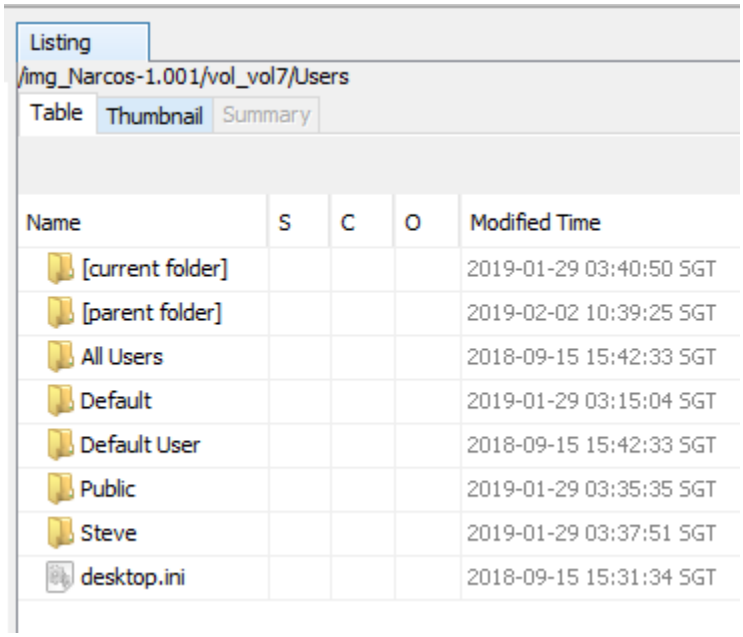
1. Who was the suspect?

- **Steve Kowhai** was the suspect



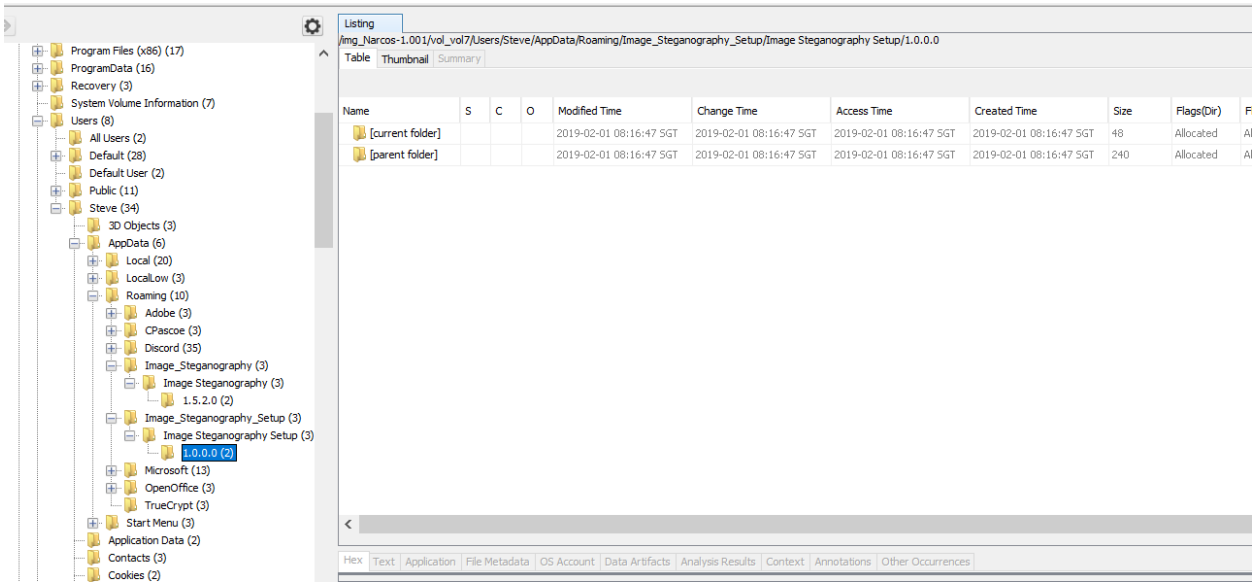
Steve has some basic digital forensics knowledge, as seen from the forensics related applications in his file system such as Image Steganography, TrueCrypt and CCleaner.

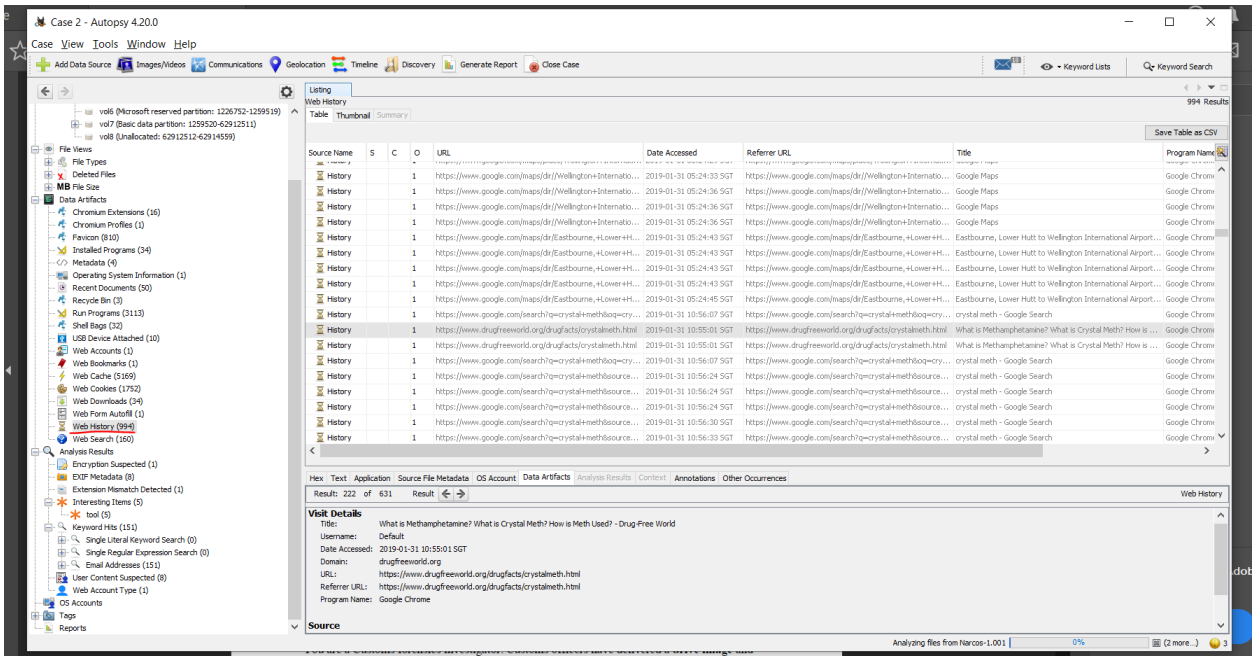
2. What did the suspect want from John during the latter's trip?

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

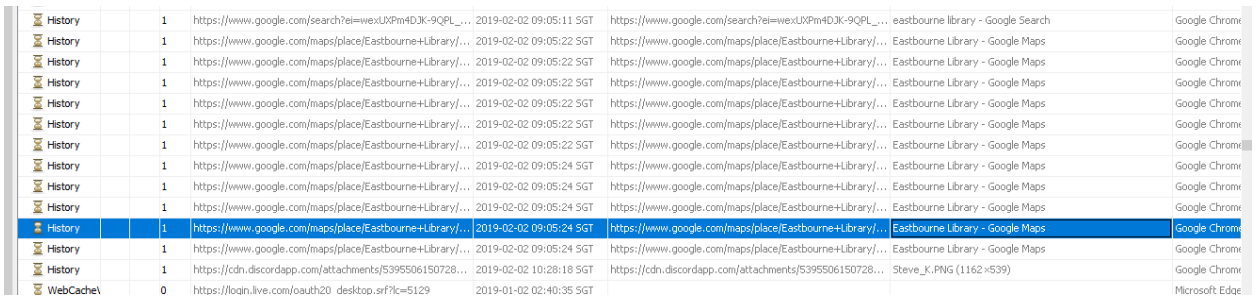
Initial dealing spot: Eastbourne library
Secondary dealing spot: 666 Rewera Avenue, Petone.

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.

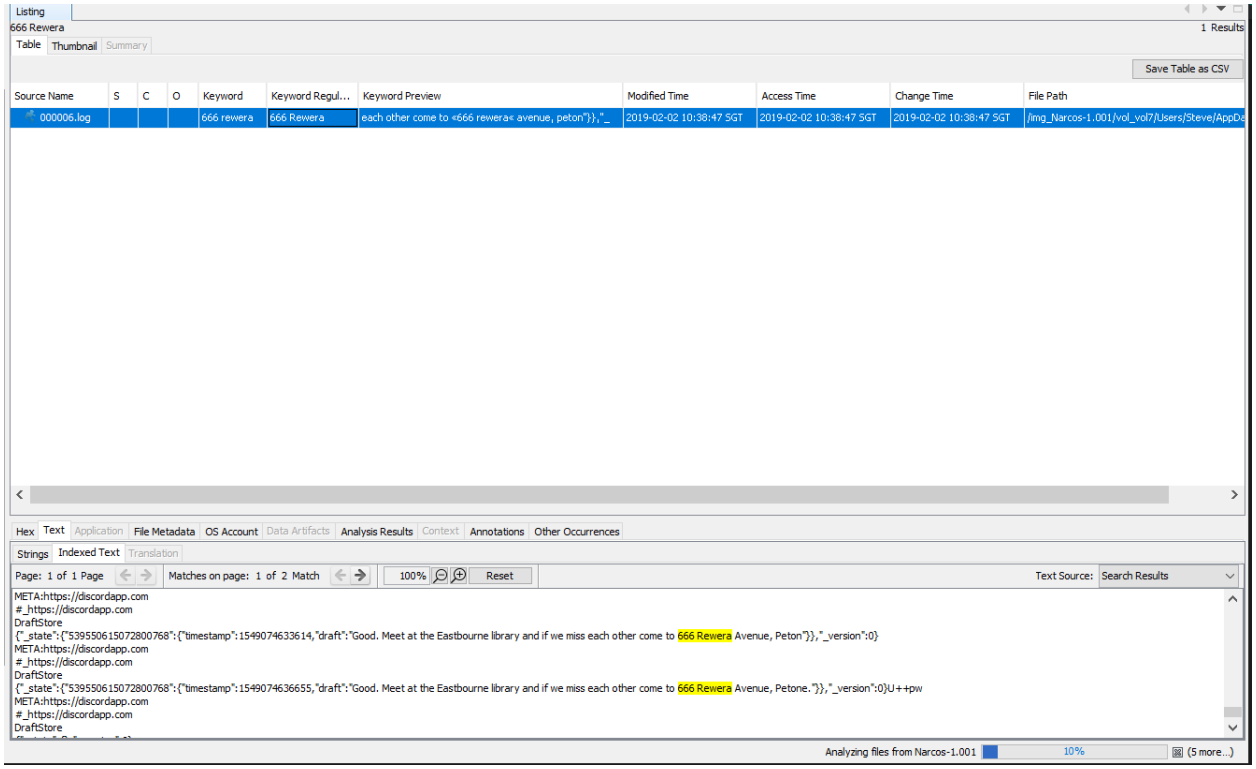




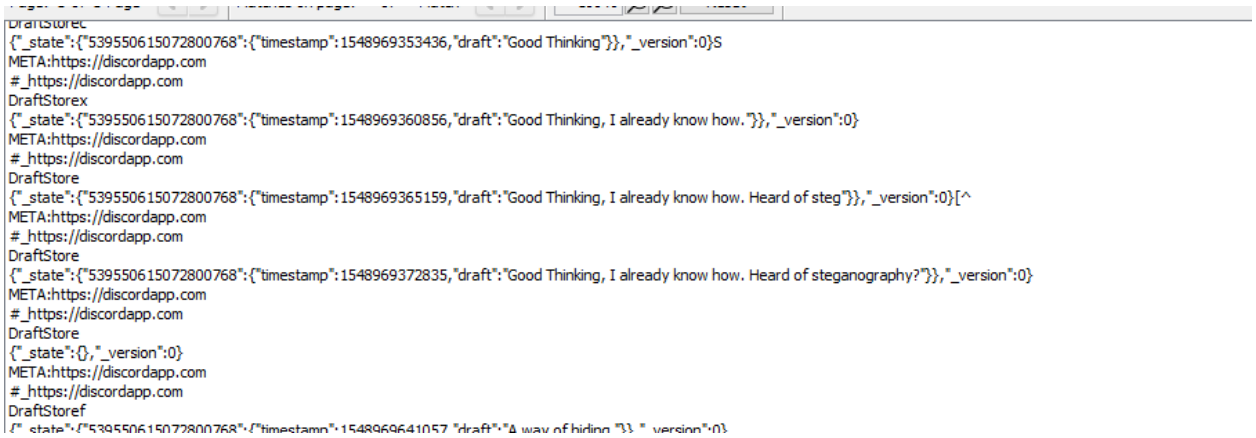
Web search of drugs and Eastbourne library



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



They hid something using steganography

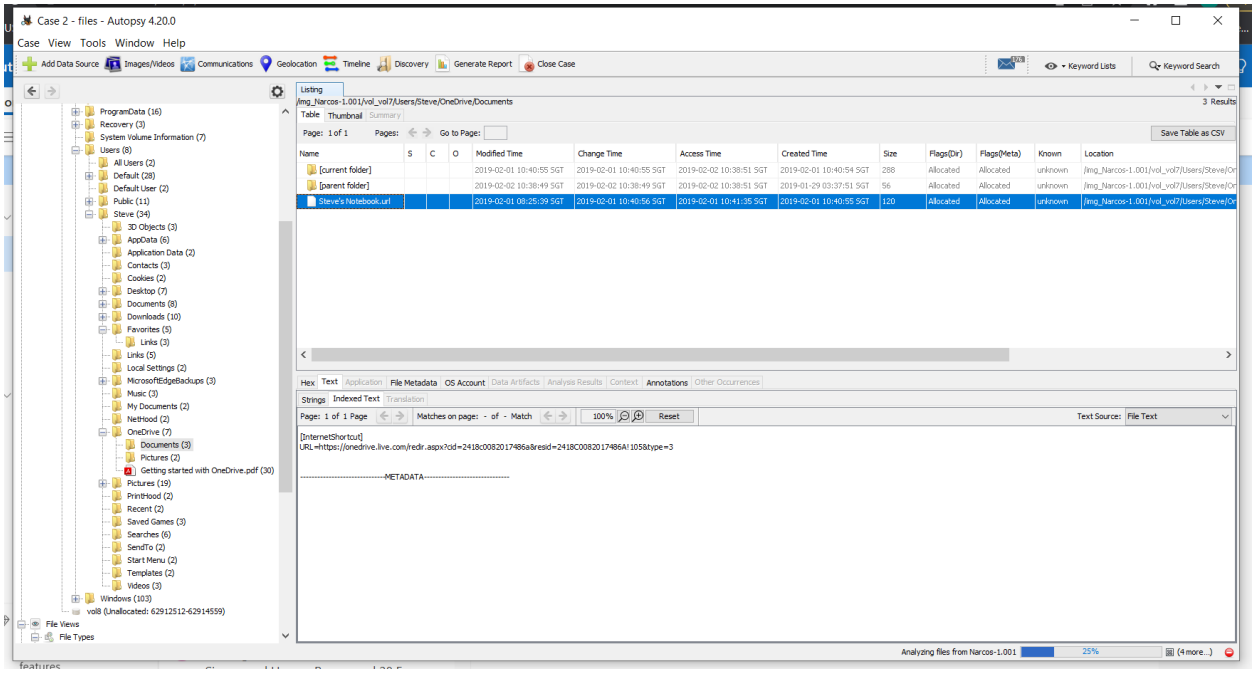


Meet at Eastbourne library

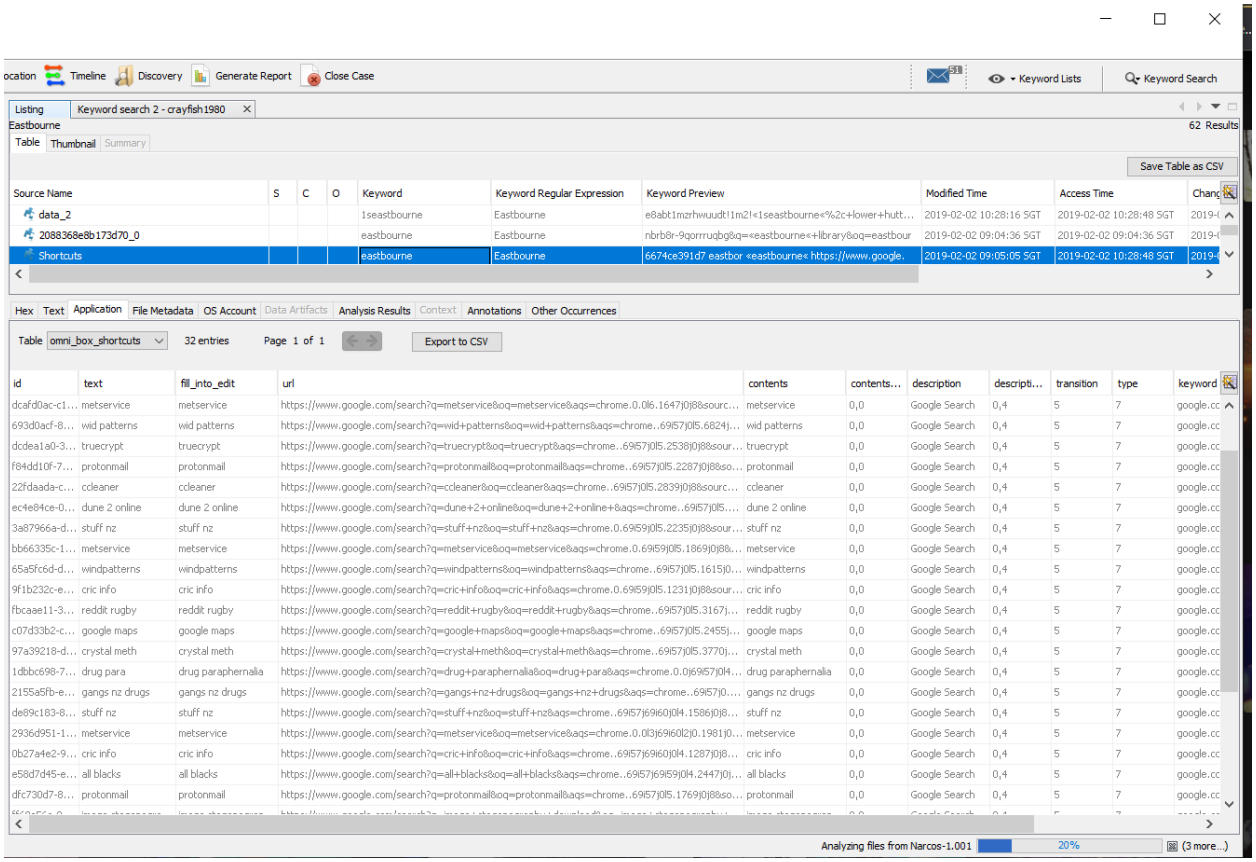
Page: 1 of 1 Page Matches on page: - of - Match 100% Reset

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}w
META:https://discordapp.com
#_https://discordapp.com
DraftStore
{"_state":{"539550615072800768":{"timestamp":1549074594238,"draft":"Good. Meet

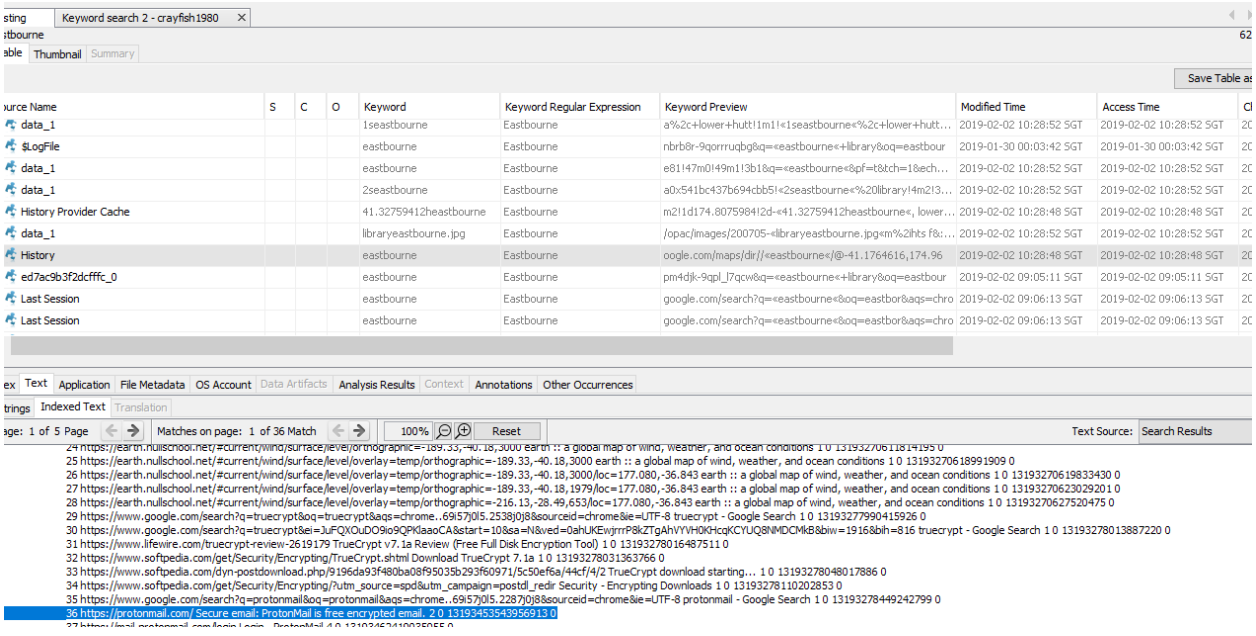
Steve notebook:
URL=https://onedrive.live.com/redir.aspx?cid=2418c0082017486a&resid=2418C0082017486A!105&type=3

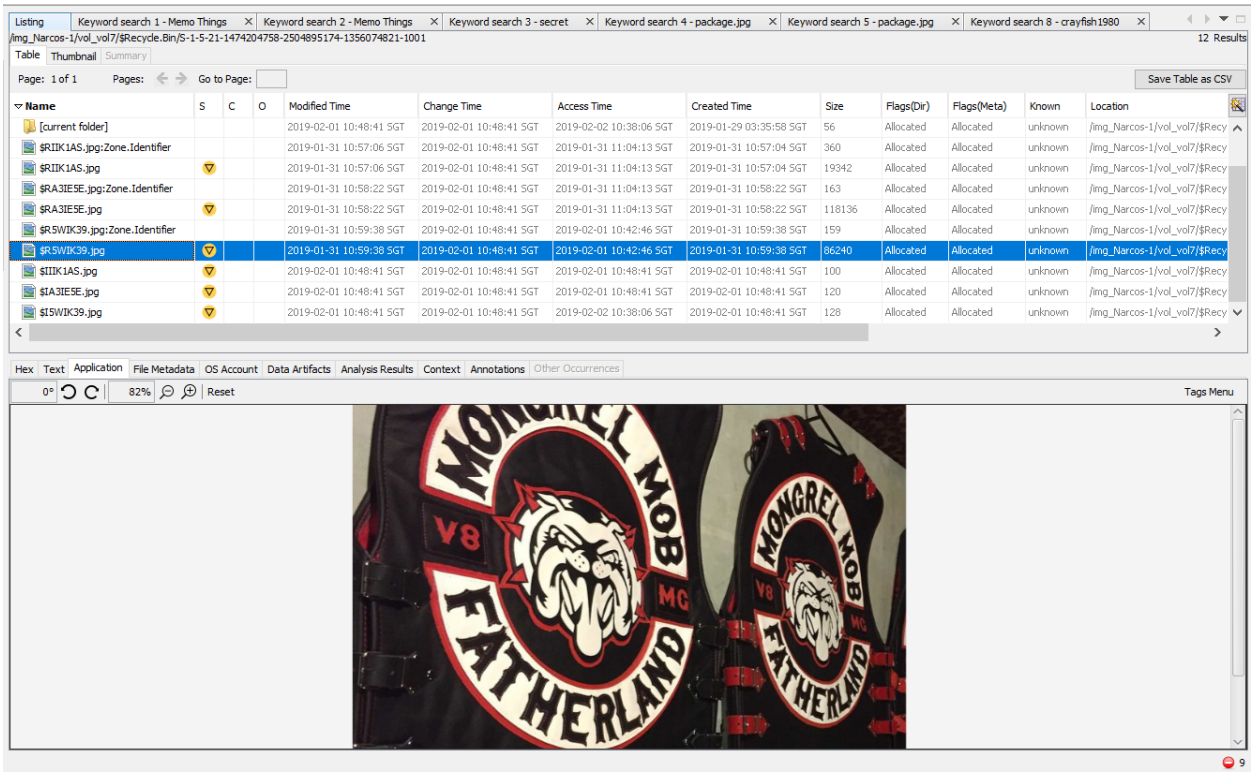


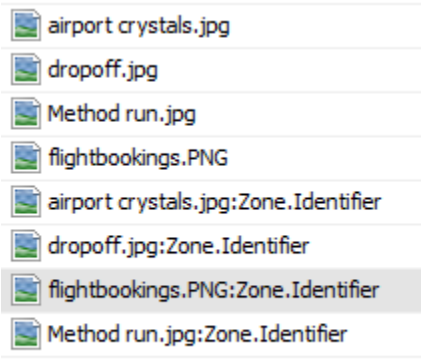
His shortcuts



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





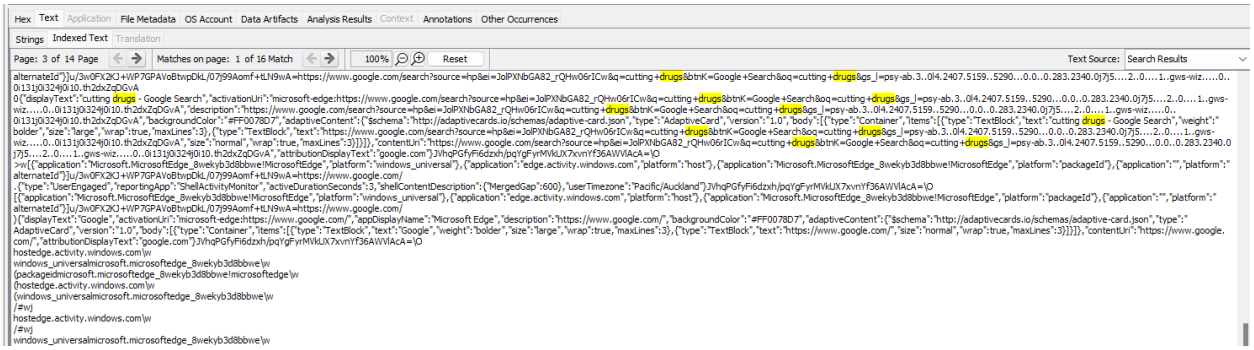


ReferrerUrl=https://cdn.discordapp.com/attachments/539550615072800768/541074665892741121/Steve_K.PNG
HostUrl=https://cdn.discordapp.com/attachments/539550615072800768/541074665892741121/Steve_K.PNG

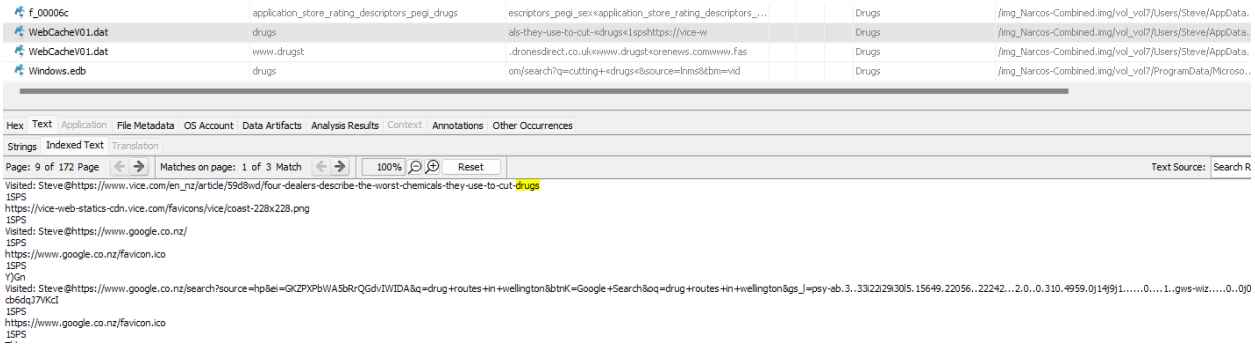
/img_Narcos-1/vol_vol7/Users/Steve/Documents/Misc/flightbookings.PNG:Zone.Identifier

3. What were their future plans and intentions?

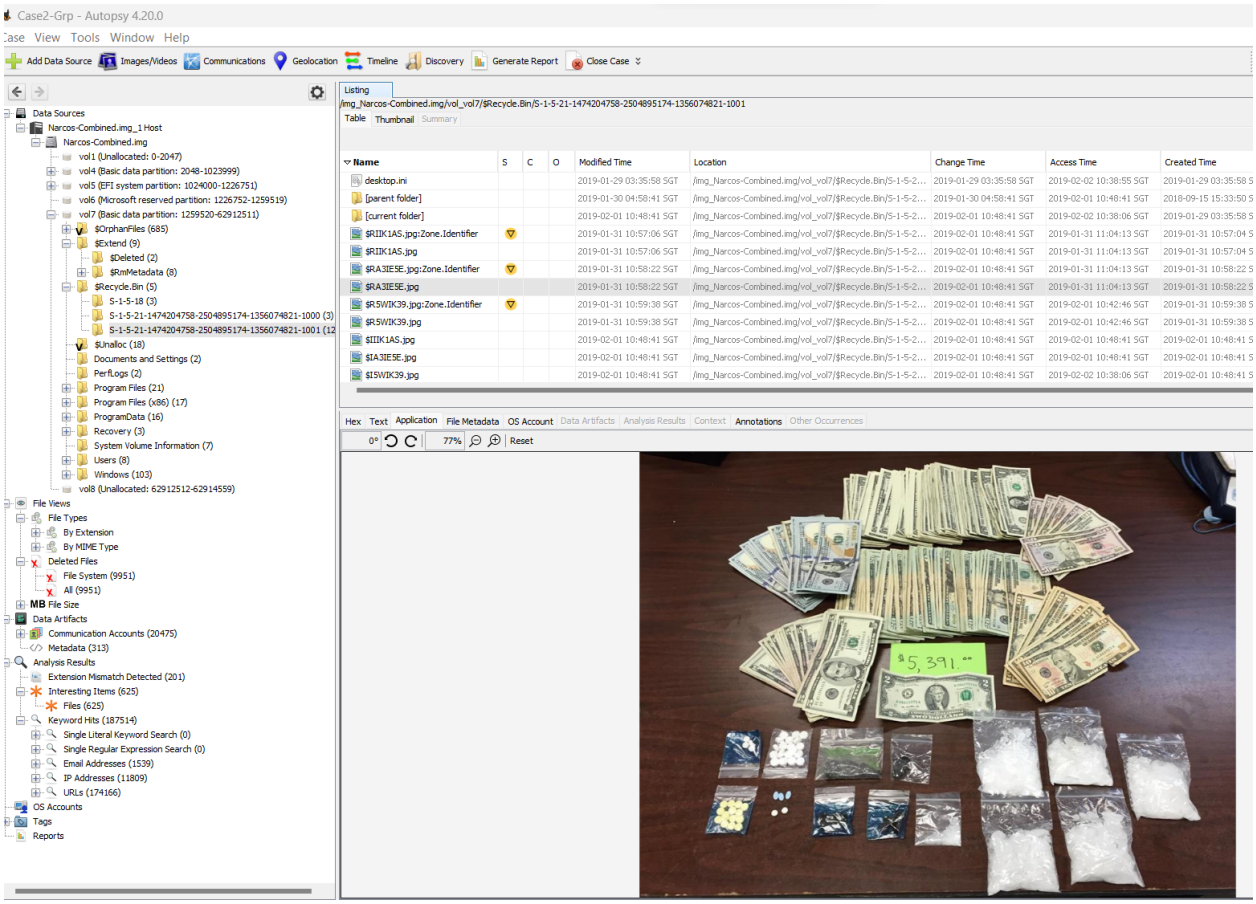
-Cutting drugs?



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



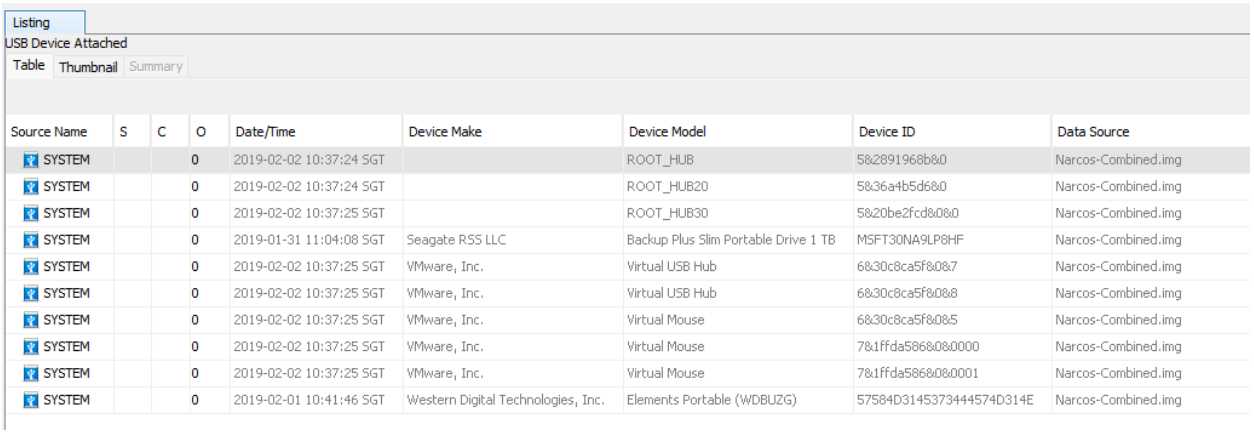
- Evidence to show that steve is a drug dealer, have made past deals



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&36a4b5d6&0	Narcos-Combined.img
SYSTEM			0	2019-02-02 10:37:25 SGT		ROOT_HUB30	5&20be2fcd&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&30c8ca5f&0&7	Narcos-Combined.img
SYSTEM			0	2019-02-02 10:37:25 SGT	VMware, Inc.	Virtual USB Hub	6&30c8ca5f&0&8	Narcos-Combined.img
SYSTEM			0	2019-02-02 10:37:25 SGT	VMware, Inc.	Virtual Mouse	6&30c8ca5f&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

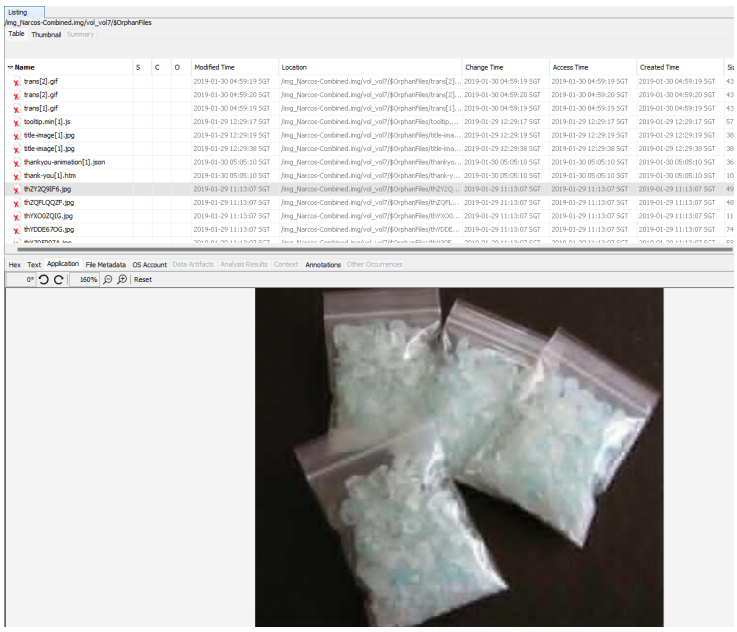
```
12799870 20 00 00 00 02 00 00 00-01 00 00 00 01 00 00 00  ................
12799880 05 00 00 00 98 00 00 00-7B 22 63 6F 6E 74 65 6E ........{"conten
12799890 74 22 3A 22 47 6F 6F 64-2E 20 4D 65 65 74 20 61 t":"Good. Meet a
127998a0 74 20 74 68 65 20 45 61-73 74 62 6F 75 72 6E 65 t the Eastbourne
127998b0 20 6C 69 62 72 61 72 79-20 61 6E 64 20 69 66 20  library and if
127998c0 77 65 20 6D 69 73 73 20-65 61 63 68 20 6F 74 68 we miss each oth
127998d0 65 72 20 63 6F 6D 65 20-74 6F 20 36 36 36 20 52 er come to 666 R
127998e0 65 77 65 72 61 20 41 76-65 6E 75 65 2C 20 50 65 ewera Avenue, Pe
127998f0 74 6F 6E 65 2E 22 2C 22-6E 6F 6E 63 65 22 3A 22 tone.","nonce":"
12799900 35 34 31 30 38 33 30 36-30 35 39 35 30 36 34 38 5410830605950648
12799910 33 32 22 2C 22 74 74 73-22 3A 66 61 6C 73 65 7D 32","tts":false}
12799920 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ................
12799930 00 00 00 00 01 00 00 00-01 00 00 00 00 00 00 00 ................
```

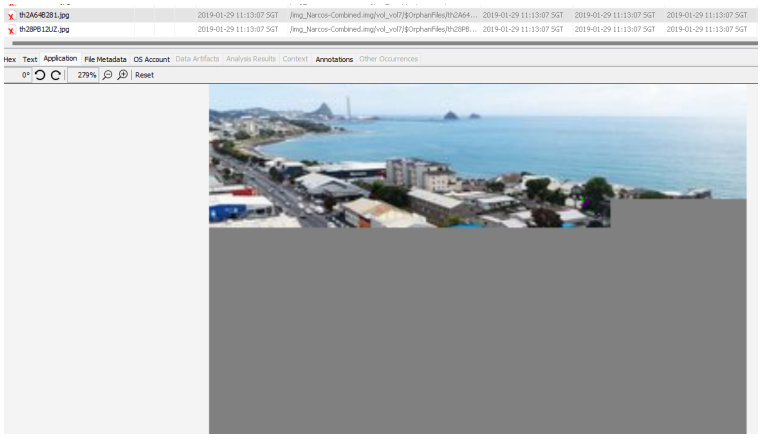
```
fla4ddf0 72 65 63 74 2E 63 6F 2E-75 6B 82 0D 77 77 77 2E rect.co.uk··www.
fla4de00 62 72 69 6D 67 2E 6E 65-74 82 12 77 77 77 2E 62 brimg.net··www.b
fla4de10 75 79 69 74 64 69 72 65-63 74 2E 69 65 82 16 77 uyitdirect.ie··w
fla4de20 77 77 2E 64 72 6F 6E 65-73 64 69 72 65 63 74 2E ww.dronesdirect.
fla4de30 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
```

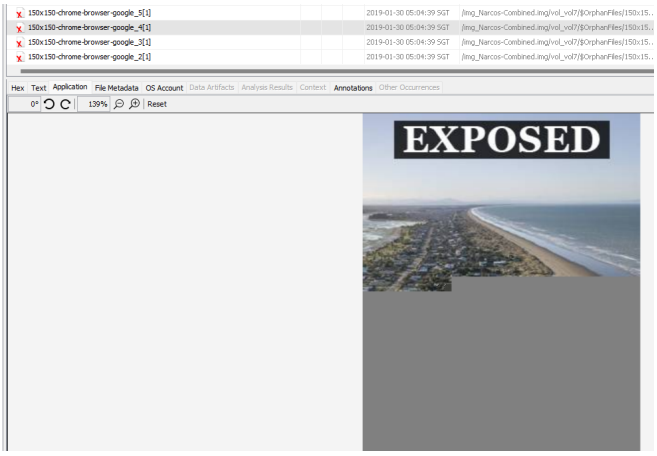
```
2521c20 5C 02 00 00 00 00 00 00-00 00 00 00 00 00 00 00 \···············
2521c30 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
2521c40 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
2521c50 00 00 00 00 00 00 00 00-00 00 00 00 0A 55 A0 50 ·············U P
2521c60 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 hXBXn0KHe-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 AhXBXn0KHe-GD28Q
2521d00 4D 77 68 63 4B 42 51 77-46 41 2E 2E 69 26 69 6D MwhcKBQwFA..i&im
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&imgurl=ht
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&imgrefurl=h
2521d90 74 74 70 73 3A 2F 2F 77-77 77 2E 72 61 64 69 6F ttps://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=StF4qrt40NxY
2521e00 33 4D 3A 26 64 6F 63 69-64 3D 73 76 75 55 38 76 3M:&docid=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&csi=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····ß·C····I····2¥··?·gi··}·····`·`····.
·û··R·§u2·ÿÇ(ú`ÿÇYúo·Oë··ÓY·úT··https://securepubads.g.doubleclick.net/gampad/ad
s?gdfp_req=1&pvsid=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%3D797635a01955b9d
93eacf51d56a11d207800%26obsession%3Dhow-we-buy%26topic%3Dfinance-and-economics%2
6tags%3Donline-drug-trade%252Ctor-browser%252Ccrystal-meth%252Cdread-pirate-robe
rts%252Cross-ulbricht%252Cecstasy%252Cmethamphetamine%252Cmdma%252Cillegal-drugs
%252Cdrug-trade%252Clsd%252Cdark-web%252Cblack-market%252Cnarcotics%252Ccocaine%
252Csilk-road%252Cheroin%252Ccannabis%252Cmarijuana%252Cdrugs%252Ccryptocurrency
%252Cbitcoin%26wpid%3D481037%26tile%3D8%26split%3Da%26entryTopic%3Dfinance-and-e
conomics%26entryObsession%3Dhow-we-buy%26adType%3Dinline%26contentId%3D481037&co
okie=ID%3D8c91607fe51d5884%3AT%3D1549069036%3AS%3DALNI_MYY9Gwp38xAL_wZMsvlWFpNf9
5gbw&cookie_enabled=1&bc=15&abxe=1&lmt=1549069068&dt=1549069068781&dlt=154906903
4881&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&dssz=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=CjoItJ6NlxJA9ZMVWL2JrbASWOz
N2LASeAHoAb68v4ODBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCkAI5du-mBJAmf6rsgFI3csU
WL2JrbASWOzN2LASeAHoAZjX-oSDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCjoItJ6NlxJA9
ZMVWL2JrbASWOzN2LASeAHoAdmHmYSDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ&ga_vid=60810
9901.1549069036&ga_sid=1549069036&ga_hid=2017045959&fws=4·····················
·····························································
```

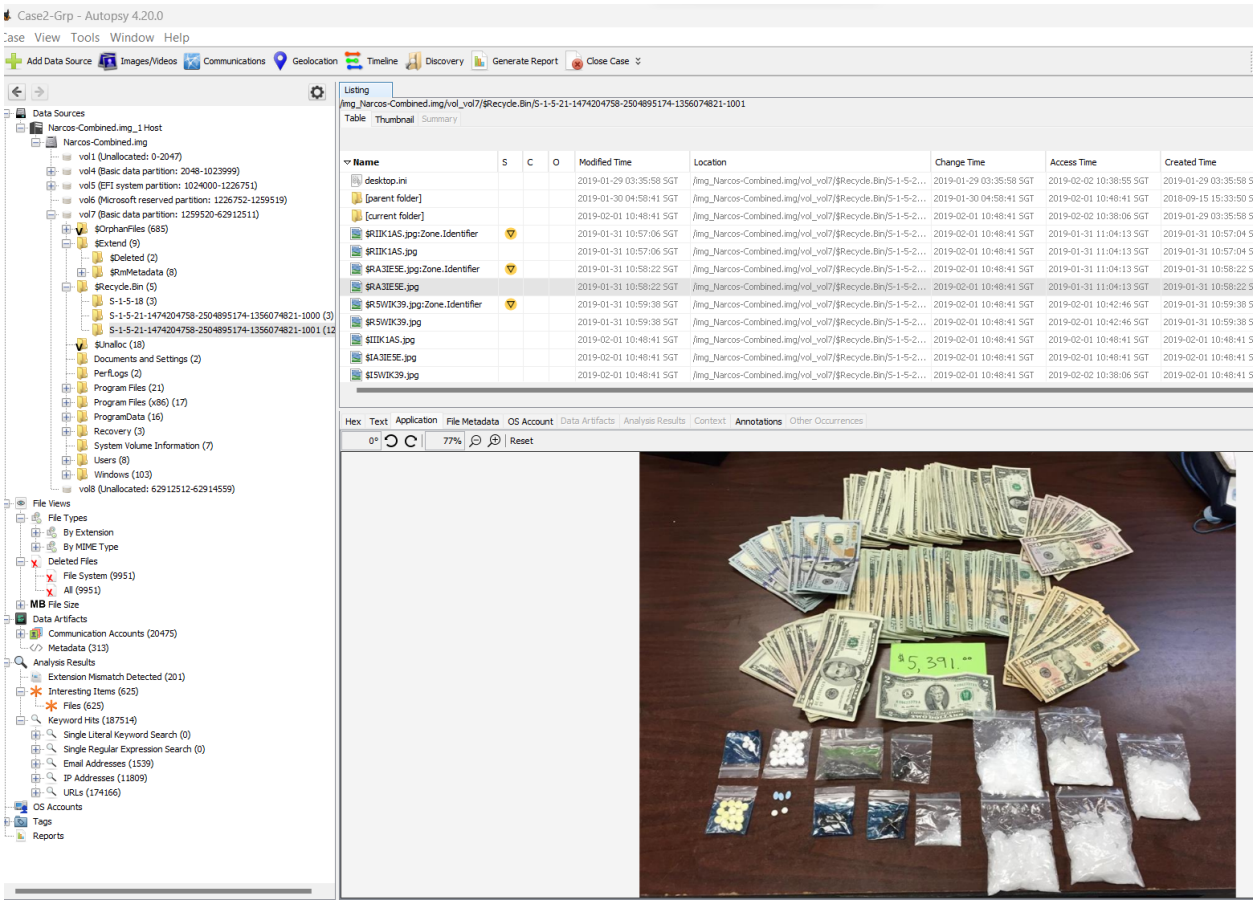
https://securepubads.g.doubleclick.net/gampad/ads?gdfp_req=1&pvsid=3257724645068240&correlator=1436628257927774&output=json_html&callback=googletag.impl.pubads.callbackProxy8&impl=fif&adsid=NT&eid=21062414%2C21062420&vrg=299&guci=2.2.0.0.2.2.0.0&plat=1%3A32776%2C2%3A32776&sc=1&sfv=1-0-31&iu=%2F56091333%2Fquartz%2Farticle&sz=640x363%7C640x380%7C300x600%7C970x253&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%252Cmdma%252Cillegal-drugs%252Cdrug-trade%252Clsd%252Cdark-web%252Cblack-market%252Cnarcotics%252Ccocaine%252Csilk-road%252Cheroin%252Ccannabis%252Cmarijuana%252Cdrugs%252Ccryptocurrency%252Cbitcoin%26wpid%3D481037%26tile%3D10%26split%3Da%26entryTopic%3Dfinance-and-economics%26entryObsession%3Dhow-we-buy%26adType%3Dinline%26contentId%3D481037&cookie=ID%3D8c91607fe51d5884%3AT%3D1549069036%3AS%3DALNI_MYY9Gwp38xAL_wZMsv1WFpNf95gbw&cookie_enabled=1&bc=15&abxe=1&lmt=1549069079&dt=1549069079918&dlt=1549069034881&idt=1322&frm=20&biw=1899&bih=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&dssz=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=CjoItJ6NlxJA9ZMVWL2JrbASWOzN2LASeAHoAb68v4ODBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCjoIyvfqkRJA9ZMVWL2JrbASWOzN2LASeAHoAfa-v4ODBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCkAI5du-mBJAmf6rsgFI3csUWL2JrbASWOzN2LASeAHoAZjX-oSDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCjoItJ6NlxJA9ZMVWL2JrbASWOzN2LASeAHoAdmHmYSDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ%2CCjoItJ6NlxJA9ZMVWL2JrbASWOzN2LASeAHoAeHPp4SDBIAChcGiGoAC_cGiGoAC88v581CAAvbL-fJQ&ga_vid=608109901.1549069036&ga_sid=1549069036&ga_hid=2017045959&fws=4

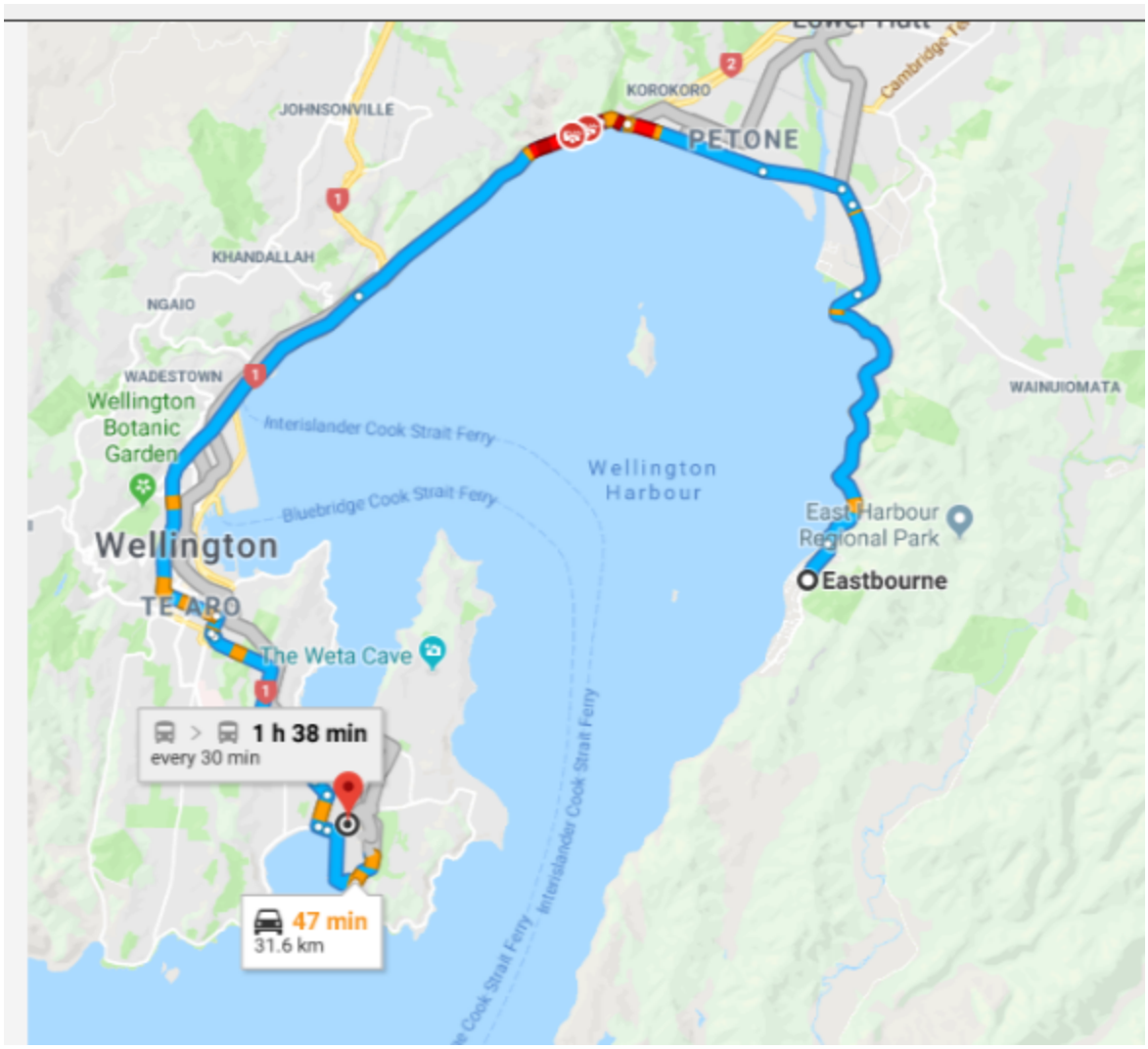



th2A64B281.jpg
2019-01-29 11:13:07 SGT
/img_Narcos-Combined.img/vol_vol7/$OrphanFiles/th2A64...
2019-01-29 11:13:07 SGT
2019-01-29 11:13:07 SGT
2019-01-29 11:13:07 SGT
th28P812UZ.jpg
2019-01-29 11:13:07 SGT
/img_Narcos-Combined.img/vol_vol7/$OrphanFiles/th28PB...
2019-01-29 11:13:07 SGT
2019-01-29 11:13:07 SGT
2019-01-29 11:13:07 SGT
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
0°
279%
Reset



\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)
vol4 (Basic data partition: 2048-1023999)
vol5 (EFI system partition: 1024000-1226751)
vol6 (Microsoft reserved partition: 1226752-1259519)
vol7 (Basic data partition: 1259520-62912511)
$OrphanFiles (685)
$Extend (9)
$Deleted (2)
$RmMetadata (8)
$Recycle.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
$Unalloc (18)
Documents and Settings (2)
PerfLogs (2)
Program Files (21)
Program Files (x86) (17)
ProgramData (16)
Recovery (3)
System Volume Information (7)
Users (8)
Windows (103)
vol8 (Unallocated: 62912512-62914559)
File Views
File Types
By Extension
By MIME Type
Deleted Files
File System (9951)
All (9951)
MB File Size
Data Artifacts
Communication Accounts (20475)
Metadata (313)
Analysis Results
Extension Mismatch Detected (201)
Interesting Items (625)
Files (625)
Keyword Hits (187514)
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Email Addresses (1539)
IP Addresses (11809)
URLs (174166)
OS Accounts
Tags
Reports
Listing
/img_Narcos-Combined.img/vol_vol7/$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001
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_vol7/$Recycle.Bin/S-1-5-2...
2019-01-29 03:35:58 SGT
2019-02-02 10:38:55 SGT
2019-01-29 03:35:58 S
[parent folder]
2019-01-30 04:58:41 SGT
/img_Narcos-Combined.img/vol_vol7/$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_vol7/$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
$RIIK1AS.jpg:Zone.Identifier
2019-01-31 10:57:06 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$RIIK1AS.jpg
2019-01-31 10:57:06 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$RA3IE5E.jpg:Zone.Identifier
2019-01-31 10:58:22 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$RA3IE5E.jpg
2019-01-31 10:58:22 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$R5WIK39.jpg:Zone.Identifier
2019-01-31 10:59:38 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$R5WIK39.jpg
2019-01-31 10:59:38 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$IIK1AS.jpg
2019-02-01 10:48:41 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$IA3IE5E.jpg
2019-02-01 10:48:41 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$I5WIK39.jpg
2019-02-01 10:48:41 SGT
/img_Narcos-Combined.img/vol_vol7/$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
$5,391.00


JOHNSONVILLE
KOROKORO
PETONE
KHANDALLAH
NGAIO
WADESTOWN
Wellington Botanic Garden
Interislander Cook Strait Ferry
Wellington Harbour
Bluebridge Cook Strait Ferry
East Harbour Regional Park
Eastbourne
WAINUIOMATA
Wellington
TE ARO
The Weta Cave
1 h 38 min
every 30 min
47 min
31.6 km

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« xuhtt…	2019-01-31 10
000003.log	methamphetamine.jpg				Methamphetamine	e04-image01-what-is-«methamphetamine.jpg«url"{https://…	2019-01-31 10
13485dbed5111290_0	methamphetamine				Methamphetamine	ixwep10w3qcydata["«methamphetamine«","https://www.g…	2019-01-31 10
13485dbed5111290_0	u003dmethamphetamine				Methamphetamine	6887f2f9510b\u0026q\«u003dmethamphetamine«\u0026s…	2019-01-31 10
3a6897da1e20e5f6_0	7cmethamphetamine				Methamphetamine	-ulbricht%7cecstasy%«7cmethamphetamine«%7cmdma%…	2019-02-02 08
BrowserMetrics-5C50C033-26A0.pma-slack	methamphetamine.jpgcache				Methamphetamine	e04-image01-what-is-«methamphetamine.jpgcache«-contr…	2019-01-30 05
DragVisualUserControl2.xbf	7cmethamphetamine				Methamphetamine	-ulbricht%7cecstasy%«7cmethamphetamine«%7cmdma%…	2019-01-30 05
History	methamphetamine				Methamphetamine	almeth.html what is «methamphetamine«? what is crystal me	2019-02-02 10
History Provider Cache	methamphetamine				Methamphetamine	tsdrugcrystalmeth«methamphetamine«usedwhatlnmsisch	2019-02-02 10
Unalloc_280525_10081198080_14450704384	methamphetamine				Methamphetamine	eneric term)(noun)|«methamphetamine«|methamphetamin…	0000-00-00 00
Unalloc_280525_10081198080_14450704384	methamphetamine.jpgcache				Methamphetamine	e04-image01-what-is-«methamphetamine.jpgcache«-contr…	0000-00-00 00
Unalloc_280525_10081198080_14450704384	methylenedioxymethamphetamine				Methamphetamine	|cristal|x|hug drug|«methylenedioxymethamphetamine« (g…	0000-00-00 00
Unalloc_280525_644890624_10077200384	2cmethamphetamine				Methamphetamine	rning%2cmany%2cbail%«2cmethamphetamine«%2cdistric…	0000-00-00 00
Unalloc_280525_644890624_10077200384	20methamphetamine				Methamphetamine	tml%title>wubat%20i%«20methamphetamine«%3f%20wub…	0000-00-00 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

```
url"{https://www.drugfreeworld.org/sites/default/files/imagecache/gcui_inline_default/page04-image01-what-is-methamphetamine.jpg"  timestampN
{https://www.drugfreeworld.org/sites/default/files/imagecache/gcui_inline_default/page04-image01-what-is-methamphetamine.jpg
{https://www.drugfreeworld.org/sites/default/files/imagecache/gcui_inline_default/page04-image01-what-is-methamphetamine.jpg
{https://www.drugfreeworld.org/sites/default/files/imagecache/gcui_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_0@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_TopFrameUnsafe_TEXT = "This website has been reported as unsafe";
†††
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.
```

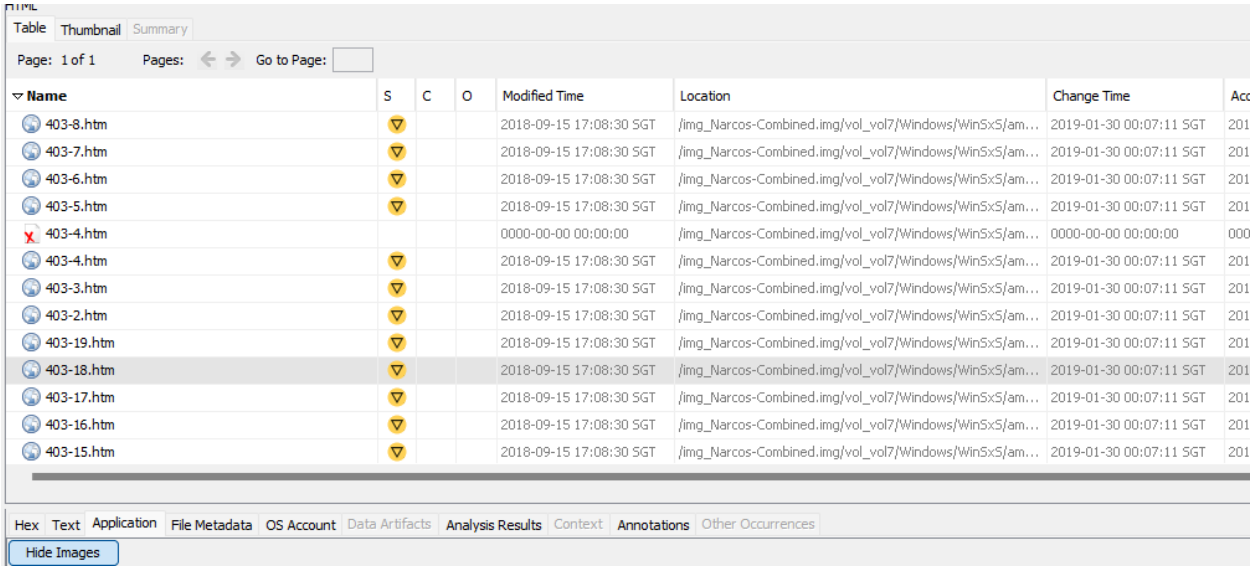
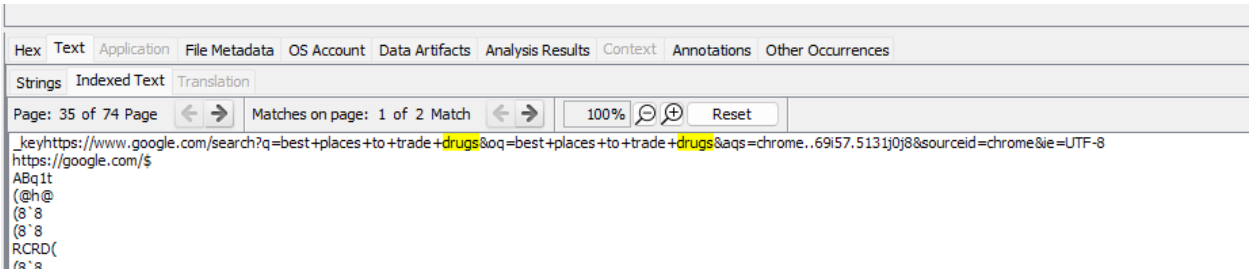
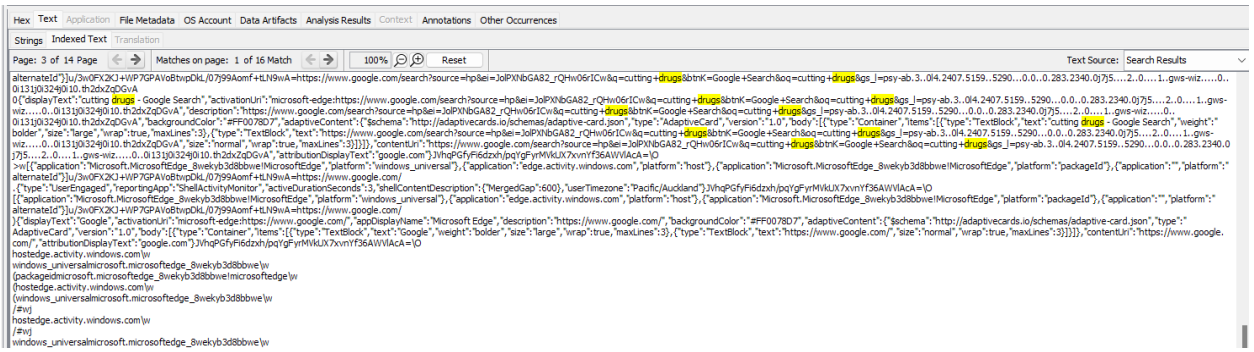
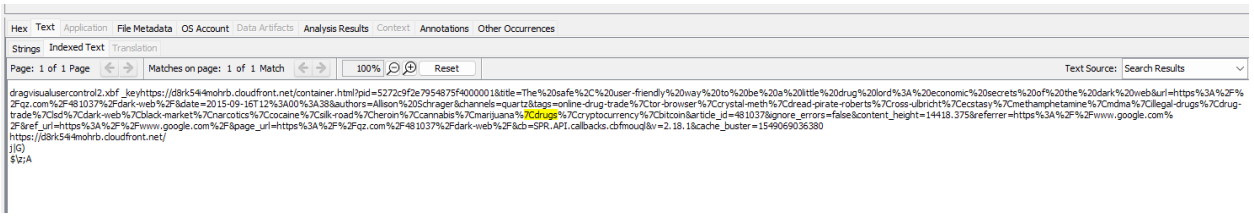
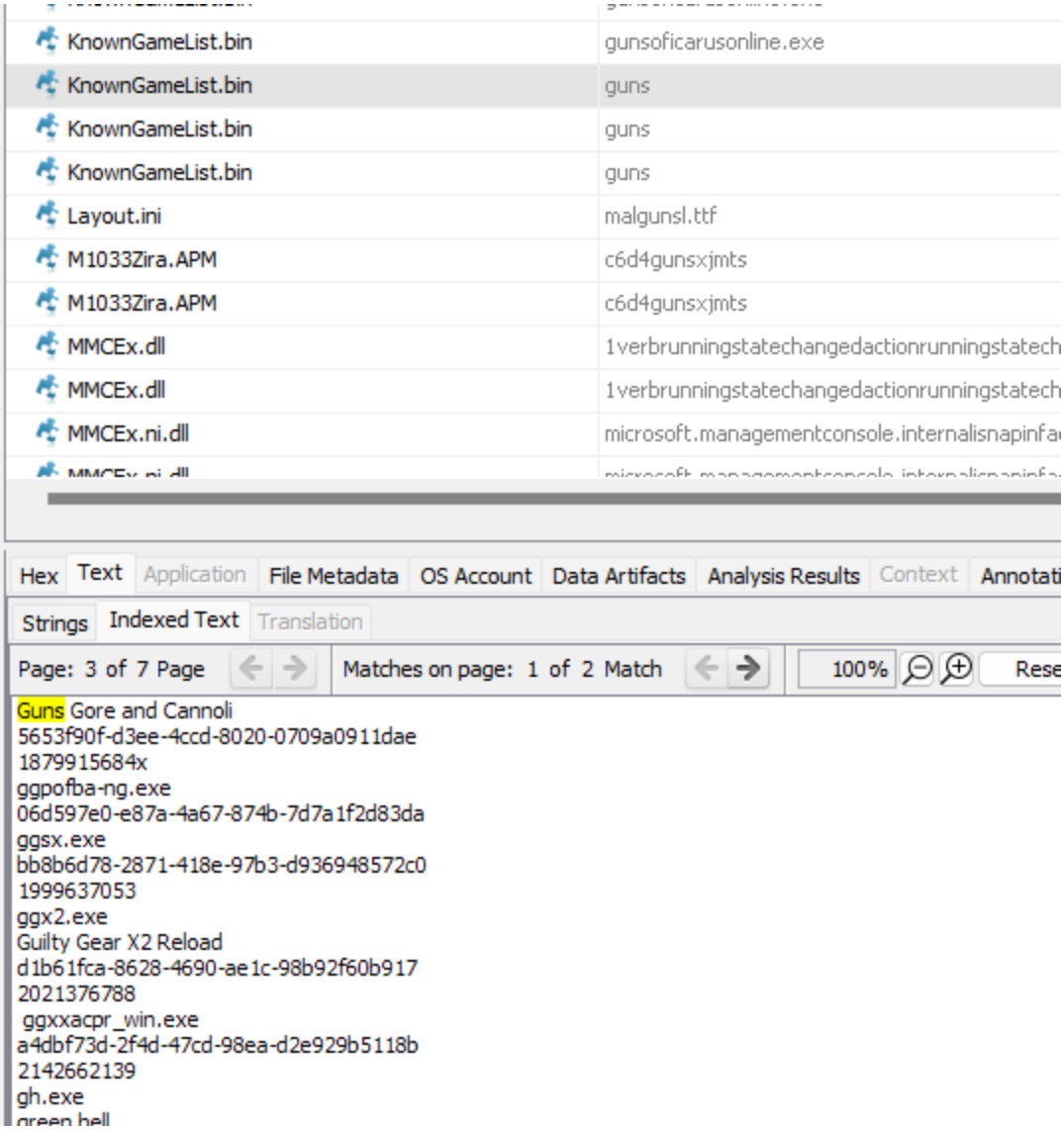


Table
Thumbnail
Summary
Page: 1 of 1
Pages:
Go to Page:
Name
S
C
O
Modified Time
Location
Change Time
403-8.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-7.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-6.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-5.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-4.htm 0000-00-00 00:00:00 /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 0000-00-00 00:00:00
403-4.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-3.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-2.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-19.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-18.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-17.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-16.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
403-15.htm 2018-09-15 17:08:30 SGT /img_Narcos-Combined.img/vol_vol7/Windows/WinSxS/am... 2019-01-30 00:07:11 SGT
Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Hide Images

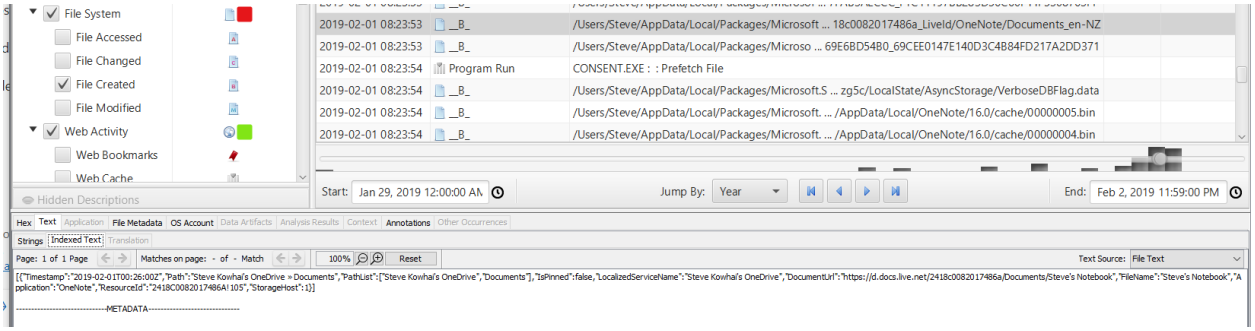

Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 35 of 74 Page
Matches on page: 1 of 2 Match
100%
Reset
_keyhttps://www.google.com/search?q=best+places+to+trade+drugs&oq=best+places+to+trade+drugs&aqs=chrome..69i57.5131j0j8&sourceid=chrome&ie=UTF-8
https://google.com/$
ABq1t
(@h@
(8`8
(8`8
RCRD(


Hex
Text
Application
File Metadata
OS Account
Data Artifacts
Analysis Results
Context
Annotations
Other Occurrences
Strings
Indexed Text
Translation
Page: 3 of 14 Page
Matches on page: 1 of 16 Match
100%
Reset
Text Source:
Search Results


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

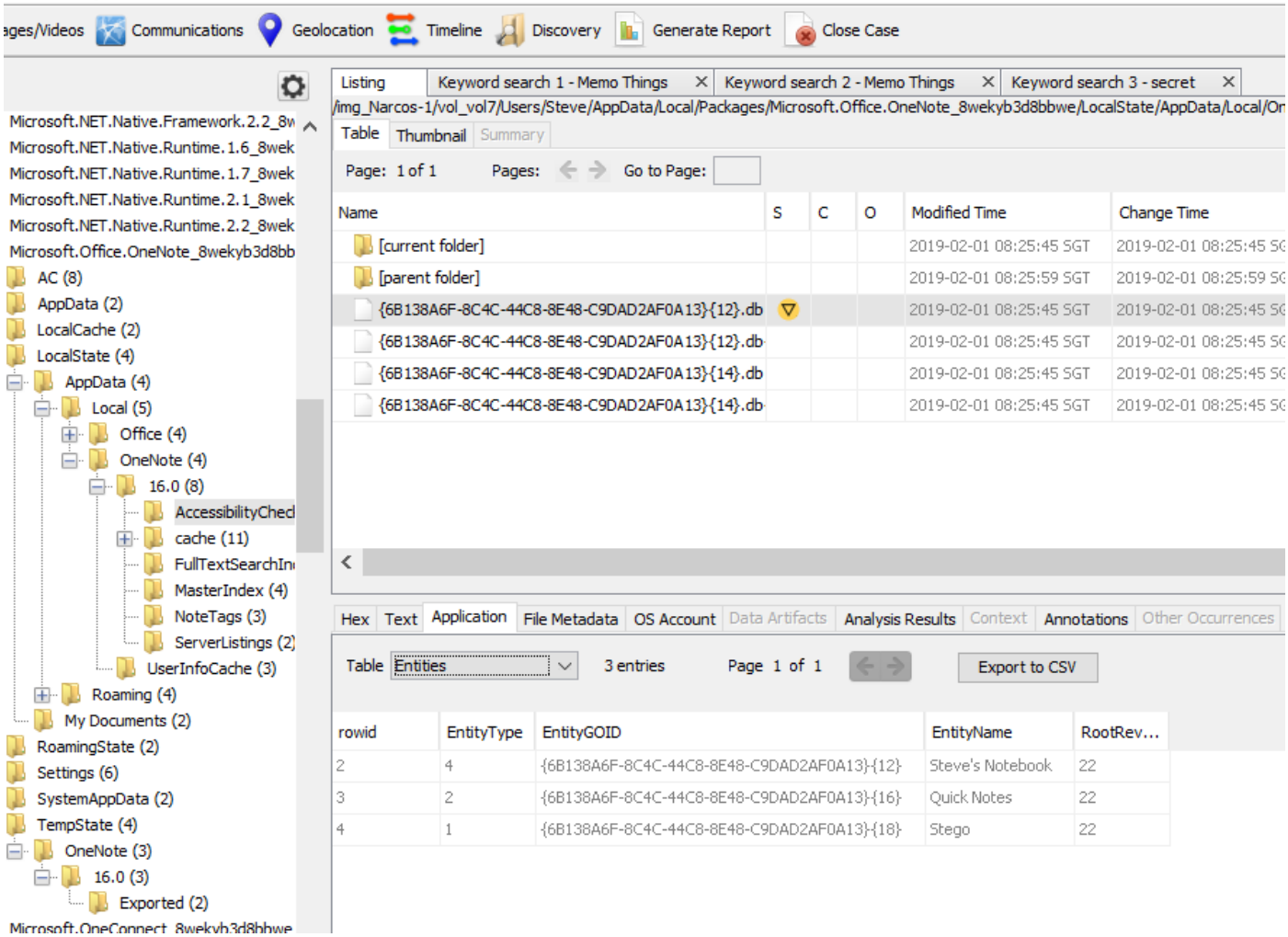

KnownGameList.bin
gunsoficarusonline.exe
KnownGameList.bin
guns
KnownGameList.bin
guns
KnownGameList.bin
guns
Layout.ini
malgunsl.ttf
M1033Zira.APM
c6d4gunsxjmts
M1033Zira.APM
c6d4gunsxjmts
MMCEx.dll
1verbrunningstatechangedactionrunningstatech
MMCEx.dll
1verbrunningstatechangedactionrunningstatech
MMCEx.ni.dll
microsoft.managementconsole.internalisnapinfa
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%
Rese
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
ggx2.exe
Guilty Gear X2 Reload
d1b61fca-8628-4690-ae1c-98b92f60b917
2021376788
ggxxacpr_win.exe
a4dbf73d-2f4d-47cd-98ea-d2e929b5118b
2142662139
gh.exe

7/4/2023

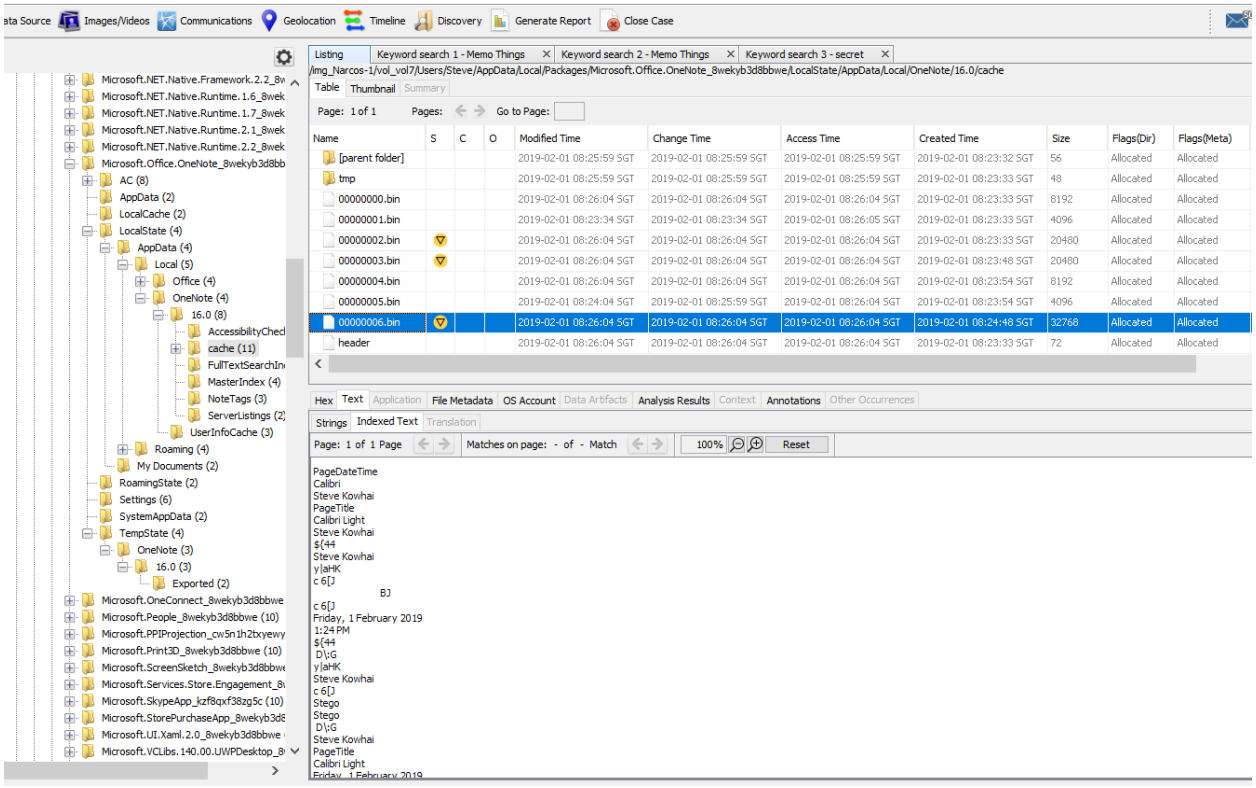


opsy 4.20.0

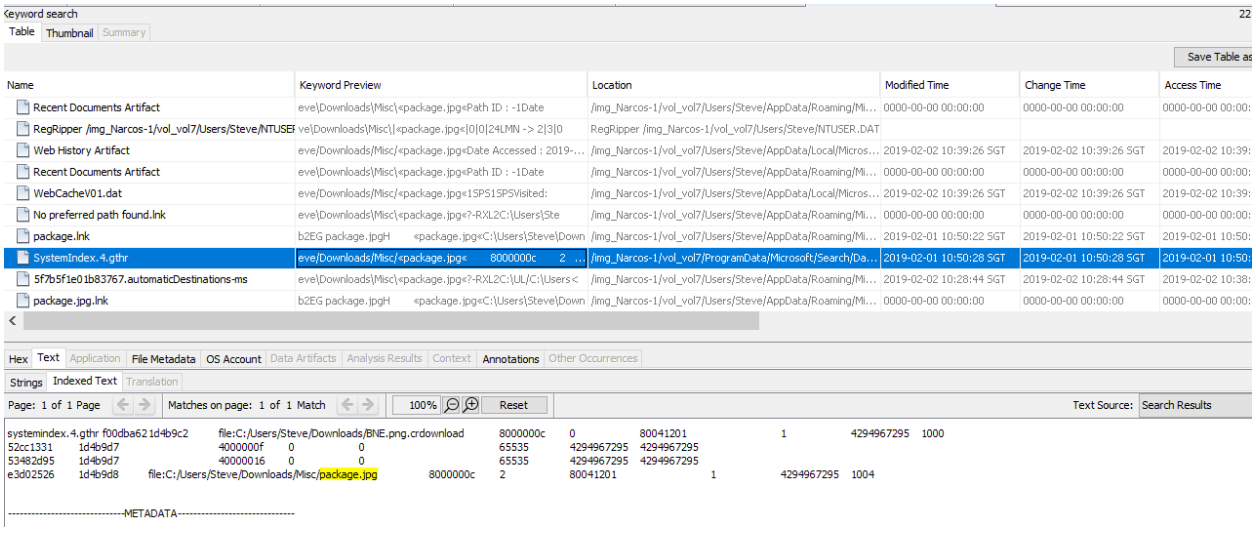
dow Help



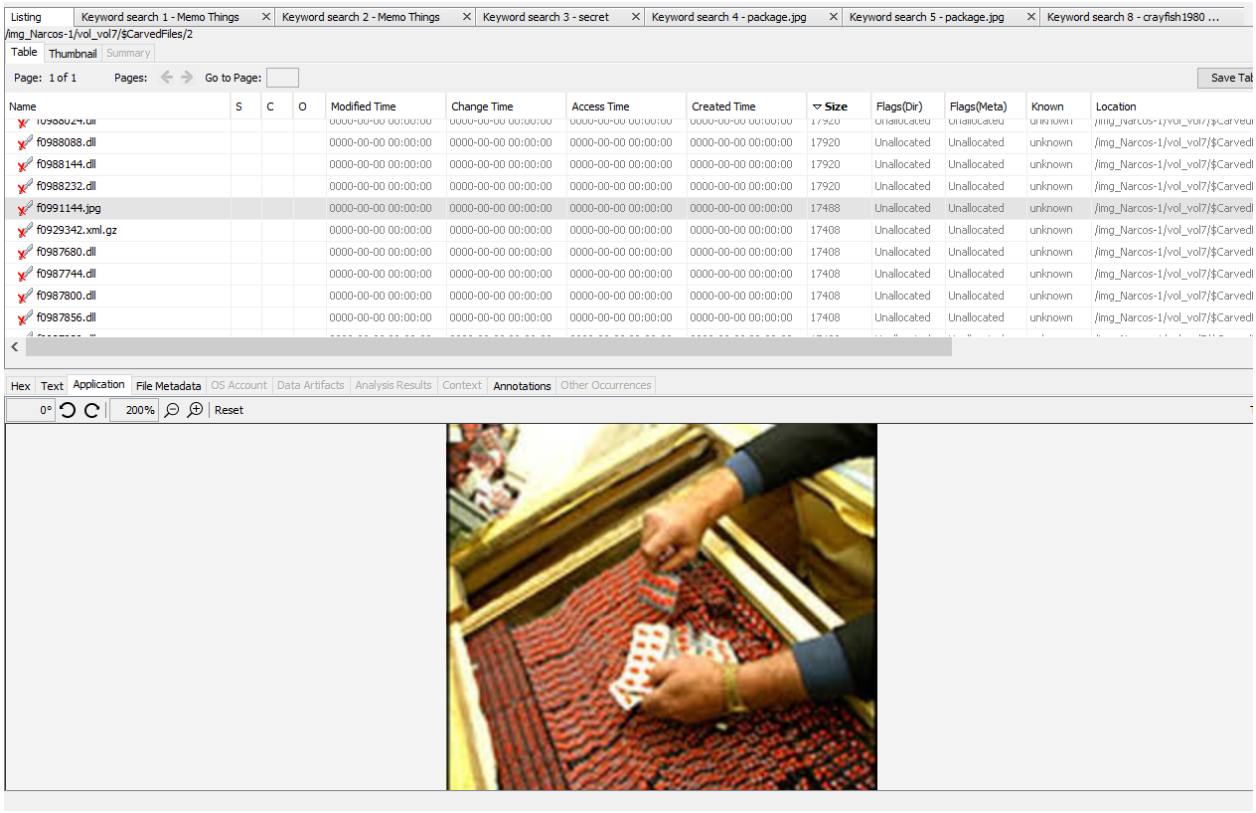
Possibly a read into steves notebook



Combi image?



Other interesting findings



/img_Narcos-1/vol_vol7/$CarvedFiles/2/f0991144.jpg

Things to find:

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

Listing

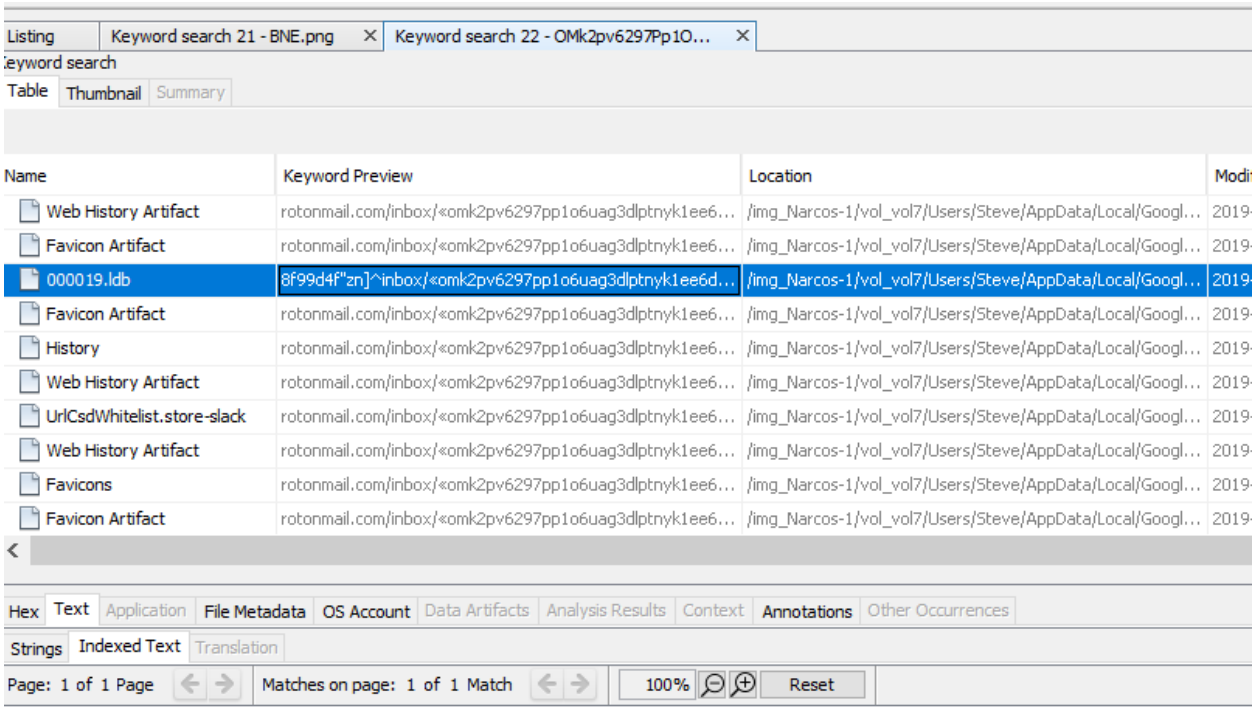
/img_Narcos-Combined.img/vol_vol7/Users/Steve/Downloads/Misc

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

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Ot

0° | 28% | Reset

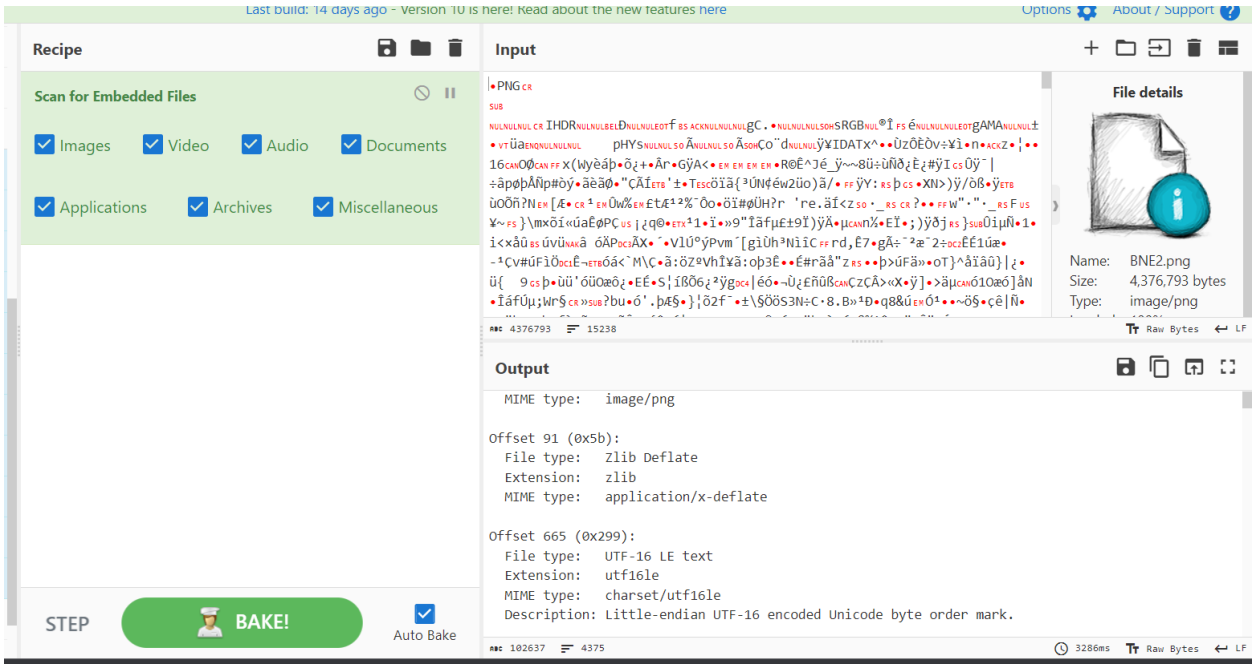



```
[000019.ldb, >5download,790f671d-7760-49c8-8443-458dcf3c6835
https://
^s.sourceforge.net/project/image-steg/Image%20Steganography%201.5.2%20Setup.exe?r=https%3A%2F%2F:]
s%2F
%2F&ts=1548980184&use_mirror=versaweb
,files/latest5P
*,^]1V.
"4e60ab90-88a00"J
Fri, 02 Sep 2011 10:10:24 GMTP
application/octet-streamb
C:\Users\Steve\Download
Unconfirmed 211922.crd:>
w(Image
xganography 1.5.2
(0etup.ex
                ,cca1d72f-06cd-4386-a85d-d286c6191f7f
Eblob:
!(mail.proton
com/f7f4f3a9-ba89-4f46-b2a8-c58bb8f99d4f
"zn]
^inbox/OMk2pv6297Pp1O6uag3DLPTnyK1ee6dVkZCT7kaMAS6Hi5ybCyevYuLxzsBwSWa5u-xmyY3XR_H51LXglEdjYw==*^
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