

1. Who was the suspect?

- **Steve Kowhai** was the suspect

Listing				
/img_Narcos-1.001/vol_vo17/Users				
Table Thumbnail Summary				
Name	S	C	O	Modified Time
[current folder]				2019-01-29 03:40:50 SGT
[parent folder]				2019-02-02 10:39:25 SGT
All Users				2018-09-15 15:42:33 SGT
Default				2019-01-29 03:15:04 SGT
Default User				2018-09-15 15:42:33 SGT
Public				2019-01-29 03:35:35 SGT
Steve				2019-01-29 03:37:51 SGT
desktop.ini				2018-09-15 15:31:34 SGT

Steve has some basic digital forensics knowledge, as seen from the forensics related applications in his file system such as Image Steganography, TrueCrypt and CCleaner.

2. What did the suspect want from John during the latter's trip?

John is the drug supplier, providing Steve the drug buyer.

Initial dealing spot: Eastbourne library

Secondary dealing spot: 666 Rewera Avenue, Petone.

Steve googled best places to deal drug.

Steve made use of image steganography to exchange information.

Steve also googled the route to the meeting location.

Listing /img_Narcos-1.001/vol_vol7/Users/Steve/AppData/Roaming/Image_Steganography_Setup/Image Steganography Setup/1.0.0.0

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

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
[current folder]				2019-02-01 08:16:47 SGT	2019-02-01 08:16:47 SGT	2019-02-01 08:16:47 SGT	2019-02-01 08:16:47 SGT	48	Allocated	A
[parent folder]				2019-02-01 08:16:47 SGT	2019-02-01 08:16:47 SGT	2019-02-01 08:16:47 SGT	2019-02-01 08:16:47 SGT	240	Allocated	A

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

Web search of drugs and Eastbourne library

History	1	https://www.google.com/search?ei=wexUXPmDJK-9QPL...	2019-02-02 09:05:11 SGT	https://www.google.com/search?ei=wexUXPmDJK-9QPL...	eastbourne library - Google Search	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:22 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:24 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:24 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:24 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 09:05:24 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
History	1	https://www.google.com/maps/place/Eastbourne+Library/...	2019-02-02 10:28:18 SGT	https://www.google.com/maps/place/Eastbourne+Library/...	Eastbourne Library - Google Maps	Google Chrome
WebCodecs	0	https://join.vivaldi.net/vtch23/index.html#E120	2019-01-01 02:00:00 SGT		Steve_K_PNG (1162>S39)	Microsoft Edge

They communicated via Discord. See Users\Steve\AppData\Roaming\Discord\Local Storage\leveldb\00000006.log

The screenshot shows a digital forensic analysis interface. At the top, there's a navigation bar with tabs like 'Listing', 'Thumbnail', and 'Summary'. Below that is a table with columns: Source Name, S, C, O, Keyword, Keyword Regul..., Keyword Preview, Modified Time, Access Time, Change Time, and File Path. A single row is selected in the table, corresponding to the file '000006.log'. The 'File Path' column shows the full path: /img_Narcos-1.001/vol_v07/Users/Steve/AppD... The bottom half of the interface is a text editor with tabs for 'Hex', 'Text', 'Application', 'File Metadata', etc. The 'Text' tab is active, displaying a series of messages from a bot named '666 Rewera'. The messages include: 'each other come to <666 rewea< avenue, peton");', 'Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone."}, "version":0}', 'Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone."}, "version":0}U++pw', and 'Good Thinking, I already know how. Heard of steg"}], "version":0}[^'. The text editor also shows some META tags and DraftStore entries.

They hid something using steganography

The screenshot shows a digital forensic analysis interface. The text view displays a series of messages from a bot named '666 Rewera'. The messages include: 'each other come to <666 rewea< avenue, peton");', 'Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone."}, "version":0}', 'Good. Meet at the Eastbourne library and if we miss each other come to 666 Rewera Avenue, Petone."}, "version":0}U++pw', and 'Good Thinking, I already know how. Heard of steg"}], "version":0}[^'. The text editor also shows some META tags and DraftStore entries.

Meet at Eastbourne library

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

```

DraftStoreo
{"_state": {"539550615072800768": {"timestamp": 1549074550106, "draft": "Good. Meet at the Eastbou"}, "_version": 0}
META:https://discordapp.com
#_https://discordapp.com
DraftStorez
{"_state": {"539550615072800768": {"timestamp": 1549074553998, "draft": "Good. Meet at the Eastbourne library"}, "_version": 0}
META:https://discordapp.com
#_https://discordapp.com
DraftStore{
{"_state": {"539550615072800768": {"timestamp": 1549074577278, "draft": "Good. Meet at the Eastbourne library "}, "_version": 0}
META:https://discordapp.com
#_https://discordapp.com
DraftStore
{"_state": {"539550615072800768": {"timestamp": 1549074588693, "draft": "Good. Meet at the Eastbourne library and if we m"}, "_version": 0}
META:https://discordapp.com
#_https://discordapp.com
DraftStore
{"_state": {"539550615072800768": {"timestamp": 1549074594238, "draft": "Good. Meet

```

Steve notebook:

URL=https://onedrive.live.com/redir.aspx?cid=2418c0082017486a&resid=2418C0082017486A!105&type=3

The screenshot shows the Autopsy 4.20.0 interface with the following details:

- Case Information:** Case 2 - files - Autopsy 4.20.0
- File System Tree:** Shows a hierarchical view of the file system, including ProgramData, Recovery, Users (with subfolders like Alarms, Default, Desktop, Public, Steve), and various system folders.
- Table View:** A table listing files from the 'Steve' folder. One row is selected: 'Steve's Notebook.url' (Modified Time: 2019-02-01 10:40:55 SGT, Access Time: 2019-02-02 10:39:51 SGT, Size: 288, Location: /Img_Narcos-1.001\vol_vd7\Users\Steve\OneDrive\Documents\Steve's Notebook.url).
- Hex Editor:** Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences.
- Text Editor:** Shows the URL of the selected file: [InternetShortcut] URL=https://onedrive.live.com/redir.aspx?cid=2418c0082017486a&resid=2418C0082017486A!105&type=3
- Analysis Progress:** Analyzing files from Narcos-1.001 (25%)

His shortcuts

Listing										Keyword Lists		Keyword Search		
Keyword search 2 - crayfish1980														
Table										Thumbnail		Summary		
Source Name	S	C	O	Keyword	Keyword Regular Expression	Keyword Preview	Modified Time	Access Time	Change	Save Table as CSV				
data_2				1eastbourne	Eastbourne	e@abt1mzrhvuud!1m2!1seastbourne<%2c+lower+htt...	2019-02-02 10:28:16 SGT	2019-02-02 10:28:48 SGT	2019-02-02 10:28:48 SGT					
2088368e88173d70_0				eastbourne	Eastbourne	nrb8r-9qorrubg&q=eastbourne<library&io=eastbour...	2019-02-02 09:04:36 SGT	2019-02-02 09:04:36 SGT	2019-02-02 09:04:36 SGT					
Shortcuts				eastbourne	Eastbourne	6674ce391d7 eastbor <eastbourne> https://www.google...	2019-02-02 09:05:05 SGT	2019-02-02 10:28:48 SGT	2019-02-02 10:28:48 SGT					
<										>				
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences														
Table omni_box_shortcuts				32 entries	Page 1 of 1									
id	text	fill_into_edit	url		contents	contents...	description	descript...	transition	type	keyword
dcaf0ac-c1... metservice	metservice		https://www.google.com/search?q=metservice&oq=metservice&qs=chrome..0.06.1647j0j8sour...	metservice	0,0	Google Search	0,4	5	7	google.cc				
b93d0af-8... wid patterns	wid patterns		https://www.google.com/search?q=wid+patterns&oq=wid+patterns&qs=chrome..6957j0l5..6824j...	wid patterns	0,0	Google Search	0,4	5	7	google.cc				
dcde1a0-3... truecrypt	truecrypt		https://www.google.com/search?q=truecrypt&oq=truecrypt&qs=chrome..6957j0l5..2538j0j8sour...	truecrypt	0,0	Google Search	0,4	5	7	google.cc				
f84dd10f-7... protonmail	protonmail		https://www.google.com/search?q=protonmail&oq=protonmail&qs=chrome..6957j0l5..2207j0j8sou...	protonmail	0,0	Google Search	0,4	5	7	google.cc				
22fdaad-0... coleman	coleman		https://www.google.com/search?q=cleaner&oq=cleaner&qs=chrome..6957j0l5..2839j0j8sour...	coleman	0,0	Google Search	0,4	5	7	google.cc				
ec4e04c-0... dune 2 online	dune 2 online		https://www.google.com/search?q=dune+2+online&oq=dune+2+online&qs=chrome..6957j0l5..dune 2 online	dune 2 online	0,0	Google Search	0,4	5	7	google.cc				
97a3976a-0... stuff nz	stuff nz		https://www.google.com/search?q=stuff+nz&oq=stuff+nz&qs=chrome..6959j0l5..2235j0j8sour...	stuff nz	0,0	Google Search	0,4	5	7	google.cc				
bb66335c-1... metservice	metservice		https://www.google.com/search?q=metservice&oq=metservice&qs=chrome..0.6959j0l5..1869j0j8s...	metservice	0,0	Google Search	0,4	5	7	google.cc				
65a5f6d-0... windpatterns	windpatterns		https://www.google.com/search?q=windpatterns&oq=windpatterns&qs=chrome..6957j0l5..1615j0...	windpatterns	0,0	Google Search	0,4	5	7	google.cc				
9fb1c32c-0... cric info	cric info		https://www.google.com/search?q=cric+info&oq=cric+info&qs=chrome..6959j0l5..1231j0j8sour...	cric info	0,0	Google Search	0,4	5	7	google.cc				
fbc8e11-3... reddit rugby	reddit rugby		https://www.google.com/search?q=reddit+rugby&oq=reddit+rugby&qs=chrome..6957j0l5..3167j0...	reddit rugby	0,0	Google Search	0,4	5	7	google.cc				
c07d33b2-... google maps	google maps		https://www.google.com/search?q=google+maps&oq=google+maps&qs=chrome..6957j0l5..2455j0...	google maps	0,0	Google Search	0,4	5	7	google.cc				
97a39718-0... crystal meth	crystal meth		https://www.google.com/search?q=crystal+meth&oq=crystal+meth&qs=chrome..6957j0l5..3770j0...	crystal meth	0,0	Google Search	0,4	5	7	google.cc				
1dbbc699-7... drug para	drug para		https://www.google.com/search?q=drug+para&oq=drug+para&qs=chrome..0.6957j0l4.. drug+parapharm...	drug parapharm...	0,0	Google Search	0,4	5	7	google.cc				
2155a5fb-e... gangs nz drugs	gangs nz drugs		https://www.google.com/search?q=gangs+nz+drugs&oq=gangs+nz+drugs&qs=chrome..6957j0l5.. gangs nz drugs	gangs nz drugs	0,0	Google Search	0,4	5	7	google.cc				
de9c183-8... stuff nz	stuff nz		https://www.google.com/search?q=stuff+nz&oq=stuff+nz&qs=chrome..6957j0l5..1566j0j8sour...	stuff nz	0,0	Google Search	0,4	5	7	google.cc				
2396d51-1... metservice	metservice		https://www.google.com/search?q=metservice&oq=metservice&qs=chrome..0.03j0l5..1981j0...	metservice	0,0	Google Search	0,4	5	7	google.cc				
0b72e49-2... cric info	cric info		https://www.google.com/search?q=cric+info&oq=cric+info&qs=chrome..6957j0l5..1287j0...	cric info	0,0	Google Search	0,4	5	7	google.cc				
e58d745e-1... all blacks	all blacks		https://www.google.com/search?q=all+blacks&oq=all+blacks&qs=chrome..6957j0l5..0.2447j0...	all blacks	0,0	Google Search	0,4	5	7	google.cc				
dfc730d7-8... protonmail	protonmail		https://www.google.com/search?q=protonmail&oq=protonmail&qs=chrome..6957j0l5..1769j0j8sou...	protonmail	0,0	Google Search	0,4	5	7	google.cc				

crayfish1980@protonmail.com is Steve's account. Protonmail is a free encrypt mail

Listing Keyword search 1 - Memo Things X Keyword search 2 - Memo Things X Keyword search 3 - secret X Keyword search 4 - package.jpg X Keyword search 5 - package.jpg X Keyword search 8 - crayfish1980 X

/img_Narcos-1/vol_volt7/\$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001

Table Thumbnail Summary Save Table as CSV

Page: 1 of 1 Pages: < > Go to Page: []

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[Current folder]				2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-02 10:39:06 SGT	2019-01-29 03:35:58 SGT	56	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$RIIK1AS.jpg;Zone.Identifier				2019-01-31 10:57:06 SGT	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:57:04 SGT	360	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$RIIK1AS.jpg	▼			2019-01-31 10:57:06 SGT	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:57:04 SGT	19342	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$RA3IE5E.jpg;Zone.Identifier				2019-01-31 10:58:22 SGT	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:58:22 SGT	163	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$RA3IE5E.jpg	▼			2019-01-31 10:58:22 SGT	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:58:22 SGT	118136	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$R5WIK39.jpg;Zone.Identifier				2019-01-31 10:59:38 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:42:46 SGT	2019-01-31 10:59:38 SGT	159	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$R5WIK39.jpg	▼			2019-01-31 10:59:38 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:42:46 SGT	2019-01-31 10:59:38 SGT	86240	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$IIIK1AS.jpg	▼			2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	100	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$IA3IE5E.jpg	▼			2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	120	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy
\$I5WIK39.jpg	▼			2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-02 10:38:06 SGT	2019-02-01 10:48:41 SGT	128	Allocated	Allocated	unknown	/img_Narcos-1/vol_volt7/\$Recy

< >

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

0% 82% 🔍 Reset Tags Menu



- airport crystals.jpg
- dropoff.jpg
- Method run.jpg
- flightbookings.PNG
- airport crystals.jpg:Zone.Identifier
- dropoff.jpg:Zone.Identifier
- flightbookings.PNG:Zone.Identifier
- Method run.jpg:Zone.Identifier

ReferrerUrl=https://cdn.discordapp.com/attachments/539550615072800768/541074665892741121/Steve_K.PNG
HostUrl=https://cdn.discordapp.com/attachments/539550615072800768/541074665892741121/Steve_K.PNG

/img_Narcos-1/vol₁/vol7/Users/Steve/Documents/Misc/flightbookings.PNG:Zone.Identifier

3. What were their future plans and intentions?

-Cutting drugs?

<https://sunrisehouse.com/wp-content/uploads/2016/09/asprin-to-cut-Drugs-with.jpg>

f_00006c	application_store_rating_descriptors_pegi_drugs	descriptors_pegi_hex<application_store_rating_descriptors_... als-they-use-to-cut-drugs-1sp&https://vide-w	Drugs	/img_Narcos-Combined.img/vol_0/vol_7/Users/Steve/AppData/Local/Temp/
WebCacheV01.dat	drugs	.dronedirect.co.uk/www.drugstornewson/www.fas	Drugs	/img_Narcos-Combined.img/vol_0/vol_7/Users/Steve/AppData/Local/Temp/
WebCacheV01.dat	www.drugst	on/search?q=cutting+drugs&source=lnms&tbm=vid	Drugs	/img_Narcos-Combined.img/vol_0/vol_7/Users/Steve/AppData/Local/Temp/
Windows.edb	drugs		Drugs	/img_Narcos-Combined.img/vol_0/vol_7/ProgramData/Micros

- Evidence to show that steve is a drug dealer, have made past deals

Case2-Grp - Autopsy 4.20.0

Case View Tools Window Help

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

Data Sources

- Narcos-Combined.img_1 Host
 - Narcos-Combined.img
 - vol1 (Unallocated; 0:2047)
 - vol1 (Basic data partition: 2048-1023999)
 - vol1 (EFI system partition: 1024000-1226751)
 - vol1 (Microsoft reserved partition: 1226752-1259519)
 - vol1 (Basic data partition: 1259520-6291251)
 - \$OrphanFiles (685)
 - \$Extend (9)
 - \$Deleted (2)
 - \$Recovery.Bin (5)
 - S-1-5-18 (3)
 - S-1-5-21-1474204758-2504895174-1356074821-1000 (3)
 - S-1-5-21-1474204758-2504895174-1356074821-1001 (12)
 - \$UNDLOC (18)
 - Documents and Settings (2)
 - PerfLogs (2)
 - Program Files (21)
 - Program Files (x86) (17)
 - ProgramData (16)
 - Recovery (3)
 - System Volume Information (7)
 - Users (8)
 - Windows (103)
 - volB (Unallocated: 62912512-62914559)

File Views

 - File Types
 - By Extension
 - By MIME Type
 - Deleted Files
 - File System (9951)
 - All (9951)
 - MB File Size
 - Data Artifacts
 - Communication Accounts (20475)
 - Metadata (313)
 - Analysis Results
 - Extension Mismatch Detected (201)
 - Interesting Items (625)
 - Files (625)
 - Keyword Hits (187514)
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
 - Email Addresses (1539)
 - IP Addresses (11809)
 - URLs (174166)
 - OS Accounts
 - Tags
 - Reports

File	File Path
thZY2Q9IF6.jpg	/img_Narcos-Combined.img/vol_vol7/\$OrphanFiles/thZY2Q9IF6.jpg
\$RA3IE5E.jpg	/img_Narcos-Combined.img/vol_vol7/\$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/\$RA3IE5E.jpg
\$RIIK1AS.jpg	/img_Narcos-Combined.img/vol_vol7/\$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/\$RIIK1AS.jpg



4. What was the role of Jane in the case and whether she was guilty as well?

We dk what Jane plays. We will need more evidence such as her laptop image.

Listing								
USB Device Attached								
Table Thumbnail Summary								
Source Name	S	C	O	Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM		0		2019-02-02 10:37:24 SGT		ROOT_HUB	5&2891968b&0	Narcos-Combined.img
SYSTEM		0		2019-02-02 10:37:24 SGT		ROOT_HUB20	5&364b5d6&0	Narcos-Combined.img
SYSTEM		0		2019-02-02 10:37:25 SGT		ROOT_HUB30	5&20be2fd&0&0	Narcos-Combined.img
SYSTEM		0		2019-01-31 11:04:08 SGT	Seagate RSS LLC	Backup Plus Slim Portable Drive 1 TB	MSFT30NA9LP8HF	Narcos-Combined.img
SYSTEM		0		2019-02-02 10:37:25 SGT	VMware, Inc.	Virtual USB Hub	6&30c8ca5f8&0&7	Narcos-Combined.img
SYSTEM		0		2019-02-02 10:37:25 SGT	VMware, Inc.	Virtual USB Hub	6&30c8ca5f8&0&8	Narcos-Combined.img
SYSTEM		0		2019-02-02 10:37:25 SGT	VMware, Inc.	Virtual Mouse	6&30c8ca5f8&0&5	Narcos-Combined.img
SYSTEM		0		2019-02-02 10:37:25 SGT	VMware, Inc.	Virtual Mouse	7&1ffda586&0&0000	Narcos-Combined.img
SYSTEM		0		2019-02-02 10:37:25 SGT	VMware, Inc.	Virtual Mouse	7&1ffda586&0&0001	Narcos-Combined.img
SYSTEM		0		2019-02-01 10:41:46 SGT	Western Digital Technologies, Inc.	Elements Portable (WDBUZG)	57584D3145373444574D314E	Narcos-Combined.img

Using FTK Imager - on memory dump

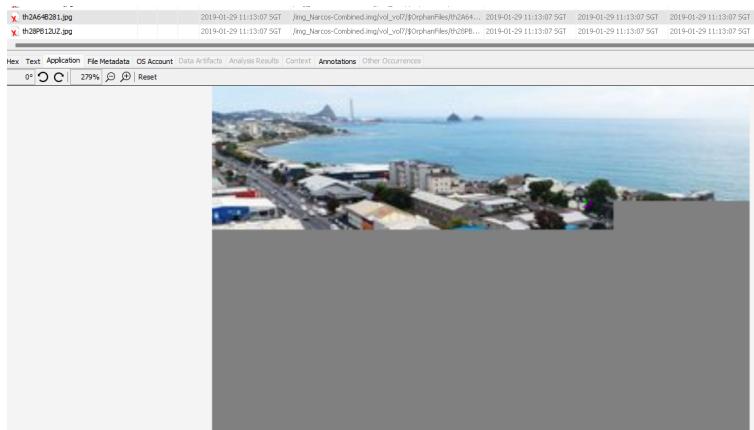
127999870	20 00 00 00 02 00 00 00-01 00 00 00 01 00 00 00
127999880	05 00 00 00 98 00 00 00-7B 22 63 6F 6E 74 65 6E{"conten
127999890	74 22 3A 22 47 6F 6F 64-2E 20 4D 65 65 74 20 61	t":"Good. Meet a
1279998a0	74 20 74 68 65 20 45 61-73 74 62 6F 75 72 6E 65	t the Eastbourne
1279998b0	20 6C 69 62 72 61 72 79-20 61 6E 64 20 69 66 20	library and if
1279998c0	77 65 20 6D 69 73 73 20-65 61 63 68 20 6F 74 68	we miss each oth
1279998d0	65 72 20 63 6F 6D 65 20-74 6F 20 36 36 36 20 52	er come to 666 R
1279998e0	65 77 65 72 61 20 41 76-65 6E 75 65 2C 20 50 65	ewera Avenue, Pe
1279998f0	74 6F 6E 65 2E 22 2C 22-6E 6F 6E 63 65 22 3A 22	tone.", "nonce": "
127999900	35 34 31 30 38 33 30 36-30 35 39 35 30 36 34 38	5410830605950648
127999910	33 32 22 2C 22 74 74 73-22 3A 66 61 6C 73 65 7D	32", "tts": false}
127999920	00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00
127999930	00 00 00 00 01 00 00 00-01 00 00 00 00 00 00 00
127999940	01 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
fla4ddf0	72 65 63 74 2E 63 6F 2E-75 6B 82 0D 77 77 77 2E	rect.co.uk · www.
fla4de00	62 72 69 6D 67 2E 6E 65-74 82 12 77 77 77 2E 62	brimg.net · www.b
fla4de10	75 79 69 74 64 69 72 65-63 74 2E 69 65 82 16 77	uyitdirect.ie · w
fla4de20	77 77 2E 64 72 6F 6E 65-73 64 69 72 65 63 74 2E	ww.dronesdirect.
fla4de30	63 6F 2E 75 6B 82 15 77-77 77 2E 64 72 75 67 73	co.uk · www.drugs
fla4de40	74 6F 72 65 6E 65 77 73-2E 63 6F 6D 82 13 77 77	torenews.com · ww
fla4de50	77 2E 66 61 73 68 69 6F-6E 65 74 74 65 2E 63 6F	w.fashionette.co
fla4de60	6D 82 0D 77 77 77 2E 66-61 73 74 6C 79 2E 69 6F	m · www.fastly.io
fla4de70	82 16 77 77 77 2E 66 75-72 6E 69 74 75 72 65 31	· www.furniture1
fla4de80	32 33 2E 63 6F 2E 75 6B-82 14 77 77 77 2E 6C 61	23.co.uk · www.la

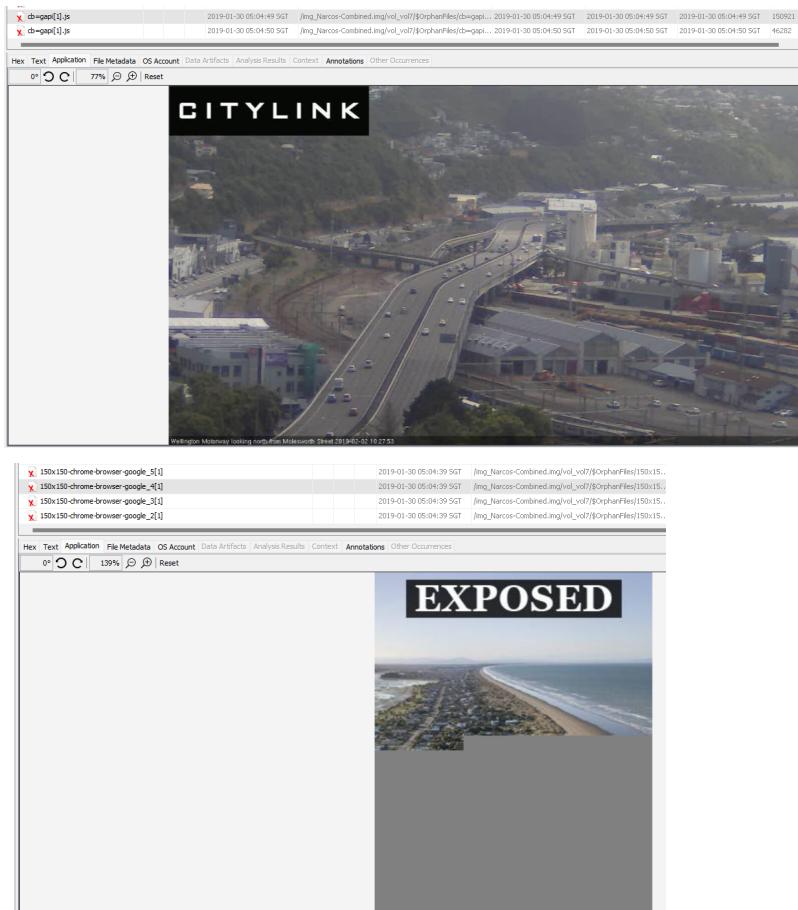
:2521c20 5C 02 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00 00 00 | \.....
:2521c30 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00 00 00 |
:2521c40 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00 00 00 00 |
:2521c50 00 00 00 00 00 00 00 00-00 00 00 00 0A 55 A0 50U P
:2521c60 68 74 74 70 73 3A 2F 2F-77 77 77 2E 67 6F 6F 67 https://www.goog
:2521c70 6C 65 2E 63 6F 6D 2F 61-73 79 6E 63 2F 69 6D 67 le.com/async/img
:2521c80 72 63 3F 65 69 3D 68 32-52 53 58 4A 69 72 4E 4D rc?ei=h2RSXJirNM
:2521c90 47 39 39 51 50 76 6A 62-37 34 42 67 26 79 76 3D G99QPvjb74Bg&yv=
:2521ca0 33 26 69 61 63 74 3D 72-63 26 76 65 64 3D 30 61 3&iact=rc&ved=0a
:2521cb0 68 55 4B 45 77 6A 59 69-75 69 7A 67 35 66 67 41 hUKEwjYiuizg5fgA
:2521cc0 68 58 42 58 6E 30 4B 48-65 2D 47 44 32 38 51 4D hXBXnOKHe-GD28QM
:2521cd0 77 68 63 4B 42 51 77 46-41 26 76 65 74 3D 31 30 whcKBQwFA&vet=10
:2521ce0 61 68 55 4B 45 77 6A 59-69 75 69 7A 67 35 66 67 ahUKEwjYiuizg5fg
:2521cf0 41 68 58 42 58 6E 30 4B-48 65 2D 47 44 32 38 51 AhXBXnOKHe-GD28Q
:2521d00 4D 77 68 63 4B 42 51 77-46 41 2E 2E 69 26 69 6D MwhcKBQwFA..isim
:2521d10 67 72 74 3D 30 26 71 3D-67 61 6E 67 73 2B 6E 7A grt=0&q=gangs+nz
:2521d20 2B **64** 72 75 67 73 26 69-6D 67 75 72 6C 3D 68 74 +drugs
:2521d30 74 70 73 3A 2F 2F 77 77-77 2E 72 61 64 69 6F 6E tps://www.radion
:2521d40 7A 2E 63 6F 2E 6E 7A 2F-61 73 73 65 74 73 2F 6E z.co.nz/assets/n
:2521d50 65 77 73 5F 63 72 6F 70-73 2F 35 39 30 33 35 2F ews_crops/59035/
:2521d60 65 69 67 68 74 5F 63 6F-6C 5F 70 61 74 63 68 65 eight_col_patche
:2521d70 73 5F 63 72 70 2E 6A 70-67 3F 31 35 32 38 35 37 s_crp.jpg?152857
:2521d80 38 36 32 37 26 69 6D 67-72 65 66 75 72 6C 3D 68 8627
:2521d90 74 74 70 73 3A 2F 2F 77-77 77 2E 72 61 64 69 6F https://www.radio
:2521da0 6E 7A 2E 63 6F 2E 6E 7A-2F 6E 61 74 69 6F 6E 61 nz.co.nz/nationa
:2521db0 6C 2F 70 72 6F 67 72 61-6D 6D 65 73 2F 69 6E 73 l/programmes/ins
:2521dc0 69 67 68 74 2F 61 75 64-69 6F 2F 32 30 31 38 36 ight/audio/20186
:2521dd0 34 38 34 36 34 2F 69 6E-73 69 67 68 74 2D 66 75 48464/insight-fu
:2521de0 74 75 72 65 2D 6F 66 2D-67 61 6E 67 73 26 74 62 ture-of-gangs&tb
:2521df0 6E 69 64 3D 53 74 46 34-71 72 74 34 30 4E 78 59 nid=StF4qrt4ONXY
:2521e00 33 4D 3A 26 64 6F 63 69-64 3D 73 76 75 55 38 76 3M:**adocid**=svuU8v
:2521e10 4F 45 6F 36 46 33 4C 4D-26 75 61 63 74 3D 33 26 OEo6F3LM&uact=3&
:2521e20 69 63 74 78 3D 31 26 63-73 69 3D 56 4A 53 2E 30 ictx=1&csci=VJS.0
:2521e30 2C 56 4F 53 2E 34 26 72-69 3D 32 30 26 62 69 68 ,VOS.4&ri=20&bih
... y·ù·c·y·z·A·r·...@·e·...,)N·O·...·B·C·...I·...2¥·?·gi·}·...`·...
·ù·R·\$u2·ÿÇ(ù·ÿÇYúo·Öe··ÓY·üT··https://securepubads.g.doubleclick.net/gampad/ad
s?gdfp_req=1&pvnid=3257724645068240&correlator=1436628257927774&output=json_html
&callback=googletag.impl.pubads.callbackProxy6&impl=fif&adsid=NT&eid=21062414%2C
21062420&vrg=299&guci=2.2.0.0.2.2.0.0&plat=1%3A32776%2C2%3A32776&sc=1&sfv=1-0-31
&iu=%2F56091333%2Fquartz%2Farticle&sz=640x363%7C640x380%7C300x600%7C970x253&scp=permanentId%3Dfc2b9e223dd54abf76ee76c77804180be37d%26sessionId%3D797635a01955b9d93eacf51d56a11d207800%26obsession%3Dhow-we-buy%26topic%3Dfinance-and-economics%26tags%3Donline-drug-trade%252Ctor-browser%252Ccrystal-meth%252Cdread-pirate-roberts%252Cross-ulbricht%252Cecstasy%252Cmethamphetamine%252Cdma%252Cillegal-drugs%252Cdrug-trade%252C1sd%252Cdark-web%252Cblack-market%252Cnarcotics%252Ccocaine%252Csilk-road%252Cherooin%252Cmarijuana%252Cdrugs%252Ccryptocurrency%252Cbitcoin%26wpid%3D481037%26tile%3D8%26split%3Da%26entryTopic%3Dfinance-and-economics%26entryObsession%3Dhow-we-buy%26adType%3Dinline%26contentId%3D481037&cookie=ID%3D8c91607fe51d5884%3AT%3D1549069036%3AS%3DALNI_MYY9Gwp38xAL_w2MsV1WFpNf95gbw&cookie_enabled=1&bc=15&abxe=1&lmt=1549069068&dt=1549069068781&dlt=1549069034881&idt=1322&frm=20&biw=1899&bih=816&oid=3&adx=800&ady=6954&adk=448747667&uci=6&ifi=6&u_tz=780&u_his=3&u_h=927&u_w=1916&u_ah=887&u_aw=1916&u_cd=24&u_nplug=3&u_nmime=4&u_sd=1&flash=0&url=https%3A%2F%2Fqz.com%2F481037%2Fdark-web%2F&ref=https%3A%2F%2Fwww.google.com%2F&dz=40&icsg=9345915855360&std=0&vis=1&dmc=4&scr_x=0&scr_y=6229&psz=620x-1&msz=620x-1&blev=1&bisch=1&psts=CjoItJ6NlxJA9ZMVWL2JrbASW0ZN2LASeAHoAb68v40DBIAChcGiGoAC_cGiGoAC88v581CAAvtL-fJQ%2CCkAI5du-mBJAmf6rsgFI3csUWL2JrbASW0zN2LASeAHoAzjX-oSDBIACChcGiGoAC_cGiGoAC88v581CAAvtL-fJQ%2CCjоItJ6NlxJA9ZMVWL2JrbASW0zN2LASeAHoAdmHmYSDBIACChcGiGoAC_cGiGoAC88v581CAAvtL-fJQ&ga_vid=608109901.1549069036&ga_sid=1549069036&ga_hid=2017045959&fws=4

<a href="https://securepubads.g.doubleclick.net/gampad/ads?gdfp_req=1&pvsid=3257724645068240&correlator=1436628257927774&output=json_html&callback=googletag.impl.pubads.callbackProxy8&impl=fif&adsid=NT&eid=21062414%2C21062420&vrg=299&uci=2.2.0.0.2.2.0.0&plat=1%3A32776%2C2%3A32776&sc=1&sfv=1-0-31&iu=%2F56091333%2Fquartz%2Farticles&sz=640x363%7C640x380%7C300x600%7C970x253&scp=permanentId%3Dfc2b9e223dd54abf76ee76c77804180be37d%26sessionId%3D797635a01955b9d93eacf51d56a11d207800%26obsession%3Dhow-we-buy%26topic%3Dfinance-and-economics%26tags%3Donline-drug-trade%252Cto r-browser%252Ccrystal-meth%252Cdread-pirate-roberts%252Cross-ulbricht%252Cecstasy%252Cmethamphetamine%252Cmdma%252Cillegal-drugs%252Cdrug-trade%252Cldsd%252Cdark -web%252Cblack-market%252Cnarcotics%252Ccocaine%252Csilk-road%252Cherooin%252Ccan nabis%252Cmarijuana%252Cdrugs%252Ccryptocurrency%252Cbitcoin%26pid%3D481037%26t ile%3D10%26split%3Da%26entryTopic%3Dfinance-and-economics%26entryObsession%3Dhow -we-buy%26adType%3Dinline%26contentId%3D481037&cookie=ID%3D8c91607fe51d5884%3AT%3D1549069036%3AS%3DALNI_MYY9Gwp38xAL_wZMsvlWFpNf95gbw&cookie_enabled=1&bc=15&abx e=1&lmt=15490690797&dt=1549069079918&dlt=1549069034881&idt=1322&frm=20&biw=1899&b ih=816&oid=3&adx=800&ady=9390&adk=3849631498&uci=8&ifi=8&u_tz=780&u_his=3&u_h=927&u_w=1916&u_ah=887&u_aw=1916&u_cd=24&u_nplug=3&u_nmime=4&u_sd=1&flash=0&url=https%3A%2F%2Fqz.com%2F481037%2Fdark-web%2F&ref=https%3A%2F%2Fwww.google.com%2F&ds z=40&icsg=9345915855360&std=0&vis=1&dmc=4&scr_x=0&scr_y=8629&psz=620x-1&msz=620x -1&blev=1&bisch=1&psts=CjoItJ6N1xJA9ZMVWL2JrbASW0zN2LASEAHoAb68v40DBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCjoIyvfqkJRA9ZMVWL2JrbASW0zN2LASEAHoAfa-v40DBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCkAI5du-mBJAmf6rsgFI3csUWL2JrbASW0zN2LASEAHoAZjX-osDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCjoItJ6N1xJA9ZMVWL2JrbASW0zN2LASEAHoAdmHmYSDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCjoItJ6N1xJA9ZMVWL2JrbASW0zN2LASEAHoAeHPp4SDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ&ga_vid=608109901.1549069036&ga_sid=1549069036&ga_hid=2017045959&fws=4.....ÉÉýüüüý++ý++ý++ý++ý+.....</p>

Listing						
Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles						
Table: Thumblnk_Summary						
Name	S	C	O	Modified Time	Location	Change Time
trans[3].gif				2019-01-30 04:59:19.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\trans[3].g	2019-01-30 04:59:19.507
trans[2].gif				2019-01-30 04:59:20.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\trans[2].g	2019-01-30 04:59:20.507
trans[1].gif				2019-01-30 04:59:19.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\trans[1].g	2019-01-30 04:59:19.507
tooth[1].js				2019-01-29 12:20:17.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\tooth[1].js	2019-01-29 12:20:17.507
title-image[1].jpg				2019-01-29 12:20:19.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\title-image[1].jpg	2019-01-29 12:20:19.507
title-image[1].png				2019-01-29 12:20:36.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\title-image[1].png	2019-01-29 12:20:36.507
thankyou-avenger[1].htm				2019-01-30 05:05:10.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\thankyou-avenger[1].htm	2019-01-30 05:05:10.507
thankyou1.htm				2019-01-30 05:05:10.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\thankyou1.htm	2019-01-30 05:05:10.507
tiny29QF5.jpg				2019-01-29 11:13:07.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\tiny29QF5.jpg	2019-01-29 11:13:07.507
tiny29ZCQZ.jpg				2019-01-29 11:13:07.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\tiny29ZCQZ.jpg	2019-01-29 11:13:07.507
tinyX002QJ.jpg				2019-01-29 11:13:07.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\tinyX002QJ.jpg	2019-01-29 11:13:07.507
tinyYDFOG.jpg				2019-01-29 11:13:07.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\tinyYDFOG.jpg	2019-01-29 11:13:07.507
tinyYDFOG.htm				2019-01-29 11:13:07.507	Jing_Narcos-Combined.mpg vol_0 0 OrphanFiles\tinyYDFOG.htm	2019-01-29 11:13:07.507







\USERS\STEVE\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTEdge_8WEKYB3D8BBWE\AC\#!001\MICROSOFTEdge\CACHE\9ANASQ89\OSD[1].JS

Case2-Grp - Autopsy 4.20.0

Case View Tools Window Help

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

Data Sources

- Narcos-Combined.img_1 Host
 - Narcos-Combined.img
 - vol1 (Unallocated: 0-2047)
 - vol5 (Basic data partition: 2048-1023999)
 - vol5 (EFI system partition: 1024000-126751)
 - vol6 (Microsoft reserved partition: 1268752-1259519)
 - vol7 (Basic data partition: 1259520-62912511)
 - \$Orphaned files (685)
 - Extend (9)
 - *Deleted (2)
 - *\$RawMetadata (8)
 - \$Recycle.Bin (5)
 - S-1-5-18 (3)
 - S-1-5-21-1474204758-250-4895174-1356074821-1000 (3)
 - S-1-5-21-1474204758-250-4895174-1356074821-1001 (12)
 - \$Unalloc (18)
 - Documents and Settings (2)
 - PerfLogs (2)
 - Program Files (21)
 - Program Files (x86) (17)
 - ProgramData (16)
 - Recovery (3)
 - System Volume Information (7)
 - Users (8)
 - Windows (103)
 - vol8 (Unallocated: 62912512-62914559)

File Views

 - File Types
 - By Extension
 - By MIME Type
 - Deleted File
 - File System (9951)
 - All (9951)
 - MB File Size
 - Data Artifacts
 - Communication Accounts (20475)
 - Metadata (313)
 - Analysis Results
 - Extension Mismatch Detected (201)
 - Interesting Items (625)
 - Files (625)
 - Keyword Hits (187514)
 - Single Literal Keyword Search (0)
 - Single Regular Expression Search (0)
 - Email Addresses (1539)
 - IP Addresses (11809)
 - URLs (174166)
 - OS Accounts
 - Tags
 - Reports

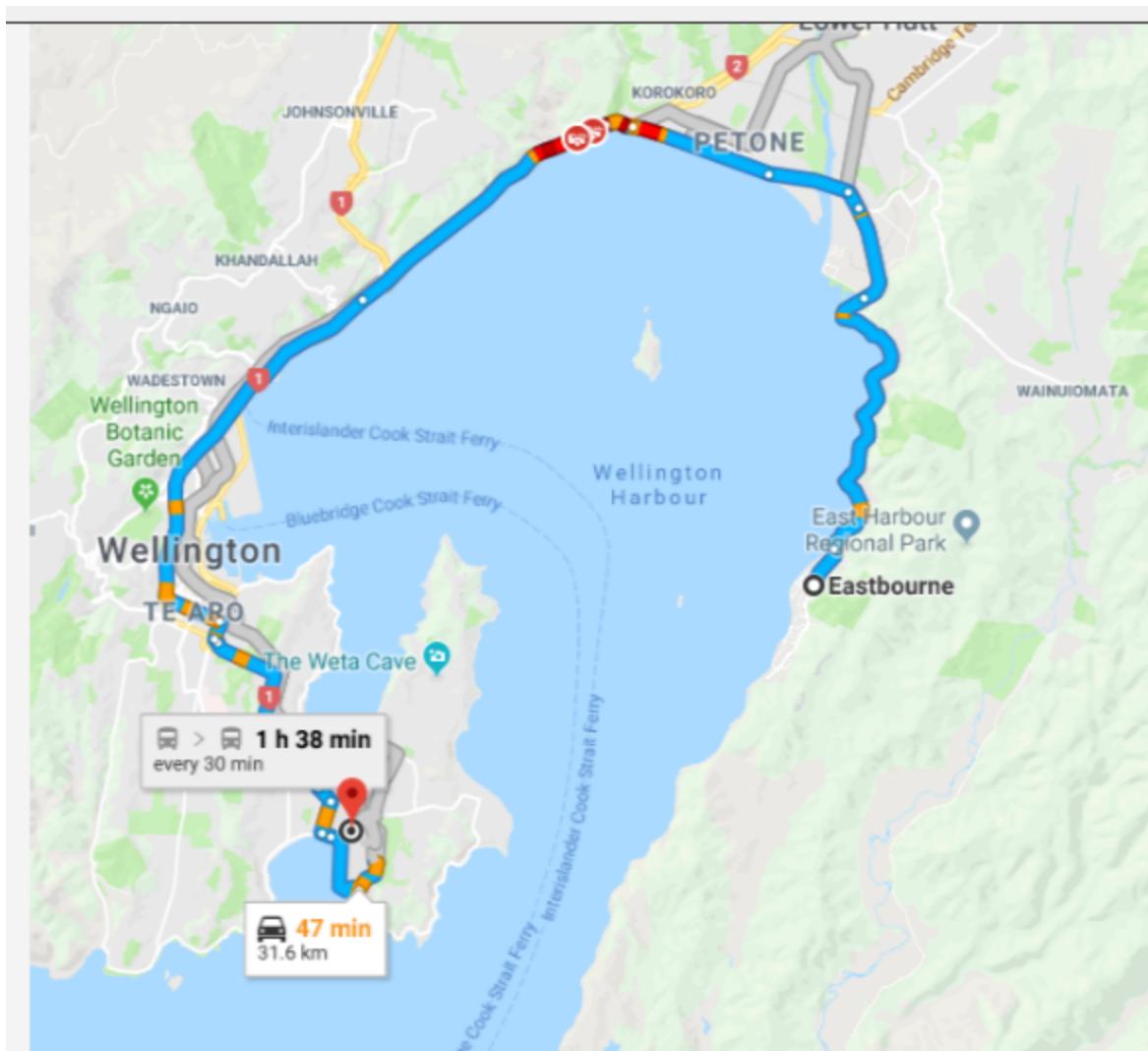
Listing /Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-21-1474204758-250-4895174-1356074821-1001

Table Thumbnail Summary

Name	S	C	O	Modified Time	Location	Change Time	Access Time	Created Time
desktop.ini				2019-01-29 03:35:58 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-01-29 03:35:58 SGT	2019-02-02 10:38:55 SGT	2019-01-29 03:35:58 S...
[parent folder]				2019-01-30 04:58:41 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-01-30 04:58:41 SGT	2019-02-01 10:48:41 SGT	2018-09-15 15:33:50 S...
[current folder]				2019-02-01 10:48:41 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-02-02 10:38:06 SGT	2019-01-29 03:35:58 S...
\$RDIK1AS.jpg;Zone.Identifier				2019-01-31 10:57:06 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:57:04 S...
\$RDIK1AS.jpg				2019-01-31 10:57:06 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:57:04 S...
\$RA3IE5.jpg;Zone.Identifier				2019-01-31 10:58:22 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:58:22 S...
\$RA3IE5.jpg				2019-01-31 10:58:22 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-01-31 11:04:13 SGT	2019-01-31 10:58:22 S...
\$RSWIK39.jpg;Zone.Identifier				2019-01-31 10:59:38 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-02-01 10:42:46 SGT	2019-01-31 10:59:38 S...
\$RSWIK39.jpg				2019-01-31 10:59:38 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-02-01 10:42:46 SGT	2019-01-31 10:59:38 S...
\$IIK1AS.jpg				2019-02-01 10:48:41 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 S...
\$IA3IE5.jpg				2019-02-01 10:48:41 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 SGT	2019-02-01 10:48:41 S...
\$I5WIK39.jpg				2019-02-01 10:48:41 SGT	/Img_Narcos-Combined.img/vol_volt/\$Recycle.Bin/S-1-5-2...	2019-02-01 10:48:41 SGT	2019-02-02 10:38:06 SGT	2019-02-01 10:48:41 S...

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

0% 77% | Reset



Listing

Methamphetamine

Table | Thumbnail | Summary

Page: 1 of 1 Pages: < > Go to Page: []

Source Name	Keyword	S	C	O	Keyword Regular Expression	Keyword Preview	Modified Time
000003.log	methamphetamine.jpgw				Methamphetamine	e04-image01-what-is-<methamphetamine.jpgw< xuht...	2019-01-31 1C
000003.log	methamphetamine.jpg				Methamphetamine	e04-image01-what-is-<methamphetamine.jpg<url:{https://...}	2019-01-31 1C
13485dbed5111290_0	methamphetamine				Methamphetamine	ixwep10w3qcydata["<methamphetamine>","https://www.g...	2019-01-31 1C
13485dbed5111290_0	u003dmethamphetamine				Methamphetamine	6887f2f9510bu0026q<u003dmethamphetamine<u0026s...	2019-01-31 1C
3a6897da1e20e5f6_0	7cmethamphetamine				Methamphetamine	-ulbricht%7cectasy%<7cmethamphetamine<%7cmdna%...	2019-02-02 0E
BrowserMetrics-5C50C033-26A0.pma-slack	methamphetamine.jpgcache				Methamphetamine	e04-image01-what-is-<methamphetamine.jpgcache<contr...	2019-01-30 0E
DragVisualUserControl2.xbf	7cmethamphetamine				Methamphetamine	-ulbricht%7cectasy%<7cmethamphetamine<%7cmdna%...	2019-01-30 0E
History	methamphetamine				Methamphetamine	almeth.html what is <methamphetamine> what is crystal me	2019-02-02 1C
History Provider Cache	methamphetamine				Methamphetamine	tsdrugcrystalmeth<methamphetamine><usedwhathmsisch	2019-02-02 1C
Unalloc_280525_10081198080_14450704384	methamphetamine				Methamphetamine	eneric term(noun) <methamphetamine> methamphetamine...	0000-00-00 0C
Unalloc_280525_10081198080_14450704384	methamphetamine.jpgcache				Methamphetamine	e04-image01-what-is-<methamphetamine.jpgcache<contr...	0000-00-00 0C
Unalloc_280525_10081198080_14450704384	methyleneoxideymethamphetamine				Methamphetamine	crystal x hug drug <methyleneoxideymethamphetamine> (g...	0000-00-00 0C
Unalloc_280525_544890624_10077200384	2cmethamphetamine				Methamphetamine	rning%2cmany%2cbail%2cmethamphetamine<%2cdistic...	0000-00-00 0C
Unalloc_280525_544890624_10077200384	2cmethamphetamine				Methamphetamine	hing%2cmany%2cbail%2cmethamphetamine<%2cdistic...	0000-00-00 0C

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

Strings Indexed Text Translation

Page: 1 of 1 Page < > Matches on page: 1 of 1 Match < > 100% Reset

```
url("https://www.drugfreeworld.org/sites/default/files/imagecache/gcu_inline_default/page04-image01-what-is-methamphetamine.jpg") timestampN
(url("https://www.drugfreeworld.org/sites/default/files/imagecache/gcu_inline_default/page04-image01-what-is-methamphetamine.jpg
(url("https://www.drugfreeworld.org/sites/default/files/imagecache/gcu_inline_default/page04-image01-what-is-methamphetamine.jpg
(url("https://www.drugfreeworld.org/sites/default/files/imagecache/gcu_inline_default/page04-image01-what-is-methamphetamine.jpgw") xu
https://www.drugfreeworld.org/FURL/imagecache/cropfit=w=992@cr=305,0,783,799@qa=85/data/www.thewaytohappiness.org/files/mobile-menu-background.jpg
url"
https://www.drugfreeworld.org/FURL/imagecache/cropfit=w=992@cr=305,0,783,799@qa=85/data/www.thewaytohappiness.org/files/mobile-menu-background.jpg" timestampN
https://www.drugfreeworld.org/FURL/imagecache/cropfit=w=992@cr=305,0,783,799@qa=85/data/www.thewaytohappiness.org/files/mobile-menu-background.jpg
https://www.drugfreeworld.org/FURL/imagecache/cropfit=w=992@cr=305,0,783,799@qa=85/data/www.thewaytohappiness.org/files/mobile-menu-background.jpg
https://www.drugfreeworld.org/FURL/imagecache/cropfit=w=992@cr=305,0,783,799@qa=85/data/www.thewaytohappiness.org/files/mobile-menu-background.jpg@.
https://www.drugfreeworld.org_@1
sw-toolbox.html-cache
store
timestamp
```

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

Strings Indexed Text Translation

Page: 1 of 1 Page < > Go to Page: []

```
<!DOCTYPE html>
<html lang="en" xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
<meta charset="utf-8"/>
<link rel="stylesheet" type="text/css" href="ms-appx-web:///Assets/ErrorPages/phishSiteStyles.css">
<link rel="stylesheet" type="text/css" href="PhishSiteStyles.css">
<title>Reported Unsafe Website: Navigation Blocked</title>
<script language="javascript" type="text/javascript">
// Localized strings used by phishsite.js.
var L_PhishingThreat_TEXT = "Phishing threat: This is a phishing website that impersonates a trusted website to trick you into revealing personal or financial information.";
+++
var L_MalwareThreat_TEXT = "Malicious software threat: This site contains links to viruses or other software programs that can reveal personal information stored or typed on your computer to malicious persons.";
+++
var L_ContentUnsafe_TEXT = "Content on this website has been reported as unsafe";
var L_Content_TEXT = "Hosted by: ";
// Localized strings used by httpErrorPagesScripts.js.
var L_MOREINFO_TEXT = "More information";
<script>
<script src="ms-appx-web:///Assets/ErrorPages/ErrorPageScripts.js" language="javascript" type="text/javascript">
</script>
<script src="ms-appx-web:///Assets/ErrorPages/httpErrorPagesScripts.js" language="javascript" type="text/javascript">
</script>
<script src="ms-appx-web:///Assets/ErrorPages/phishsite.js" language="javascript" type="text/javascript">
</script>
<script language="javascript" type="text/javascript">
function expandCollapsePhish(elem, changeImage) {
+++++
if (document.getElementById) {
+++++
ecBlock = document.getElementById(elem);
+++++
elemImage = document.getElementById(elem + "Span");
if (ecBlock != undefined && ecBlock != null) {
var displayValue = getDisplayValue(ecBlock);
if (displayValue == "none" || displayValue == null || displayValue == "") {
+++++
//shows the info.
```

Name	S	C	O	Modified Time	Location	Change Time	A
403-8.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-7.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-6.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-5.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-4.htm				0000-00-00 00:00:00	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	0000-00-00 00:00:00	0000-00-00 00:00:00
403-4.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-3.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-2.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-19.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-18.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-17.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-16.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT
403-15.htm	▼			2018-09-15 17:08:30 SGT	/img_Narcos-Combined.img/vol_volt7/Windows/Win5xS/am...	2019-01-30 00:07:11 SGT	2018-09-15 17:08:30 SGT

The screenshot shows a NetworkMiner interface with the following details:

- Tab bar: Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences.
- Sub-tab bar: Strings, Indexed Text, Translation.
- Search bar: Page: 35 of 74 Page, Matches on page: 1 of 2 Match, 100%, Reset.
- Text area:
 - URI: `_keyhttps://www.google.com/search?q=best+places+to+trade+drugs&oq=best+places+to+trade+drugs&aq=chrome..69|57.5131j0j8&sourceid=chrome&ie=UTF-8`
 - Host: `https://google.com/$`
 - ABut1
 - (@:@
 - (@`@
 - (@`@
 - RCRD(
 - (@`@

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings	Indexed Text	Translation							
Page: 1 of 1 Page	Matches on page: 1 of 1 Match	100%	<input type="button" value="Reset"/>						Text Source: Search Results

KnownGameList.bin	gunsoficarusonline.exe
KnownGameList.bin	guns
KnownGameList.bin	guns
KnownGameList.bin	guns
Layout.ini	malgunsl.ttf
M1033Zira.APM	c6d4gunsxjmts
M1033Zira.APM	c6d4gunsxjmts
MMCEEx.dll	1verbrunningstatechangedactionrunningstatech
MMCEEx.dll	1verbrunningstatechangedactionrunningstatech
MMCEEx.ni.dll	microsoft.managementconsole.internalisnapinfa
MMCEEx_ni.dll	microsoft.managementconsole.internalsnapinfa

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotati
Strings	Indexed Text	Translation						
Page: 3 of 7 Page			Matches on page: 1 of 2 Match			100%		

Guns Gore and Cannoli
5653f90f-d3ee-4ccd-8020-0709a0911dae
1879915684x
ggpofba-ng.exe
06d597e0-e87a-4a67-874b-7d7a1f2d83da
ggsx.exe
bb8b6d78-2871-418e-97b3-d936948572c0
1999637053
gx2.exe
Guilty Gear X2 Reload
d1b61fca-8628-4690-ae1c-98b92f60b917
2021376788
ggxxacpr_win.exe
a4dbf73d-2f4d-47cd-98ea-d2e929b5118b
2142662139
gh.exe
green hell

7/4/2023

The screenshot shows a timeline of file system activity. The left sidebar has checkboxes for 'File System' (selected) and 'Web Activity'. The timeline table lists events such as file access, creation, modification, and program runs. The bottom section shows search and filter options.

Date	Event	Details
2019-02-01 08:23:53	_B_	/Users/Steve/AppData/Local/Packages/Microsoft ... 18c0082017486a_LiveId/OneNote/Documents_en-NZ
2019-02-01 08:23:53	_B_	/Users/Steve/AppData/Local/Packages/Microso ... 69E6BD54B0_69CE0147E140D3C4B84FD217A2DD371
2019-02-01 08:23:54	Program Run	CONSENT.EXE : Prefetch File
2019-02-01 08:23:54	_B_	/Users/Steve/AppData/Local/Packages/Microsoft.S ... zg5c/LocalStorage/VerboseDBFlag.data
2019-02-01 08:23:54	_B_	/Users/Steve/AppData/Local/Packages/Microsoft. ... /AppData/Local/OneNote/16.0/cache/00000005.bin
2019-02-01 08:23:54	_B_	/Users/Steve/AppData/Local/Packages/Microsoft. ... /AppData/Local/OneNote/16.0/cache/00000004.bin

copy 4.20.0

down Help

The screenshot shows a file tree on the left and a table on the right. The file tree includes 'Microsoft.NET.Native.Framework.2.2_8w', 'Microsoft.NET.Native.Runtime.1.6_8wek', 'Microsoft.NET.Native.Runtime.1.7_8wek', 'Microsoft.NET.Native.Runtime.2.1_8wek', 'Microsoft.NET.Native.Runtime.2.2_8wek', 'Microsoft.Office.OneNote_8wekyb3d8bb', and various AppData and LocalState folders. The table lists files under 'OneNote (4)' and their details.

Name	S	C	O	Modified Time	Change Time
[current folder]				2019-02-01 08:25:45 SGT	2019-02-01 08:25:45 SGT
[parent folder]				2019-02-01 08:25:59 SGT	2019-02-01 08:25:59 SGT
{6B138A6F-8C4C-44C8-8E48-C9DAD2AF0A13}{12}.db	▼			2019-02-01 08:25:45 SGT	2019-02-01 08:25:45 SGT
{6B138A6F-8C4C-44C8-8E48-C9DAD2AF0A13}{12}.db				2019-02-01 08:25:45 SGT	2019-02-01 08:25:45 SGT
{6B138A6F-8C4C-44C8-8E48-C9DAD2AF0A13}{14}.db				2019-02-01 08:25:45 SGT	2019-02-01 08:25:45 SGT
{6B138A6F-8C4C-44C8-8E48-C9DAD2AF0A13}{14}.db				2019-02-01 08:25:45 SGT	2019-02-01 08:25:45 SGT

At the bottom, there is a table titled 'Entities' with columns: rowid, EntityType, EntityGID, EntityName, and RootRev... . It contains three entries:

rowid	EntityType	EntityGID	EntityName	RootRev...
2	4	{6B138A6F-8C4C-44C8-8E48-C9DAD2AF0A13}{12}	Steve's Notebook	22
3	2	{6B138A6F-8C4C-44C8-8E48-C9DAD2AF0A13}{16}	Quick Notes	22
4	1	{6B138A6F-8C4C-44C8-8E48-C9DAD2AF0A13}{18}	Stego	22

Possibly a read into steves notebook

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

Listing Keyword search 1 - Memo Things Keyword search 2 - Memo Things Keyword search 3 - secret

/Img_Narcos-1\vol_0\Users\Steve\AppData\Local\Packages\Microsoft.Office.OneNote_8wekyb3d8bbwe\LocalState\AppData\Local\OneNote\16.0\cache

Table Thumbnail Summary

Page: 1 of 1 Pages: < > Go to Page: []

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)
[parent folder]				2019-02-01 08:25:59 SGT	2019-02-01 08:25:59 SGT	2019-02-01 08:25:59 SGT	2019-02-01 08:23:32 SGT	56	Allocated	Allocated
tmp				2019-02-01 08:25:59 SGT	2019-02-01 08:25:59 SGT	2019-02-01 08:25:59 SGT	2019-02-01 08:23:33 SGT	48	Allocated	Allocated
00000001.bin				2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:23:33 SGT	8192	Allocated	Allocated
00000002.bin				2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:23:33 SGT	4096	Allocated	Allocated
00000003.bin				2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:23:33 SGT	20480	Allocated	Allocated
00000004.bin				2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:23:48 SGT	20480	Allocated	Allocated
00000005.bin				2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:23:54 SGT	8192	Allocated	Allocated
00000006.bin				2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:24:48 SGT	32768	Allocated	Allocated
header				2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:26:04 SGT	2019-02-01 08:23:33 SGT	72	Allocated	Allocated

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

Strings Indexed Text Translation

Page: 1 of 1 Page: < > Matches on page: - of - Match: < > 100% |||| Reset

PageDateTime
 Calibri
 Steve Kovhai
 PageTitle
 Calibri Light
 Steve Kovhai
 §{44
 Steve Kovhai
 ylaHK
 c 6{3
 BJ
 c 6{3
 Friday, 1 February 2019
 1:24 PM
 §{44
 DVG
 ylaHK
 Steve Kovhai
 c 6{3
 Stego
 Stego
 DVG
 Steve Kovhai
 PageTitle
 Calibri Light
 Friday, 1 February, 2019.

Combi image?

Keyword search Table Thumbnail Summary

Save Table as

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time
Recent Documents Artifact	e:\Downloads\Misc\xpackage.jpg<Path ID : -1Date	/Img_Narcos-1\vol_0\Users\Steve\NTUSER.DAT	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
RegRipper /Img_Narcos-1\vol_0\Users\Steve\NTUSER.DAT	e:\Downloads\Misc\xpackage.jpg<[0]24LMN > [3]0	RegRipper /Img_Narcos-1\vol_0\Users\Steve\NTUSER.DAT	2019-02-02 10:39:26 SGT	2019-02-02 10:39:26 SGT	2019-02-02 10:39:
Web History Artifact	e:\Downloads\Misc\xpackage.jpg<Date Accessed : 2019...>	/Img_Narcos-1\vol_0\Users\Steve\AppData\Local\Micros...	2019-02-02 10:39:26 SGT	2019-02-02 10:39:26 SGT	2019-02-02 10:39:
Recent Documents Artifact	e:\Downloads\Misc\xpackage.jpg<Path ID : -1Date	/Img_Narcos-1\vol_0\Users\Steve\AppData\Roaming\Mi...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
WebCacheV01.dat	e:\Downloads\Misc\xpackage.jpg<1SP51SP5Visited:	/Img_Narcos-1\vol_0\Users\Steve\AppData\Local\Micros...	2019-02-02 10:39:26 SGT	2019-02-02 10:39:26 SGT	2019-02-02 10:39:
No preferred path found.lnk	e:\Downloads\Misc\xpackage.jpg>+RXL2C1\Users\She...	/Img_Narcos-1\vol_0\Users\Steve\AppData\Roaming\Mi...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
package.lnk	b2EG package.lnkH <package.jpg>C:\Users\Steve\Down...	/Img_Narcos-1\vol_0\Users\Steve\AppData\Roaming\Mi...	2019-02-01 10:50:22 SGT	2019-02-01 10:50:22 SGT	2019-02-01 10:50:
SystemIndex.4.gthr	e:\Downloads\Misc\xpackage.jpg> 800000c 2 ...	/Img_Narcos-1\vol_0\Programdata\Microsoft\Search\Da...	2019-02-01 10:50:28 SGT	2019-02-01 10:50:28 SGT	2019-02-01 10:50:
5f7b5f1e01b83767,automaticDestinations-ms	e:\Downloads\Misc\xpackage.jpg>+RXL2C1\ULC\Users<...	/Img_Narcos-1\vol_0\Users\Steve\AppData\Roaming\Mi...	2019-02-02 10:28:44 SGT	2019-02-02 10:28:44 SGT	2019-02-02 10:38:
package.jpg.lnk	b2EG package.lnkH <package.jpg>C:\Users\Steve\Down...	/Img_Narcos-1\vol_0\Users\Steve\AppData\Roaming\Mi...	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

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

Strings Indexed Text Translation

Page: 1 of 1 Page: < > Matches on page: 1 of 1 Match: < > 100% |||| Reset

Text Source: Search Results

systemindex.4.gthr f00db621d4b9c2 file:C:\Users\Steve\Downloads\BNE.png,crdownload 800000c 0 65535 4294967295 4294967295 1 4294967295 1000
52cc1311 1d4b9d7 400000f 0 0 65535 4294967295 4294967295
53482d95 1d4b9d7 40000016 0 0 65535 4294967295 4294967295
e3d02526 1d4b9d8 file:C:\Users\Steve\Downloads\Misc\xpackage.jpg 800000c 2 80041201 1 4294967295 1004

METADATA

Other interesting findings

Listing Keyword search 1 - Memo Things X Keyword search 2 - Memo Things X Keyword search 3 - secret X Keyword search 4 - package.jpg X Keyword search 5 - package.jpg X Keyword search 8 - crayfish1980 ... /img_Narcos-1/vol_volt/\$CarvedFiles/2

Table | Thumbnail | Summary |

Page: 1 of 1 Pages: < > Go to Page: [] Save Tab

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
✓ f0990004.xls				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17920	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0988088.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17920	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0988144.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17920	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0988232.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17920	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0991144.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17488	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0929342.xml.gz				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17408	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0987680.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17408	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0987744.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17408	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0987800.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17408	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved
✓ f0987856.dll				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	17408	Unallocated	Unallocated	Unknown	/img_Narcos-1/vol_volt/\$Carved

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

0° C 200% ⌂ ⌂ Reset

/img_Narcos-1/vol_volt/\$CarvedFiles/2/f0991144.jpg

Things to find:

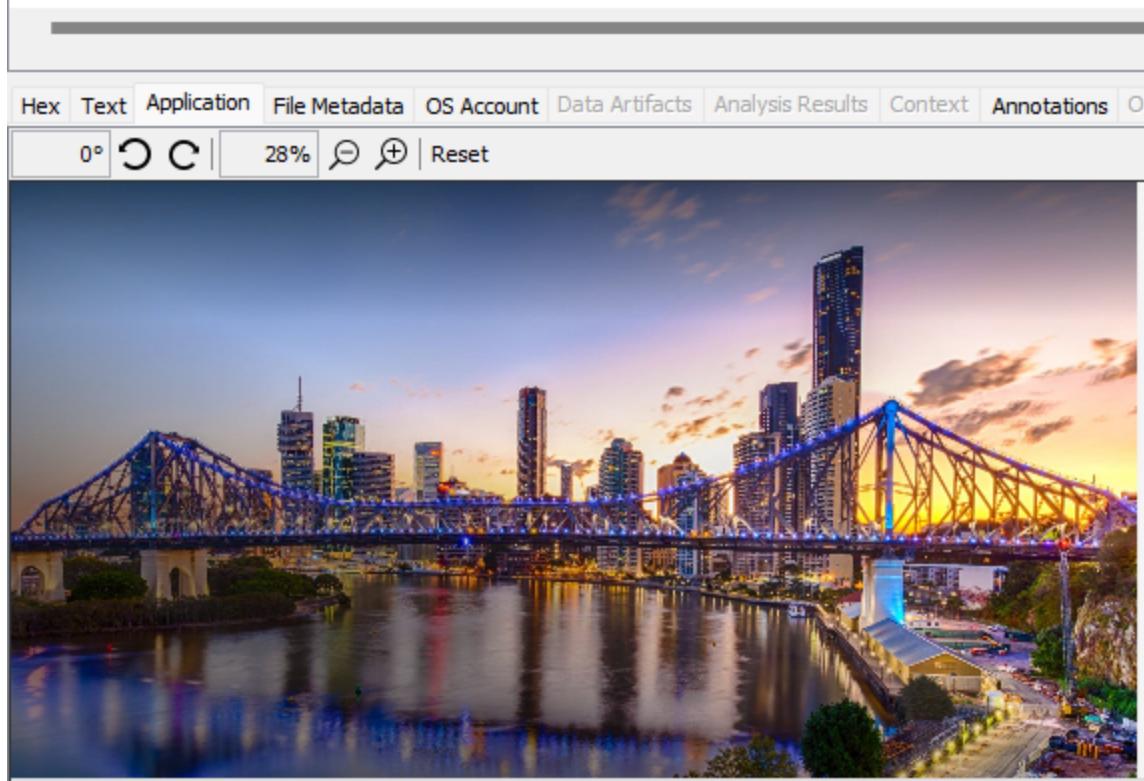
1. Web History
2. Emails
3. Image (I think BNE.png is the steganographed file 😊)

Listing

/img_Narcos-Combined.img/vol_vol7/Users/Steve/Downloads/Misc

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

Name	S	C	O	Modified Time	Location
📁 [current folder]				2019-02-01 10:50:28 SGT	/img_Narcos-Combined.img/vol_v
📁 [parent folder]				2019-02-02 10:28:44 SGT	/img_Narcos-Combined.img/vol_v
🖼️ BNE.png				2019-02-01 08:13:20 SGT	/img_Narcos-Combined.img/vol_v
🖼️ BNE.png:Zone.Identifier				2019-02-01 08:13:20 SGT	/img_Narcos-Combined.img/vol_v
DiscordSetup.exe	▼			2019-01-29 04:56:07 SGT	/img_Narcos-Combined.img/vol_v



Listing Keyword search 21 - BNE.png X Keyword search 22 - OMk2pv6297Pp1O... X

Keyword search

Table Thumbnail Summary

Name	Keyword Preview	Location	Modi
Web History Artifact	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
Favicon Artifact	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
000019.ldb	8f99d4f"zn]`^inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
Favicon Artifact	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
History	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
Web History Artifact	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
UrlCsdWhitelist.store-slack	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
Web History Artifact	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
Favicons	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-
Favicon Artifact	rotonmail.com/inbox/«omk2pv6297pp1o6uag3dlptnyk1ee6...	/img_Narcos-1/vol_vol7/Users/Steve/AppData/Local/Googl...	2019-

<

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

Strings Indexed Text Translation

Page: 1 of 1 Page < > Matches on page: 1 of 1 Match < > 100% ⌂ ⌃ Reset

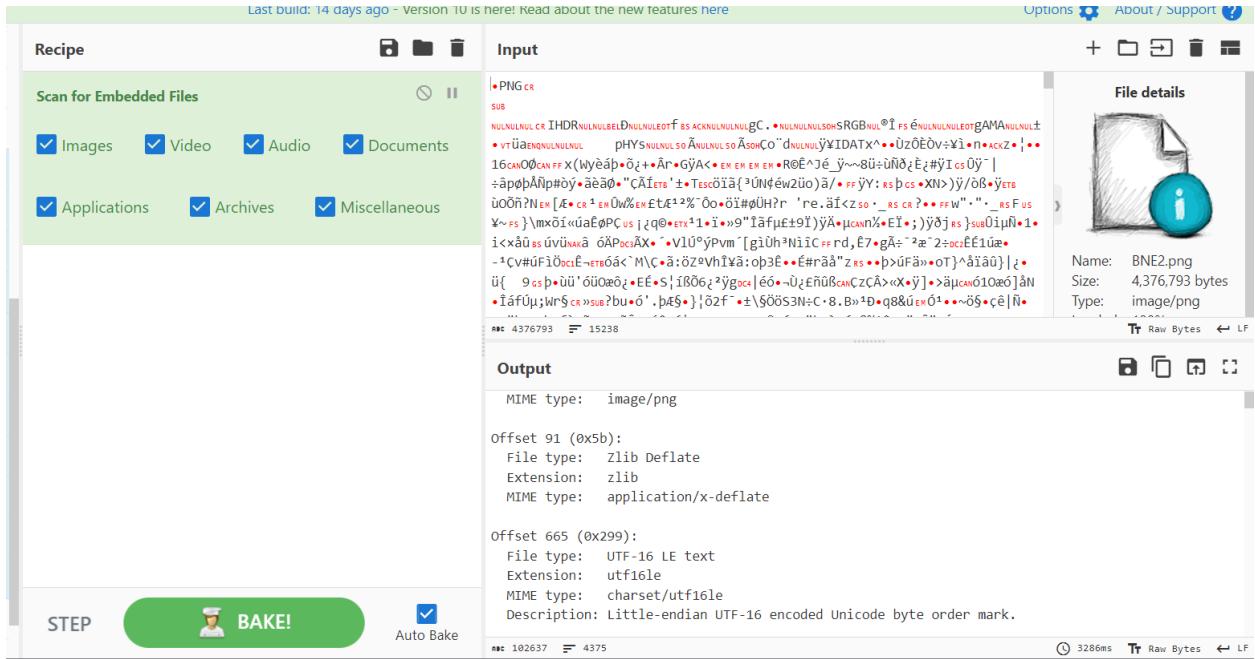
```
[000019.ldb, >5download, 790f671d-7760-49c8-8443-458dcf3c6835
https://
^s.sourceforge.net/project/image-steg/Image%20Steganography%201.5.2%20Setup.exe?r=https%3A%2F%2F]
s%2F
%2F&ts=1548980184&use_mirror=versaweb
,files/latest5P
*,^]IV.
"4e60ab90-88a00"J
Fri, 02 Sep 2011 10:10:24 GMTP
application/octet-streamb
C:\Users\Steve\Download
Unconfirmed 211922.crd:>
w\{Image
xganography 1.5.2
(Setup.ex
,cca1d72f-06cd-4386-a85d-d286c6191f7f
Eblob:
!(mail.proton
com/f7f4f3a9-ba89-4f46-b2a8-c58bb8f99d4f
"zn]
^inbox/OMk2pv6297Pp1O6uag3DLPTnyK1ee6dVkZCT7kaMAS6Hi5ybCyevYuLxzsBwSWa5u-xmyY3XR_H51LXgjEdjYw==*^
00BJP
/pngb
0BNE.pngZ]
```

I used cyberchef and they showed a couple of files embedded?

Using binwalk -Mre to extract the files

```
nnythingy@Nnythingy:/mnt/c/Users/ngjon/Desktop$ binwalk BNE.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	PNG image, 2000 x 1126, 8-bit/color RGBA, non-interlaced
91	0x5B	Zlib compressed data, compressed
...



4. File sharing