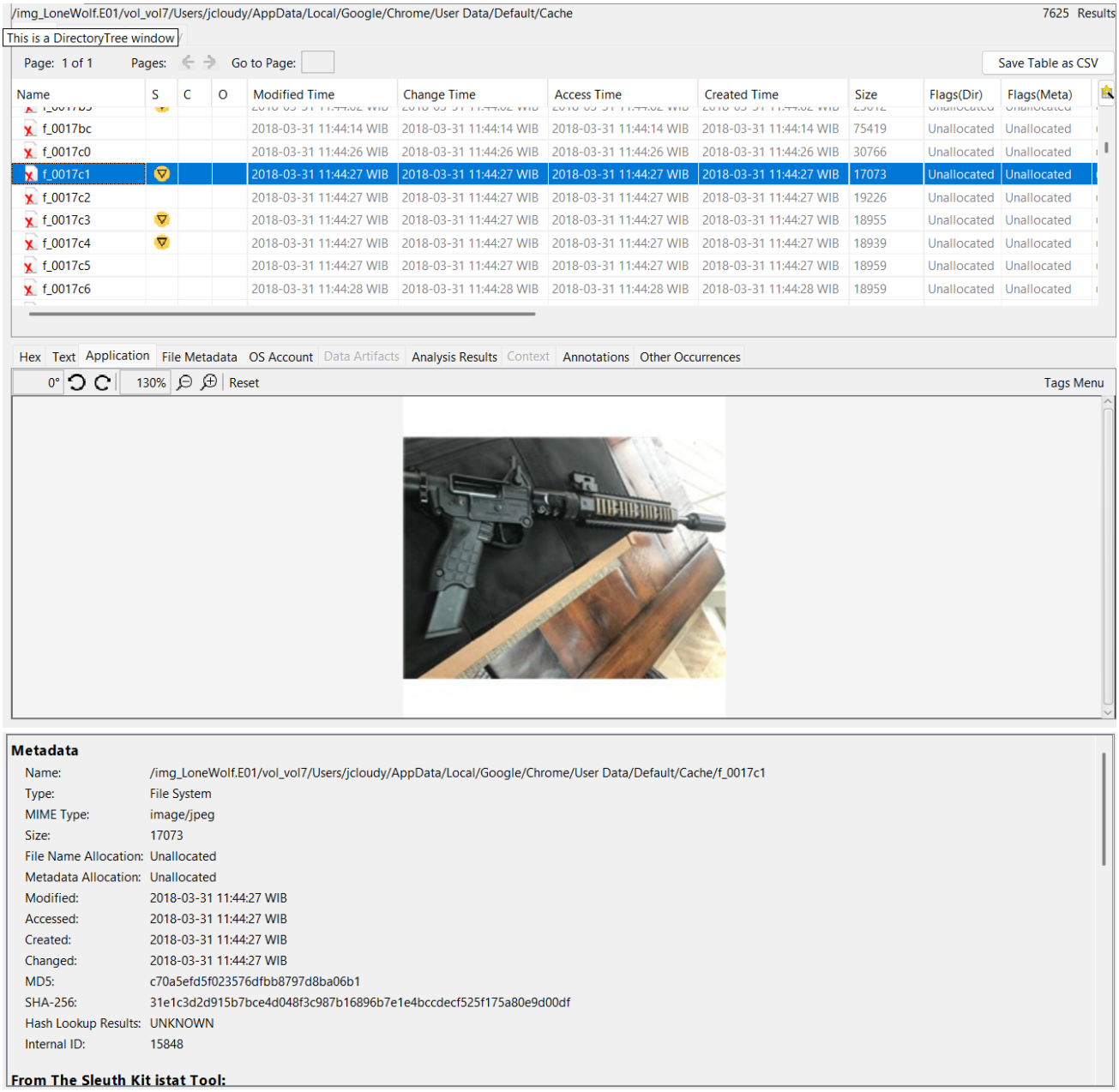

paul
67 Results
Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Save Table as CSV
Source Name
S
C
O
Keyword Preview
Keyword
Modified Time
Access Time
000044.ldb
0
ibilBrother ChatHey, «Paul« its me. Just thought this
paul
2018-04-06 14:20:02 WIB
2018-04-06 14:20:02 WIB
000238.ldb
0
lawyer floAGidea!]),s for «Paul« M-4 and Michael F!\ pre
paul
2018-04-06 11:07:40 WIB
2018-04-06 11:07:40 WIB
000265.ldb
0
&e"A>=]~)sue !m-dTEmp%NA(«Paul« J ask% fEj! judE0
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
2018-04-04 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?
m not saying I would stand out, I
m just conderned. 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
.8saved. A
D!.u
f!|f
" Hey, 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: 09b278b3c798bdcc3e77ec5a10a3096b9b6c766e14e84655d54511ae5912da19
Hash Lookup Results: UNKNOWN
Internal ID: 36017
From The Sleuth Kit istat Tool:

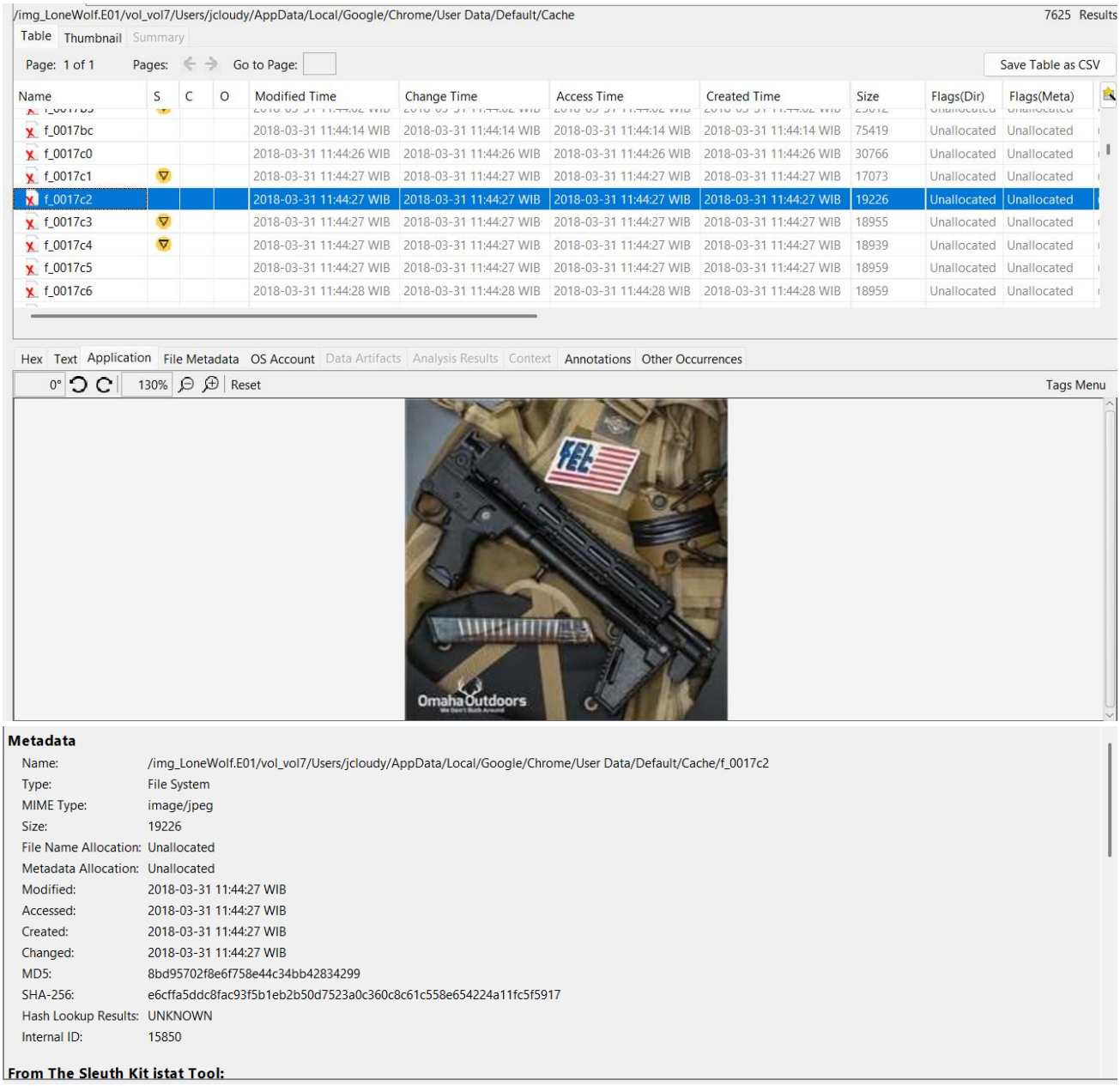
- 00000003.bin



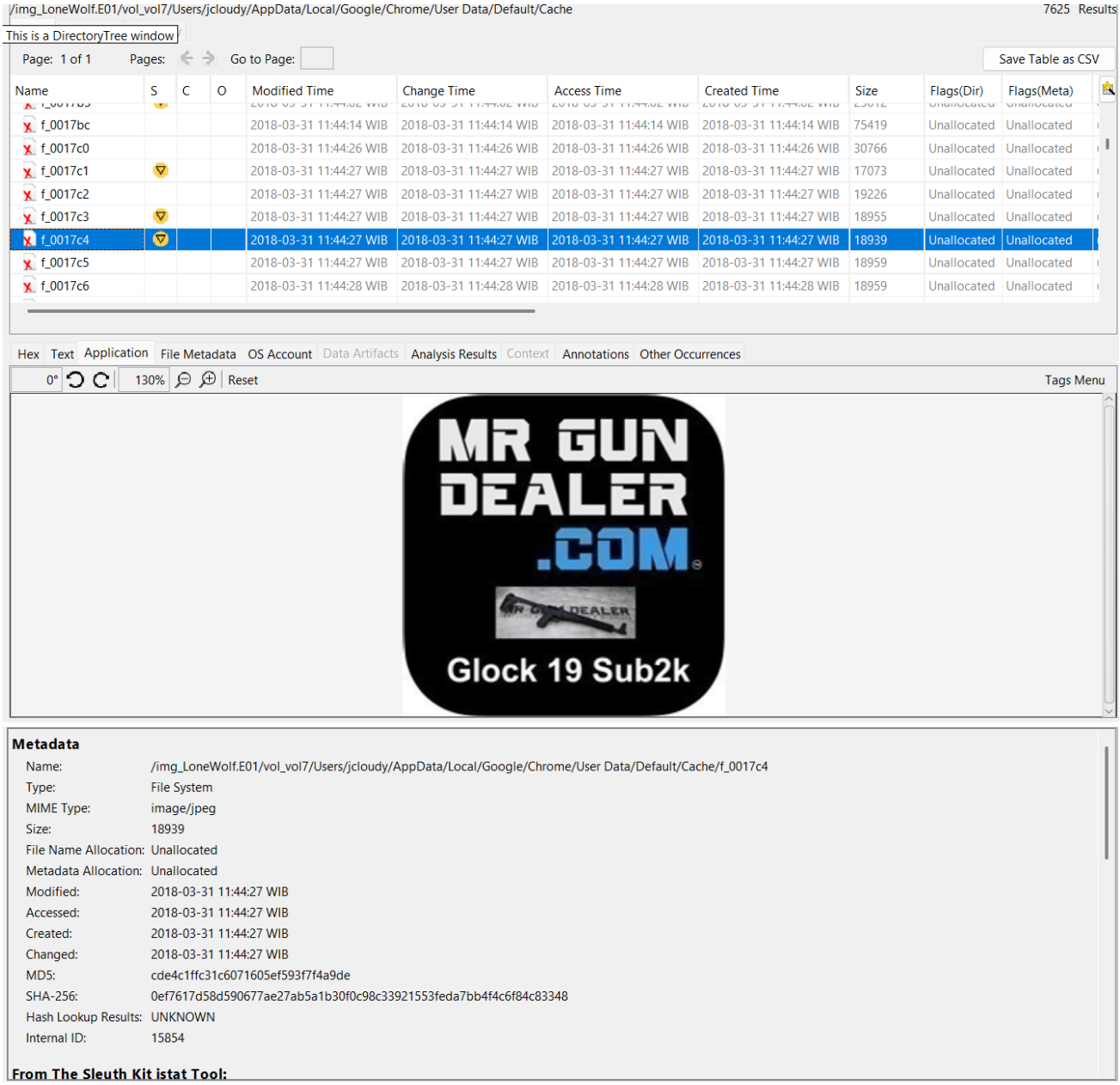
- f_0017c1


/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache
7625 Results
This is a DirectoryTree window
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)
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
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_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:

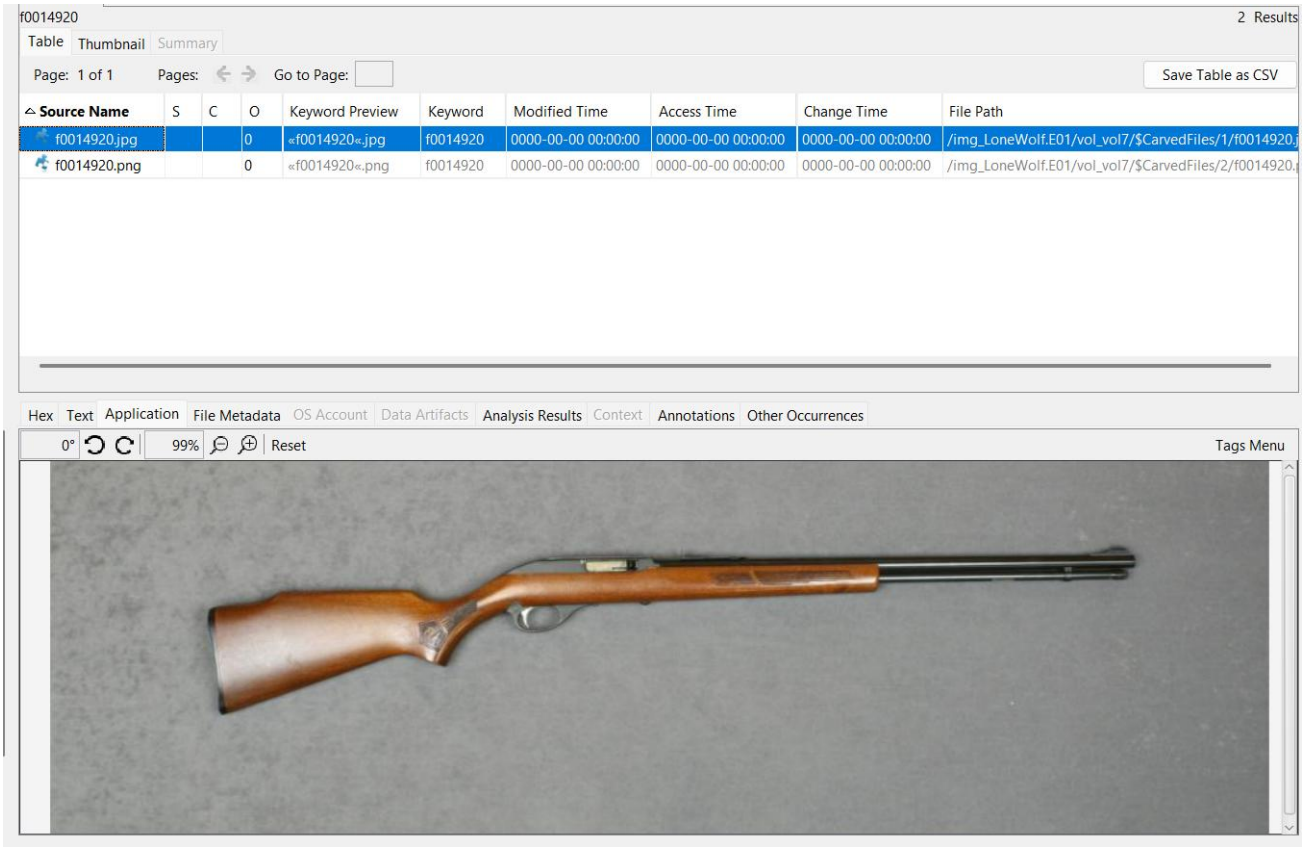
- f_0017c2


/img_LoneWolf.E01/vol_vol7/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)
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
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
0°
130%
Reset
Tags Menu
Omaha Outdoors
Metadata
Name: /img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_0017c2
Type: File System
MIME Type: image/jpeg
Size: 19226
File Name Allocation: Unallocated
Metadata Allocation: Unallocated
Modified: 2018-03-31 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: e6cffa5ddc8fac93f5b1eb2b50d7523a0c360c8c61c558e654224a11fc5f5917
Hash Lookup Results: UNKNOWN
Internal ID: 15850
From The Sleuth Kit istat Tool:

- f_0017c4

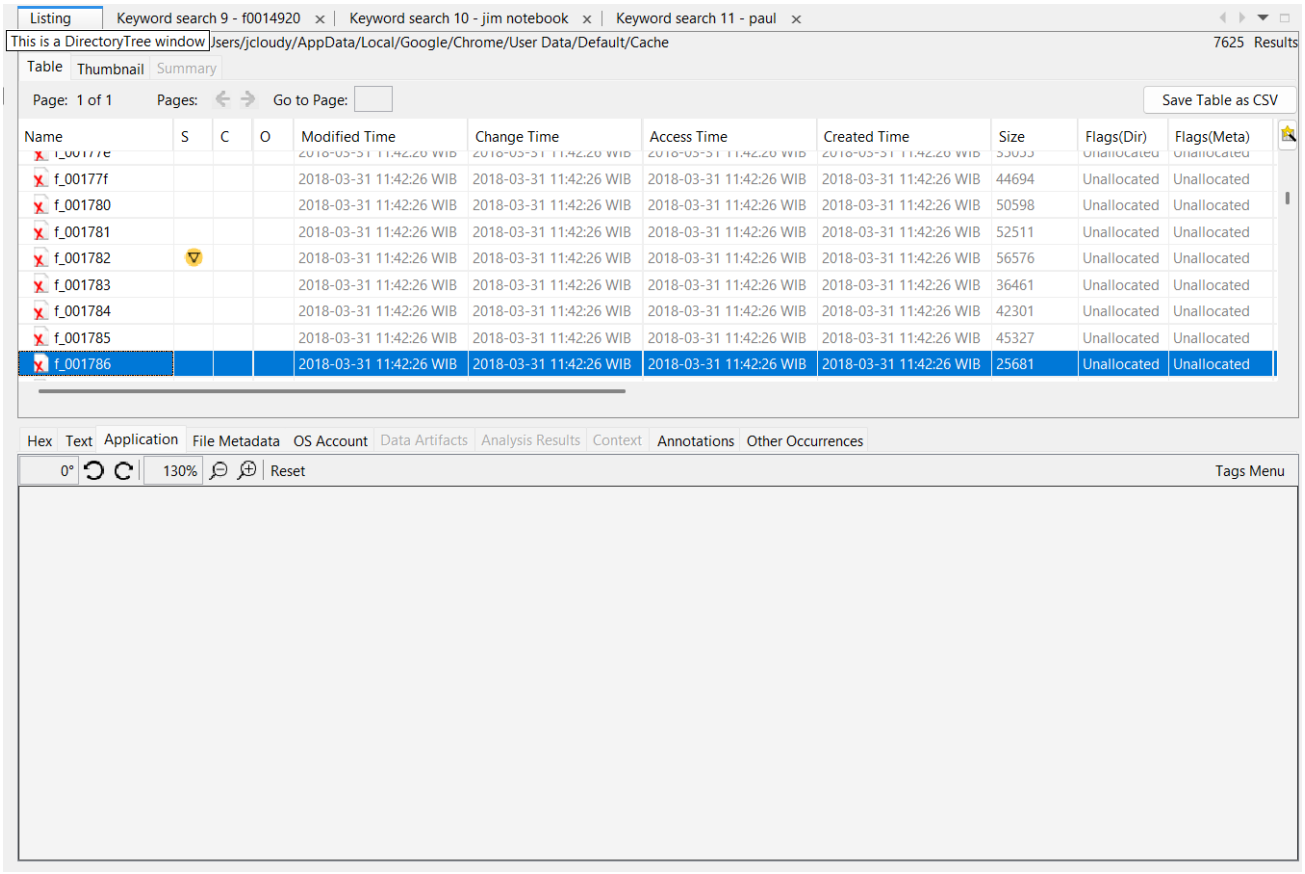

/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache
7625 Results
This is a DirectoryTree window
Page: 1 of 1
Pages:
Go to Page:
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time Size Flags(Dir) Flags(Meta)
f_0017bc 2018-03-31 11:44:14 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
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
0°
130%
Reset
Tags Menu
MR GUN DEALER .COM
Glock 19 Sub2k
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: cde4c1ffc31c6071605ef593f7f4a9de
SHA-256: 0ef7617d58d590677ae27ab5a1b30f0c98c33921553feda7bb4f4c6f84c83348
Hash Lookup Results: UNKNOWN
Internal ID: 15854
From The Sleuth Kit istat Tool:

- f0014920


f0014920
2 Results
Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Save Table as CSV
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.
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
0°
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: db9efa4f671f6b25db5c14279132a3ac86fc206cc3fbeb44e9837d7701509ebb
Hash Lookup Results: UNKNOWN
Internal ID: 412968

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

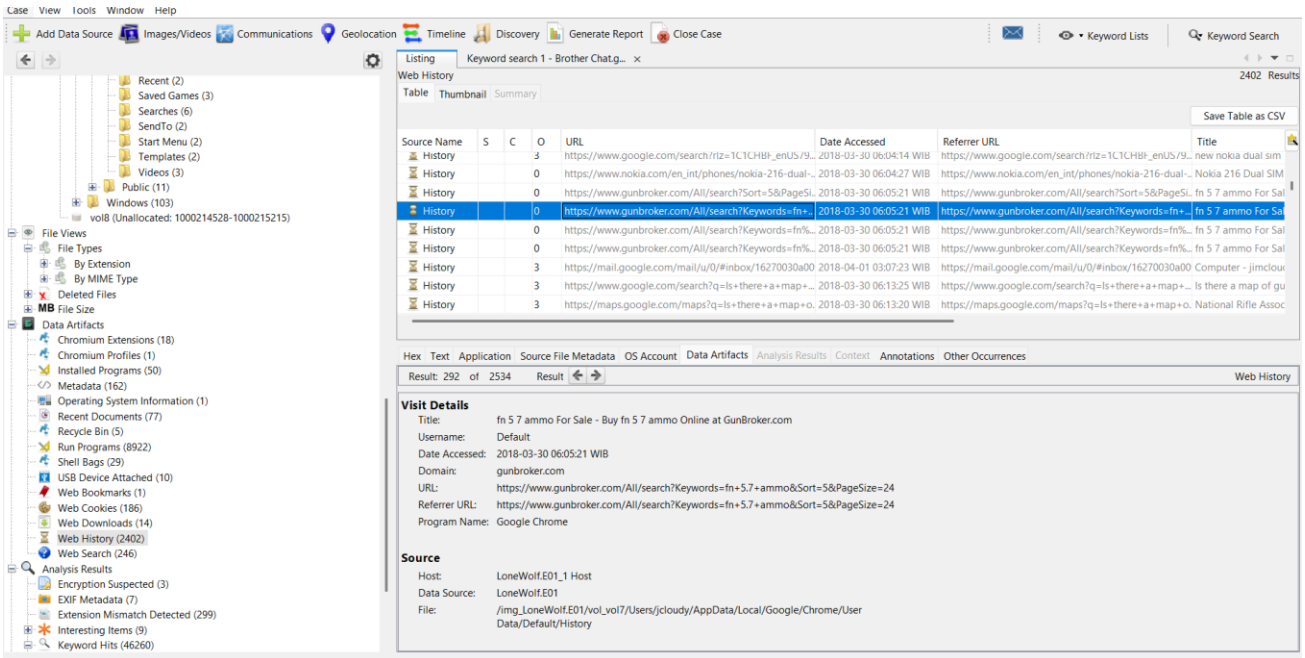


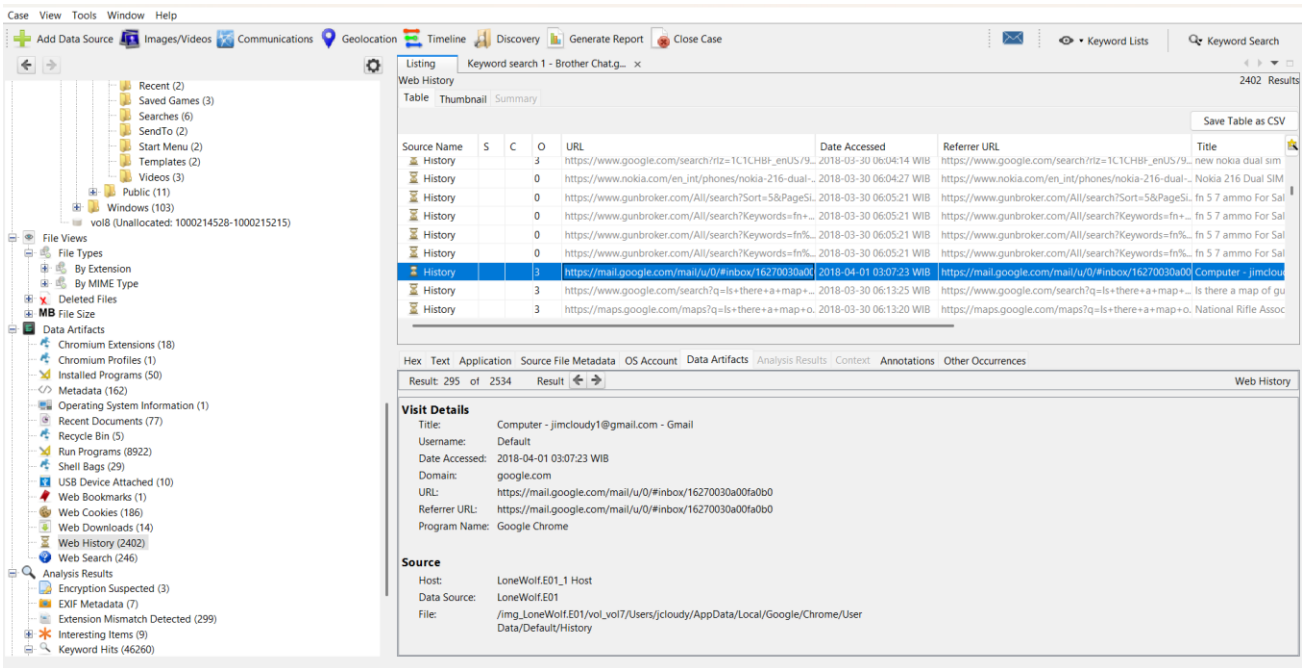
Metadata

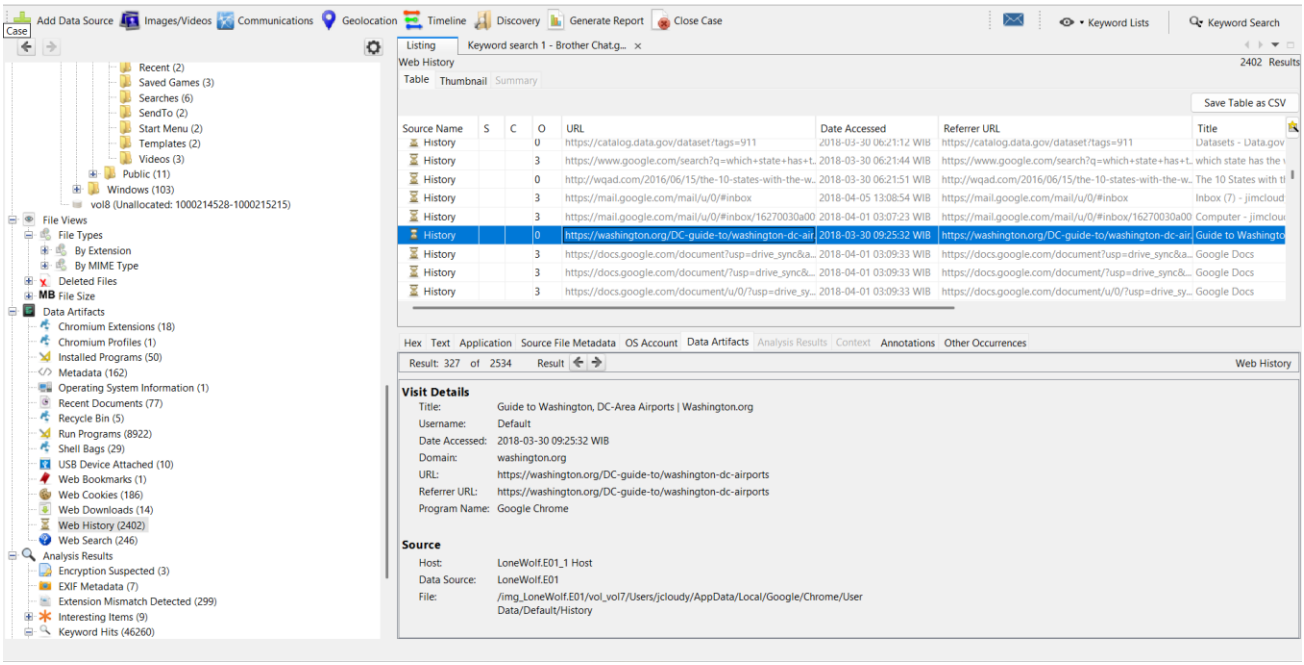
Name:	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/AppData/Local/Google/Chrome/User Data/Default/Cache/f_001786
Type:	File System
MIME Type:	image/png
Size:	25681
File Name Allocation:	Unallocated
Metadata Allocation:	Unallocated
Modified:	2018-03-31 11:42:26 WIB
Accessed:	2018-03-31 11:42:26 WIB
Created:	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

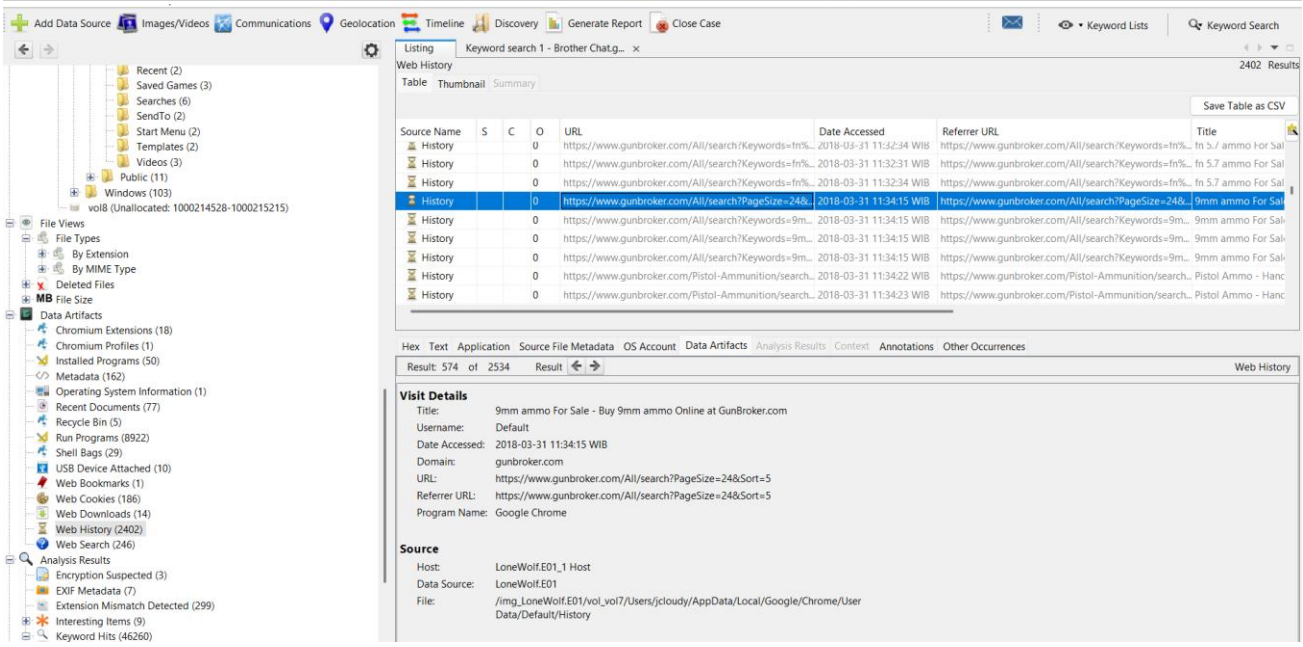
From The Sleuth Kit istat Tool:

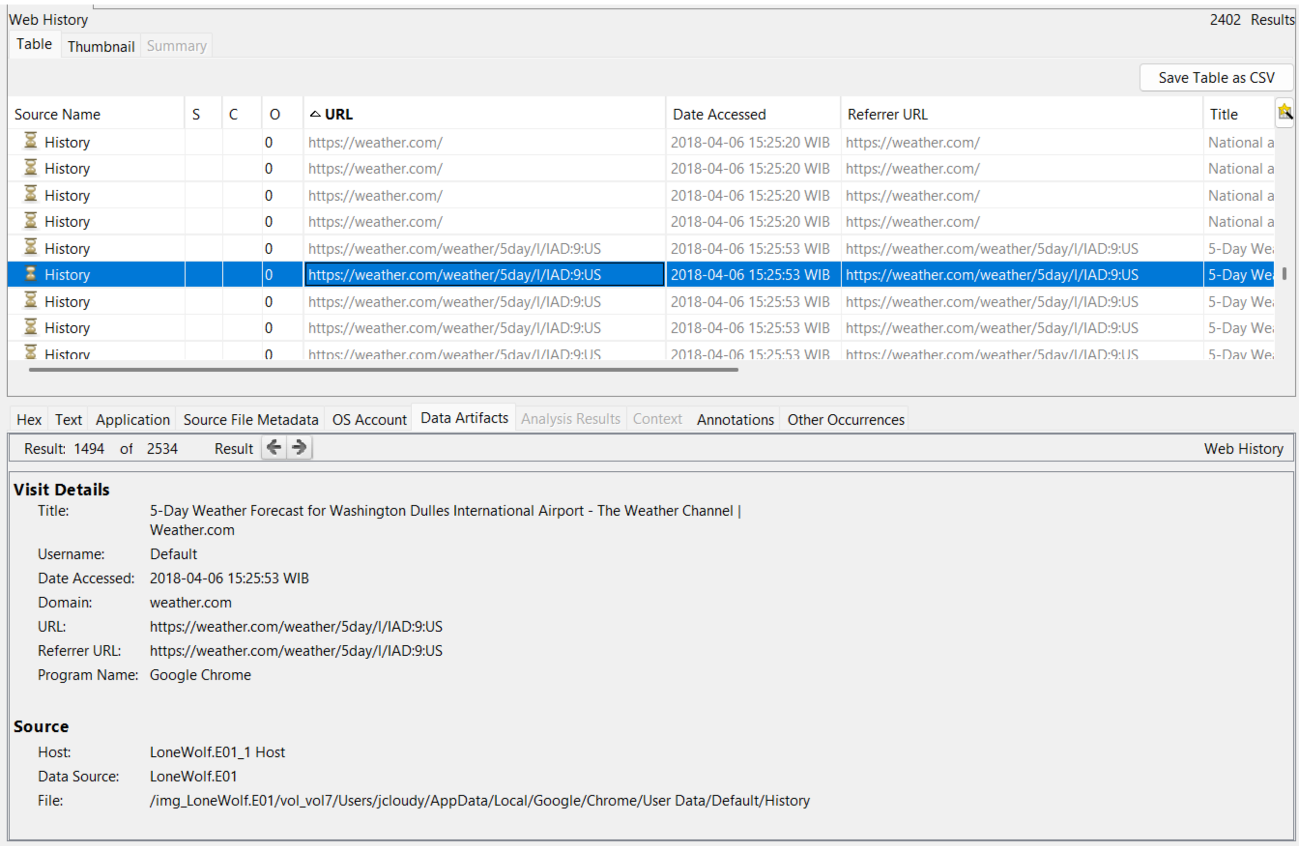
- web artefak

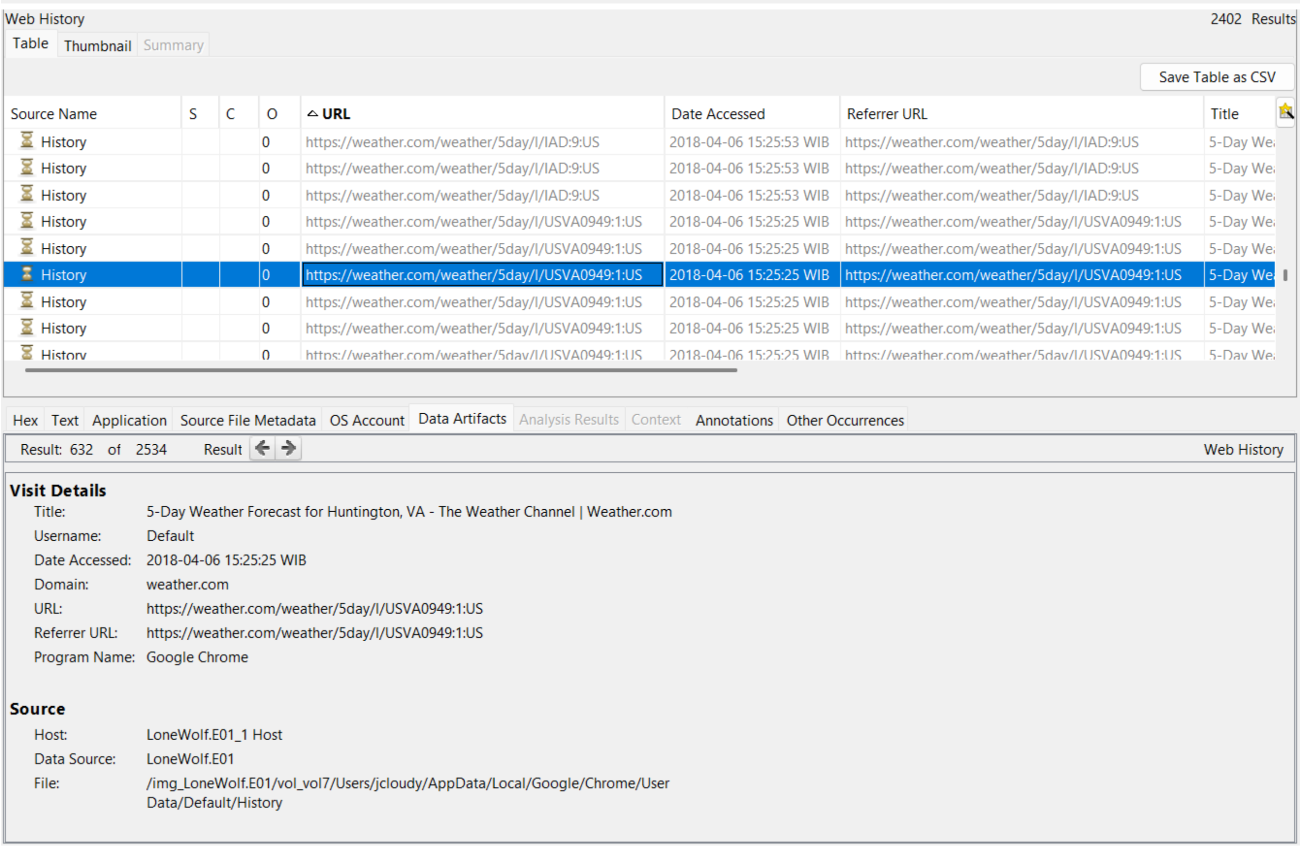


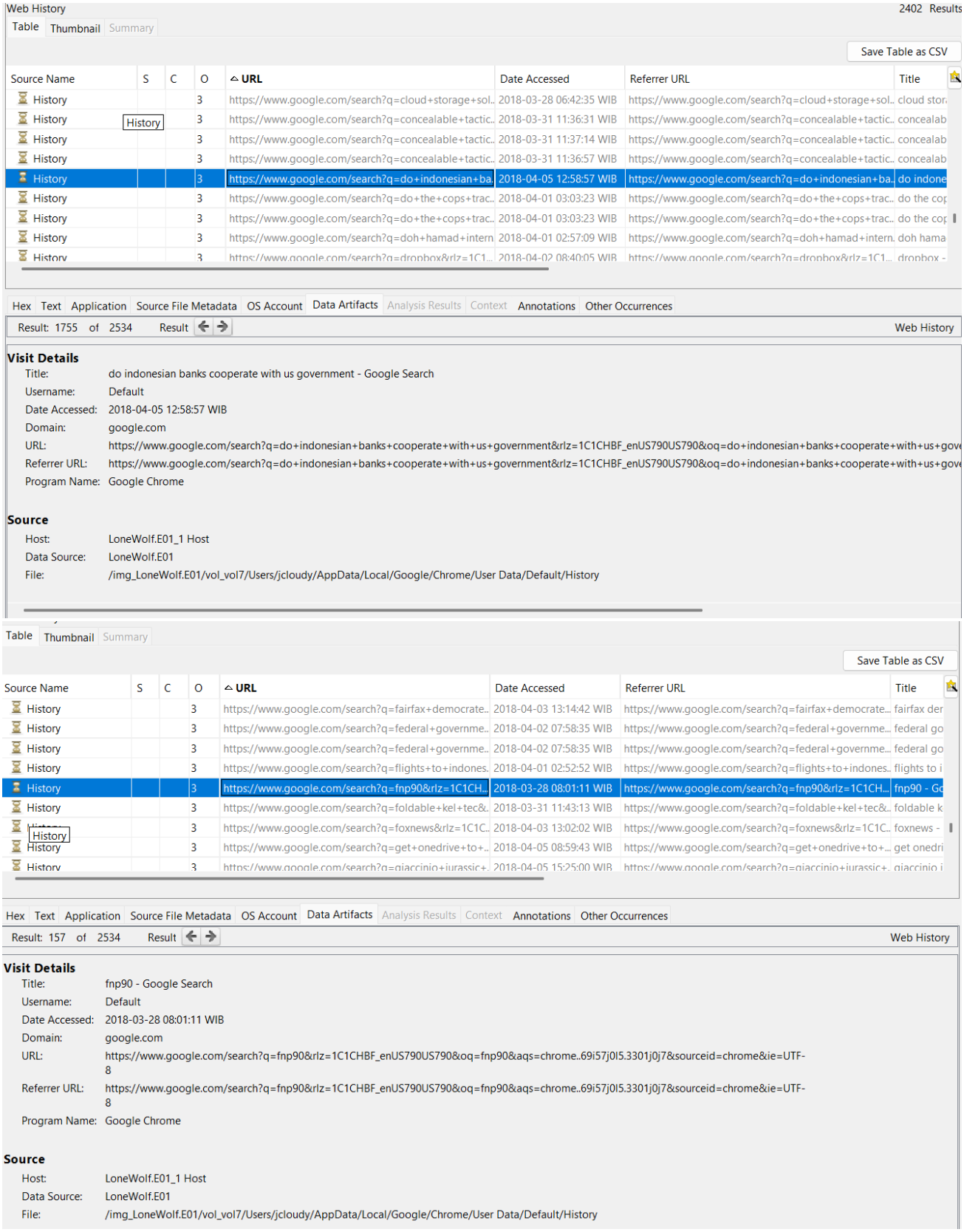


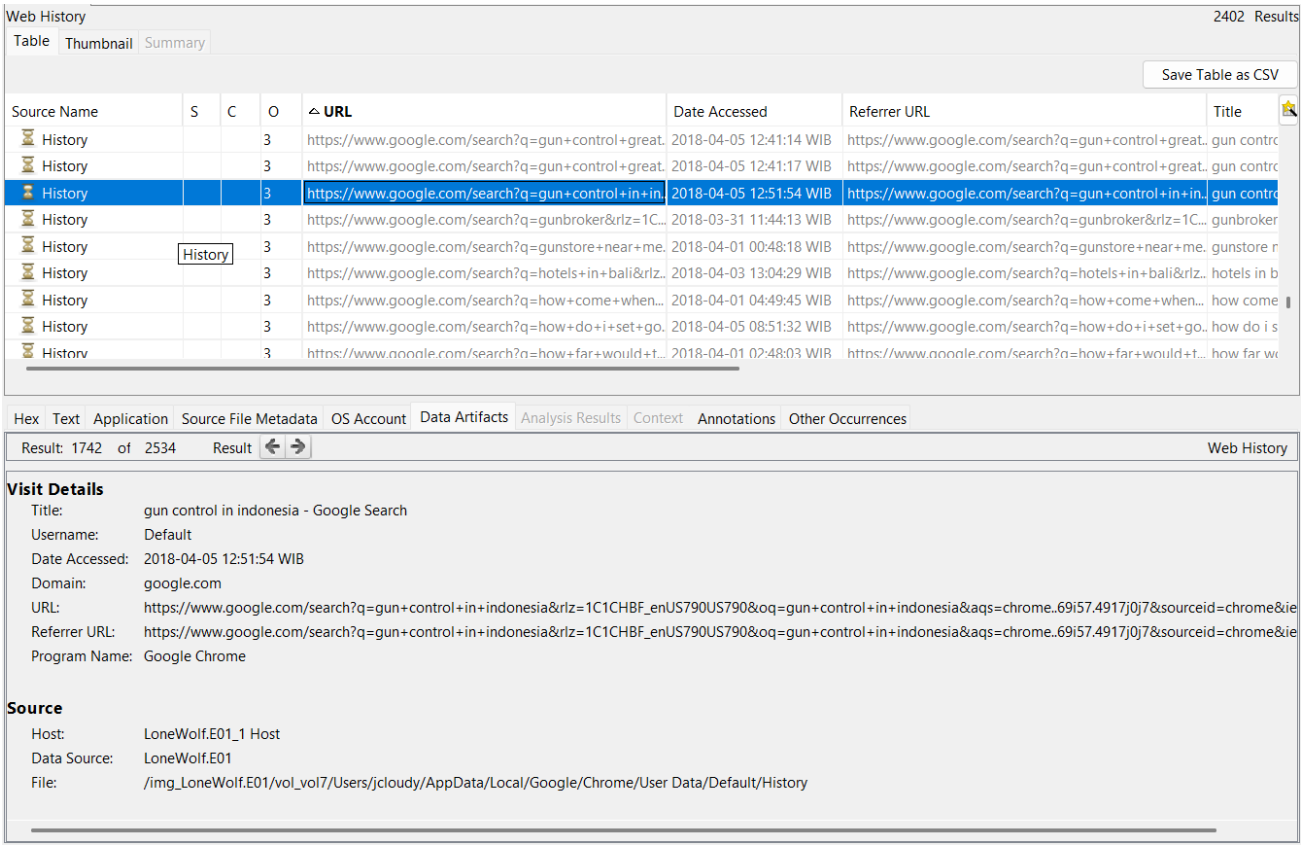

Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Case
Listing
Keyword search 1 - Brother Chat.g...
Web History
2402 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
URL
Date Accessed
Referrer URL
Title
Recent (2)
Saved Games (3)
Searches (6)
SendTo (2)
Start Menu (2)
Templates (2)
Videos (3)
Public (11)
Windows (103)
vol8 (Unallocated: 1000214528-1000215215)
File Views
File Types
By Extension
By MIME Type
Deleted Files
File Size
Data Artifacts
Chromium Extensions (18)
Chromium Profiles (1)
Installed Programs (50)
Metadata (162)
Operating System Information (1)
Recent Documents (77)
Recycle Bin (5)
Run Programs (8922)
Shell Bags (29)
USB Device Attached (10)
Web Bookmarks (1)
Web Cookies (186)
Web Downloads (14)
Web History (2402)
Web Search (246)
Analysis Results
Encryption Suspected (3)
EXIF Metadata (7)
Extension Mismatch Detected (299)
Interesting Items (9)
Keyword Hits (46260)
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/User Data/Default/History


Add Data Source
Images/Videos
Communications
Geolocation
Timeline
Discovery
Generate Report
Close Case
Keyword Lists
Keyword Search
Listing
Keyword search 1 - Brother Chat.g...
Web History
2402 Results
Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
URL
Date Accessed
Referrer URL
Title
Recent (2)
Saved Games (3)
Searches (6)
SendTo (2)
Start Menu (2)
Templates (2)
Videos (3)
Public (11)
Windows (103)
vol8 (Unallocated: 1000214528-1000215215)
File Views
File Types
By Extension
By MIME Type
Deleted Files
File Size
Data Artifacts
Chromium Extensions (18)
Chromium Profiles (1)
Installed Programs (50)
Metadata (162)
Operating System Information (1)
Recent Documents (77)
Recycle Bin (5)
Run Programs (8922)
Shell Bags (29)
USB Device Attached (10)
Web Bookmarks (1)
Web Cookies (186)
Web Downloads (14)
Web History (2402)
Web Search (246)
Analysis Results
Encryption Suspected (3)
EXIF Metadata (7)
Extension Mismatch Detected (299)
Interesting Items (9)
Keyword Hits (46260)
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/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/ 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
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/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+gove
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+gove
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=giaccinio+jurassic+.. 2018-04-05 15:25:00 WIB https://www.google.com/search?q=giaccinio+jurassic+.. giaccinio j
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



EXAMINATION

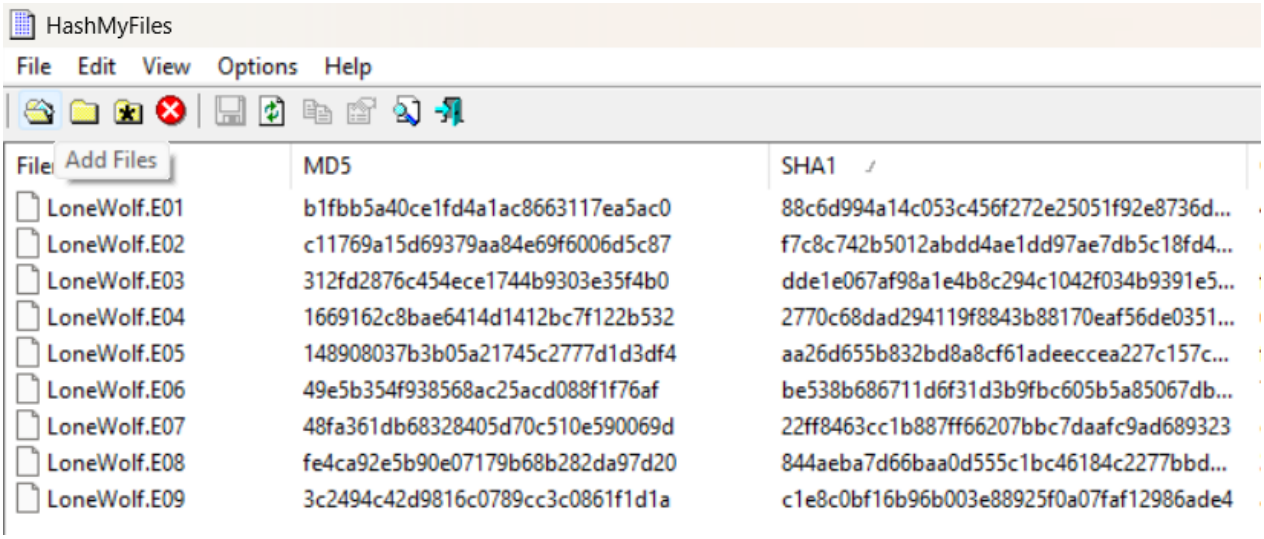
TOOLS

- 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



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.leveldb/000044.ldb
Brother Chat.gdoc	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Google Drive/Brother Chat.gdoc
Cubs' Anthony Rizzo Praises Parkland Kids, Says 'It's too Easy to Get a Gun'	/img_LoneWolf.E01/vol_vol7/Users/jcloudy/Desktop/Cubs' Anthony Rizzo Praises 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 aktiftas 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.ldb* 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.ldb" dan penyebutan 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:

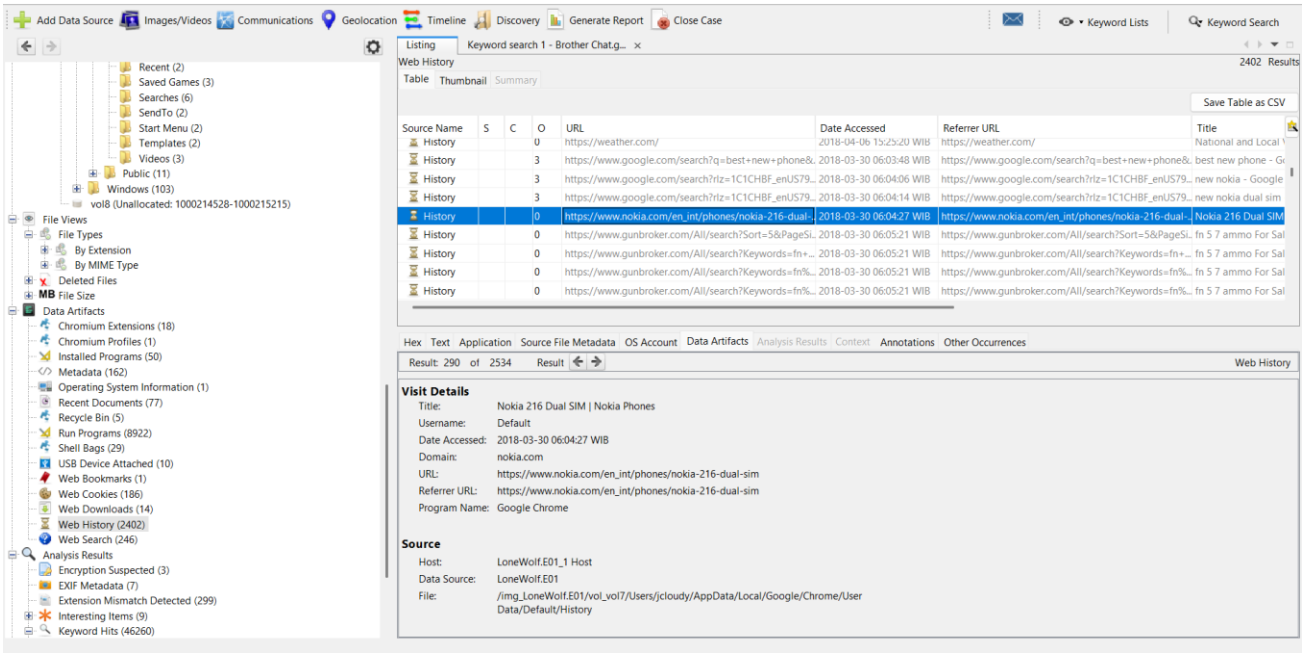
1. Pemeriksaan Lanjutan terhadap Paul
   Perlu dilakukan pemeriksaan lebih mendalam terhadap individu bernama Paul yang disebut dalam file "Cloudy Thoughts (4apr).docx" dan percakapan dalam file "000044.ldb" untuk mengetahui sejauh mana keterlibatannya dalam perencanaan tindakan tersebut.

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



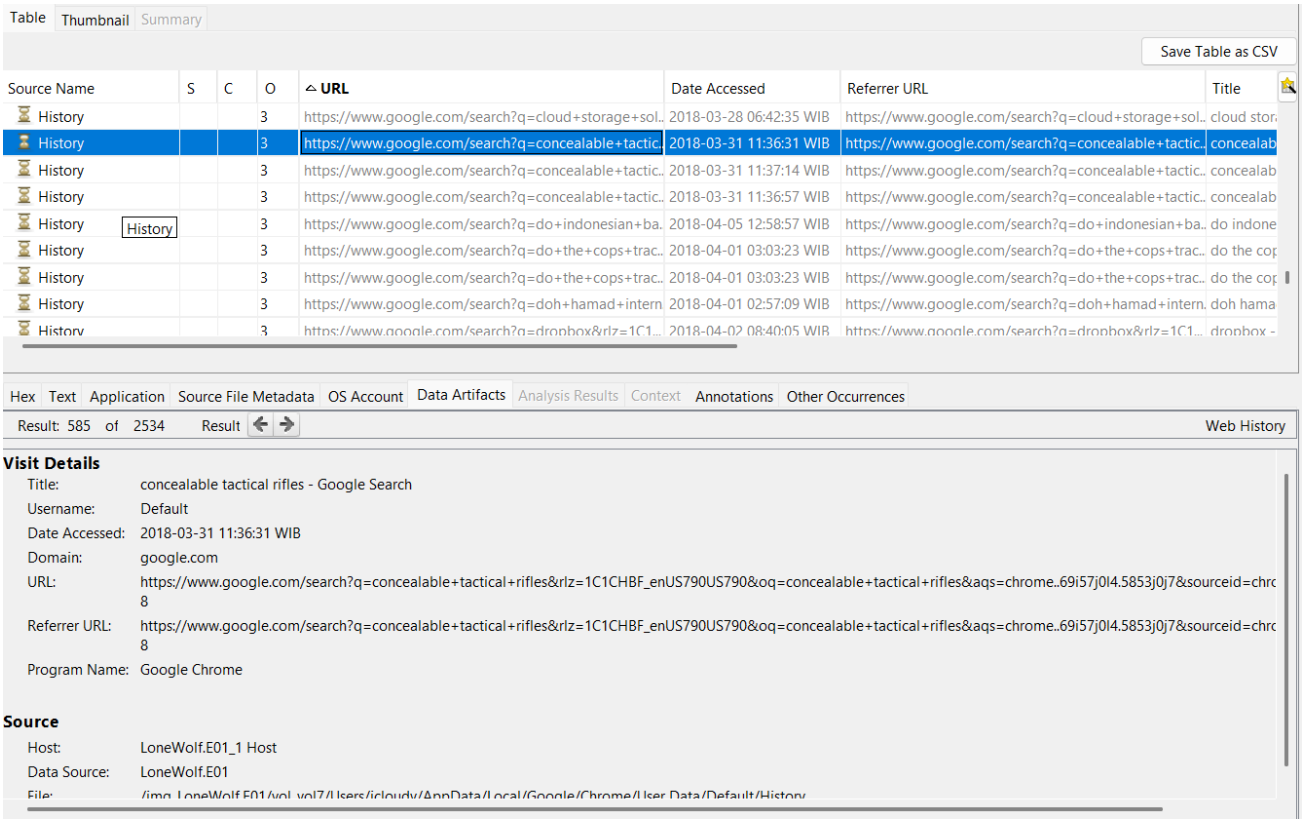


Table
Thumbnail
Summary
Save Table as CSV
Source Name
S
C
O
URL
Date Accessed
Referrer URL
Title
History
3
https://www.google.com/search?q=cloud+storage+sol..
2018-03-28 06:42:35 WIB
https://www.google.com/search?q=cloud+storage+sol..
cloud stor
History
3
https://www.google.com/search?q=concealable+tactic..
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=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: 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
8
Referrer URL: https://www.google.com/search?q=concealable+tactical+rifles&rlz=1C1CHBF_enUS790US790&oq=concealable+tactical+rifles&aqs=chrome..69i57j0l4.5853j0j7&sourceid=chrc
8
Program Name: Google Chrome
Source
Host: LoneWolf.E01_1 Host
Data Source: LoneWolf.E01
File: /img_LoneWolf.E01/vol_vol7/Users/icloudy/AppData/Local/Google/Chrome/User Data/Default/History