

3906ICT - Digital Forensics

Assessment 2: Major Assignment

Project: Forensic Analysis of Mr. Eason Hunter's Digital Assets.

Author: Yasin Çakar

S Number: 2921450

Table of Contents

Task I.....	4
I. Evidence A.....	4
i.I.1 Question 1: Who is the owner of the Desktop.....	5
i.I.2 Question 2: What programs have been installed on the desktop ? What recent programs have been run?.....	6
i.I.3 Question 3: Recover details of any files in the recycle bin.....	8
i.I.4 Question 4: Is there evidence that the owner of the desktop committed a crime?.....	8
II. Evidence B.....	9
i.II.1 Question 5: What applications are running on the memory dump computer?.....	9
i.II.2 Question 6: What web pages has the memory dump computer visited recently?.....	9
i.II.3 Question 7: What is email address of the owner of the memory dump computer?.....	10
i.II.4 Question 8: What is password of the memory dump computer?....	14
III. Evidence C.....	14
i.III.1 Question 9: Who are the people communicating in the transmission? When does the first transmission begin and the last transmission finish?.....	14
i.III.2 Question 10: What browsers and operating systems are used by the communication endpoints?.....	15
i.III.3 Question 11: What was sent for Benji to collect?.....	15
i.III.4 Question 12: Does the network capture reveal the relationship between Eason Hunter and the people participating in the intercepted communications?.....	16
IV. Evidence D.....	16
i.IV.1 Question 13: What are the non-stock applications installed on the phone? 16	
i.IV.2 Question 14: Who is in the contacts list? What messages and calls have been sent and received by the phone?.....	16
i.IV.3 Question 15: What Internet searches has the owner of the phone made? 17	
Question 16: Is there other evidence on the phone that might indicate the role of the owner in the bioweapon.....	17
i.IV.4 Question 17: Conduct a timeline analysis of the pieces of evidence.....	19

i.IV.5	Question 18: Provide a brief final analysis of the evidence and your conclusions.....	20
--------	---	----

Task II.....21

V.	Introduction.....	21
VI.	Evidence Acquisition.....	21
VII.	Forensic Analysis.....	22
VIII.	Forensic Tools.....	23
IX.	Conclusions.....	24

ii. Appendix.....25

Task I

I. Evidence A

Loading disk image:

```
cat EvidenceA.001 EvidenceA.002 EvidenceA.003 EvidenceA.004  
EvidenceA.005 EvidenceA.006 EvidenceA.007 EvidenceA.008  
EvidenceA.009 EvidenceA.010 EvidenceA.011 EvidenceA.012  
EvidenceA.013 EvidenceA.014 > boathouse.dd
```

Mount Image:

```
sudo mount -o ro,loop,offset=28672 boathouse.dd /mnt/windows_mount
```

i.I.1 Question 1: Who is the owner of the Desktop

The registered owner of the laptop is “Jim”, ownership analysis was conducted using two forensic methods one that queries for the registered owner and the second that queries the person who uses the computer most often, as shown below:

Method	Result
<pre>\$ rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/software -p winver</pre>	<div>ProductName Microsoft Windows XP</div> <div>CSDVersion Service Pack 3</div> <div>BuildLab 2600.xpsp.080413-2111</div> <div>RegisteredOrganization</div> <div>RegisteredOwner Jim</div> <div>InstallDate 2022-08-27 12:13:00Z</div>
<pre>rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/SAM -p samparse grep -C 9 "Login Count"</pre>	<div>Username : Jim [1003]</div> <div>Full Name : Jim</div> <div>User Comment :</div> <div>Account Type : Default Admin User</div> <div>Account Created : 2022-08-27 12:25:06Z</div> <div>Name :</div> <div>Last Login Date : 2022-08-28 05:29:30Z</div> <div>Pwd Reset Date : 2022-08-27 12:25:22Z</div> <div>Pwd Fail Date : 2022-08-28 05:29:23Z</div>

i.1.2 Question 2: What programs have been installed on the desktop ? What recent programs have been run?

There were 21 applications found to be installed on the device found in the Programs file directory:

```
sansforensics@siftworkstation: /mnt/windows_mount/Program Files
```

- 7-Zip
- ComPlus Applications
- Messenger
- Mozilla Firefox
- MSN Gaming Zone
- Outlook Express
- VMware
- WindowsUpdate
- Adobe
- Internet Explorer
- microsoft frontpage
- Mozilla Maintenance Service
- NetMeeting
- Uninstall Information
- Windows Media Player
- xerox
- IrfanView
- Movie Maker
- MSN
- Online Services
- VideoLAN
- Windows NT

The most recently run programs were VideoLAN, Mozilla Firefox, then Notepad respectively in that order.

Recent Apps	<pre>rip.pl -r /mnt/windows_mount/Documents\ and\ Settings/Jim/NTUSER.DAT -p runmru</pre>	<p>Launching runmru v.20200525</p> <p>runmru v.20200525</p> <p>(NTUSER.DAT) Gets contents of user's RunMRU key</p> <p>RunMru</p> <p>Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU</p> <p>LastWrite Time 2022-08-28 05:27:56Z</p> <p>MRUList = cba</p> <p>a notepad\1</p> <p>b firefox\1</p> <p>c vlc\1</p>
-------------	---	--

i.1.3 Question 3: Recover details of any files in the recycle bin.

In the recycling bin the following files were found:

- Dc1.txt
- Dc2.zip
- desktop.ini
- INFO2

The file Dc1.txt contained a string of characters that may have been an encrypted text. Dc2.zip contained two image files that were of type png and jpg the zip file was found to be password protected.

The INFO2 was a binary file leading to clues of two other text files. Following clues in the Recycler using information in INFO2 note1.txt and note2.txt was found in “Documents and Settings/Jim/My Documents”

```
$ cd /mnt/windows_mount/RECYCLER/S-1-5-21-790525478-1220945662-725345543-1003/
sansforensics@siftworkstation: /mnt/windows_mount/RECYCLER/S-1-5-21-790525478-1220945662-725345543-1003
$ ls -l
total 257
-rwxrwxrwx 1 root root    176 Aug 20 09:24 Dc1.txt
-rwxrwxrwx 1 root root 256110 Aug 20 08:12 Dc2.zip
-rwxrwxrwx 1 root root     65 Aug 28 05:20 desktop.ini
-rwxrwxrwx 1 root root   1620 Aug 28 05:29 INFO2

cd /mnt/windows_mount/Documents\ and\ Settings/Jim/My\ Documents/
ls -l
-rwxrwxrwx 1 root root     56 Aug 28 05:20  note1.txt
-rwxrwxrwx 1 root root     36 Aug 28 05:20  note2.txt
$ cat note1.txt
If I let you know where I'm going, I won't be on holiday
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/Jim/My Documents
$ cat note2.txt
Desperate times, desperate measures.
sansforensics@siftworkstation: cd /mnt/windows_mount/Documents and Settings/Jim/My Documents
```

i.1.4 Question 4: Is there evidence that the owner of the desktop committed a crime?

There no evidence of any cyber crime committed as the installed software were standard. The image files had suspicious names “bio-weapon.png” and “soviet-biological-warfare-installati.jpg”. The text files found in the My Documents directory were also suspicious to a degree. However the artifacts collected may lead to findings in a broader investigation.

II. Evidence B

Initial Analysis:

```
vol.py -f '/home/sansforensics/Downloads/evidence_B/Snapshot1.vmem' imageinfo
vol.py -f Snapshot1.vmem --profile=Win7SP1x64 hivelist
rip.pl -r registry.0xffffffff8a000baa010.SOFTWARE.reg -p winver
```

i.II.1 Question 5: What applications are running on the memory dump computer?

The running applications found on EASON-PC were the Chrome Web Browser, Thunderbird, MyNotepad++, and Internet explorer using the query:

```
vol.py -f Snapshot1.vmem --profile=Win7SP1x64 pslist | cat Running_Processes.txt
```

Two instances of “csrss.exe” processes were found in the process list, therefore a virus/malware presence is a likelihood as there should be one csrss.exe running at all times in a windows 7 Enterprise operating system

Using procdump , the sha-256 hash of the excutable files and the malware database on virustotal.com:

```
vol.py -f Snapshot1.vmem --profile=Win7SP1x64 procdump -p 328 -D Processes/csrss.exe/
vol.py -f Snapshot1.vmem --profile=Win7SP1x64 procdump -p 380 -D Processes/csrss.exe/
```

```
sudo sha256sum *
89e4ef8874af1f019714761d9904e82fa3f885d67a7c41ce905da7f43871a559 executable.328.exe
5fedadbe48e52505e0c13e7529c71d24d4618d7e3406f957e73724bb55ed5b8c executable.380.exe
```

None of the hashes above corresponded to a known virus/malware on virustotal.com

See Appendix 1 for for list of processes

i.II.2 Question 6: What web pages has the memory dump computer visited recently?

Based on the processes list the search history of the internet explorer browser and Chrome browsers were investigated:

The websites visited using interenet explorer were:

- <https://www.msn.com/?ocid=iehp> [2022-08-27 12:45:46 UTC+0000]
- <https://support.microsoft.com/internet-explorer> [2022-08-27 12:45:50 UTC+0000]
- @<https://www.google.com/search?hl=en-AU&source=hp&q=flight+morocco&iflsig=AJiK0e8AAAAAYwokDulOV3RYIAuYN94dY4wUE7pcNEAr&gbv=1> (GET request regarding flights to morrocco) [2022-08-27 13:03:03 UTC+0000]
- Flight Center (https://www.google.com/url?q=https://www.flightcentre.com.au/morocco/flights&sa=U&ved=2ahUKewiQ9ti0iuf5AhVK4TgGHbzJBTEQFnoECAoQAg&usg=AOvVaw29S2Sgg_U2GdEyHb3DlbkI) [2022-08-27 13:03:06 UTC+0000]
- A google search for the term syndicate (<https://www.google.com/search?hl=en-AU&gbv=1&oq=&aqs=&q=syndicate>) [2022-08-27 13:03:24 UTC+0000]
- A Wikipedia page on “Syndicate” (<https://www.google.com/url?q=https://en.wikipedia.org/wiki/Syndicate&sa=U&ved=2ahUKewjima9iuf>

[5AhW7xDgGHajCAMQQFXoECAUQAg&usg=AOvVaw2KKAm60k6iezT6_PUHj1j1](https://www.google.com/search?hl=en-AU&gbv=1&oq=&aqs=&q=sunscreen)) [2022-08-27 13:03:25 UTC+0000]

- google.com [2022-08-27 13:03:36 UTC+0000]
- Google search for sunscreen (<https://www.google.com/search?hl=en-AU&gbv=1&oq=&aqs=&q=sunscreen>) [2022-08-27 13:03:37 UTC+0000]
- Sunscreen on chemist warehouse (<https://www.google.com/url?q=https://www.chemistwarehouse.com.au/shop-online/214/sunscreen,-lotions-gels&sa=U&ved=2ahUKEw1w4PFiuf5AhUT3TgGHSVMA1wQFnoECAoQAg&usg=AOvVaw0Dq0KAMm72n5fYxJHPtCUW>) [2022-08-27 13:03:39 UTC+0000]
- www.chemistwarehouse.com.au [2022-08-27 13:03:42 UTC+0000]
- Sunscreens lotions and gels on chemist warehouse (<https://www.chemistwarehouse.com.au/category/shop-online/214/sunscreen,-lotions-gels>) [2022-08-27 13:03:43 UTC+0000]
- Sailing to morrocoy on bing search engine (<http://www.bing.com/search?q=sail+morocco&src=IE-SearchBox&FORM=IE8SRC>) [2022-08-27 13:04:15 UTC+0000]
- www.bing.com [2022-08-27 13:04:15 UTC+0000]
- Sailing to morrocoy on yatching world.com (<https://www.yachtingworld.com/cruising/sailing-morocco-atlas-coast-123680>) [2022-08-27 13:04:18 UTC+0000]

Using the query:

```
vol.py -f Snapshot1.vmem --profile=Win7SP1x64 iehistory -p 3656 >
'/home/sansforensics/Downloads/evidence_B/IE_History/ie_history.txt'
```

The search terms “sunscreen”, “sailing from uk to Morocco”, “syndicate” and “flight Morocco” were made on the chrome browser.

This information was retrieved using the query:

```
vol.py --plugins=plugins/ -f Snapshot1.vmem --profile=Win7SP1x64 chromesearchterms
```

i.II.3 Question 7: What is email address of the owner of the memory dump computer?

Eason’s email address is “ht317117@gmail.com” after finding thunderbird.exe on the process list the filesystem for the thunderbird application was investigated as follows:

Procedure	<p>vol.py -f Snapshot1.vmem --profile=Win7SP1x64 filescan grep -i Thunderbird</p> <p>"0x000000007e258b70 16 0 RW-rw- \Device\HarddiskVolume1\Users\Eason\AppData\Roaming\Thunderbird\Profiles\nsxx2nq9.default-release\ImapMail\imap.gmail.com\[Gmail].sbd\All Mail"</p> <p>vol.py -f Snapshot1.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007e258b70 -D '/home/sansforensics/Downloads/evidence_B/Email'</p>
Source:	file.None.0xfffffa801a4451e0.dat
Email Messages	
Email #3	
Base64 Encoded	Base64 Decoded
<p>SGkgRWFzb24sDQoNCkEgYmV0dGVyIEFuZHIvaWQgZXhwZXJpZW5jZSBpcyB3YWl0aW5nDQoNCiRh</p> <p>a2Ugb25lIG1pbmV0ZSB0byBzZXQgdXAgeW91ciBwaG9uZSB3aXR0Edvb2dsZQ0KDQpHZXQgc3Rh</p> <p>cnRIZCAgDQo8aHR0cHM6Ly9ub3RpZmlyYXRPb25zLmdvb2dsZS5jb20vZy9wL0FQTkwvGk1RHZf</p> <p>NTZRRjBEbjZMzMzNxaDNfRnNicEFFN3JBTK83V2VIM08yRlFCMmJVMHpTTkVwQIB1TE9QNKpTU3Va</p> <p>d3AzNmpfZlYyOUtjRGJMa0V4MlIDbjNvSnowT0tyQ0JZa0ZKMxhPUUYzTG12OVdscFZqZDU4YVhi</p> <p>cG9DUzdscHR3WG9PWDRZb1YyWmZJelNBXNRkdFVYQm5kQlJWb2FiMktaaFE0VHBSRUZtOGhsZzRt</p> <p>VjV1ZmUwUkc5RjFXLUhlc2dVNC1Wb1BfQWF4QzIWSktiOVFrNkIC09wdzV5Zkl5V0pPSzRuekQt</p> <p>bTF3bWITakJBTHM2Y21tWDAzMDRWB0MybFFMNkdUamhEMjl6SnI5aTNWX19RSm5QQTJwc3FibHIJ</p> <p>N2VNTFJjUXdtbmpRNVP4aHREaUJjeHU1ME0xcG1uTmZFaW5tVkp0SmNqTE40ZHdHRIZnWUlpTmMx</p>	<p>Hi Eason,</p> <p>A better Android experience is waiting</p> <p>Take one minute to set up your phone with Google</p> <p>Get started</p> <p><<a 900="" 914="" 938"="" 967="" data-label="Page-Footer" href="https://notifications.google.com/g/p/APNL1Ti5Dv_56QF0Dv3Y33qh3_FsepAE7rANO7Wee3O2FQB2bU0zSNEpBPuLOP6JSSuZwp36j_fv29KcDbLkEx2YCN3oJz0OKrCBYkFJ1xOQF3Lb69WlpVjd58aXbpoCS7lptwXoOX4YoV2ZflzSA5tdtUXBndBRVo1b2KZhQ4TpREFm8hlg4mV5ufe0RG9F1W-HHsgU4-VoP_AaxC9VJKb9Qk6IBwOpw5yflyWJOK4nzD-m1wmiSjBALs6cmmX0304VoC2iQL6GTjhD29zJr9i3V__QJnPA2psqHlyl7eMLRcQwmnjQ5ZxhtDiBcxu50M1pmnNfEinmVJtJcJLN4dwGFVMYliNc1VIYX7il4L_YLvK3ZzwXo0NF4FPX2lh9JWxrpwsdwawlkshMwCDvsS62HnPY5ljtEf17E_KSjaZeFrAlfGePs6hAEeL09eSGHEzqkquAjwQMQ_O2ALSxX0gshY9-WM-O13RpwWC6pH70XJg-yDDrRmt42xLYRvelFuJfZGby4ARI-EaEWp4rqSdsyOolPa3YEBH8l8G3cr08FgEE1l7vgWhEq-Phax0AxYwBB6rh1mnT4HMYjTjzOhz4YhOJg90UNSNLqOyEkr6bf-G8t2OoDIkoUNShE6j7Tu1X-xsqCqWXEVuJB1GPSmKowwIhPQKV_SI31EofW9M_fFhOcou6Ya73YOJDIXo91G7z11a5ISYAJRnnWdbliBBLzp2GMkAg10Q7T-vcdNWT1fcF-1tIBDHKzf7vx46-2J7t7SlqoGxhz></p> </td></tr> </table> </div> <div data-bbox=">Page 11</p>

VmxZWDdpSTRMX1IMdmszWnp3WG8wTkY
0RIBYMkloOUpXeHJwd3Nkd2F3SWtzaE13Q
0R2c1M2Mkhu

UFk1SWp0RWZsN0VfS1NqYVplRnJBbGZH
ZVBzNmhbBRVWVMMDIU0dlRXpxa3F1QWp3
UU1RX08yQUxT

eFgwZ3NoWTktV00tTzEzUnB3V0M2cEg3MF
hKZy15RERyUm10NDJ4TFISdmVsZnVKZlp
HYnk0QVJJ

LUVhRVdwNHJxU2RzeU9vbFBhM1IFQkg4S
ThHM2NyMDhGZ0VFMWw3dmdXaEVxLVBo
YXgwQXhZd0JC

NnJoMW1uVDRITVlqVGp6T2h6NFloT0pnOT
BVTINOTkxxT3lFa3l2YmYtRzh0Mk9vRGxrb1
VOU0hl

Nmo3VHUxWC14c3FDYXFXWEVWdUpCM
UdQU21Lb3d3SWWhQUUtWX1NJmzFFb2ZX
OU1fZkZoT2NvdWw2

WWE3M1IPSKRJWG85MUc3ekkxYTVsU1IB
SIJubldKYkjpQkJMenAyR01rQWcxMFE3VC1
2Y2ROV1Qx

ZmNGLTF0SUJESEt6Zjd2eDQ2LTJKN3Q3U
0lxb0d4aHo+DQoNCIRoaXMgZW1haWwgd2
FzIHNIbnQg

dG8gaHQzMTcxMTdAZ21haWwuY29tIDxod
DMxNzExN0BnbWFpbC5jb20+IGJlY2F1c2Ug
eW91ICAN

CnJIY2VudGx5IHNPZ25lZCBpbmRvIHlvdXlIgR
29vZ2xllEFjY291bnQgb24geW91ciBHb29nb
GUg

RW11YWx0b3lgZGV2aWNiLiBJZiAgDQp5b3
UgZG8gbm90IHdpdGgG8gcmVjZWl2ZSBib
WFpbHMg

dG8gaGVscCB5b3Ugc2V0IHVwIHlvdXlIgZGV
2aWNiIHdpdGgglA0KR29vZ2xllHdoZW4geW
91IHNP

Z24gaW50byB5b3VyIGFjY291bnQgb24gdGh
lIGRldmJlZSBmb3lmdGhllGZpcnN0IHhRpbWUs
ICAN

CnBsZWFzZSB1bnN1YnNjcmlZSAgDQo8aH
R0cHM6Ly9ub3RpbmJlYXRpb25zLmdvb2dsZ
S5jb20v

Zy9wL0FQTkwxVGJlS2FnVE1ybWJnWDhfVk
loMjR5bTlZREpCWlc1Qlc4Q0VuQXBYTndLe

This email was sent to ht317117@gmail.com <ht317117@gmail.com> because you recently signed into your Google Account on your Google Emualtor device. If you do not wish to receive emails to help you set up your device with Google when you sign into your account on the device for the first time, please unsubscribe

<https://notifications.google.com/g/p/APNL1TilKagTMrmbgX8_Vlh24ym9sDJBZW5BW8CEApXNwKyIBABNvBBZhGDkh1vW1MFAI5K0jgNCZ4XL_SK7bUHTFCjM9tHVo5jUkVqQfHjGgb_rOfyNDWz9xHPQWLG0-EZUE7cqnyaZZSMQXoJTUHbyFStnHIBW_Mh2BFZ98rBF6td5CfXqW5XOhpIK5eIIS4q5kuXyBcXcRboWD2_gR-POdHuPHJ3TQQfWbYFX6RXsRC7j1GAhliWRMqseMzO3kQAQujhfbmJ64HnjpdVMA-EkB6shgVKxzlpamWHcsVe__4>.

© 2022 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043
4M4M4N[1wě -u

<div>WICQUJO</div> <div>dkJCWmhHRGtoMXZXMU1GQWw1SzBqZ05DWjRYTF9TSzdiVUhURkNqTTI0SFZvNWpVa1ZxUWZlakdn</div> <div>YI9yT2Z5TkRXejl4SFBRV0xHMC1FWIVFN2NxbnlhWlpTTVFYb0pUVUhieUZTdG5IbEJXX01oMkJG</div> <div>Wjk4ckJGNnRkNUNmWHFXNVhPaHBsSzVlSUITNHE1a3VYeUJjWGNSYm9XRDJfZ1ItUE9kSHVQSEoz</div> <div>VFFRZldiWUZYNIJYc1JDN2oxR0FoSWIXUk1xc2VNek8za1FBUXVqaGZibUo2NEhuanBkVk1BLUVr</div> <div>QjZzaGdWS3h6SXBhbVdIY3NWZV9fND4uDQoNCsKplDlwMjlgR29vZ2xIIExMQyAxNjAwIEFtcGhp</div> <div>dGhIYXRyZSBQYXJrd2F5LCBNb3VudGFpbiBWaWV3LCBDQSA5NDA0Mw0K</div> <div>--0000000000005b35d305e6f58eda</div>	
--	--

See Appendix 2 to see all mails.

i.II.4 Question 8: What is password of the memory dump computer?

The password retrieved from the memory dump was “N0Tthing1simp033ible”

Using the query:

```
vol.py -f Snapshot1.vmem --profile=Win7SP1x64 lsadump >
'/home/sansforensics/Downloads/evidence_B/Password and LSA Keys/lsadump'
```

III. Evidence C

i.III.1 Question 9: Who are the people communicating in the transmission? When does the first transmission begin and the last transmission finish?

The first transmission is at 2022-08-28T02:06:33.094Z initiated by Eason, the last transmission occurs on 2022-08-28T02:20:58.647Z by a chat member aliasd as Syndicate2. The whole chat can be seen below:

Time	Person	Message
2022-08-28T02:06:33.094Z	Eason	Benji, read this message carefully. I might not have much time left
2022-08-28T02:06:46.030Z	Benji	What's wrong Eason?
2022-08-28T02:06:58.107Z	Eason	Erika Sloane asked me to deliver a package from the Russian embassy in London to Morocco. But it wasnt the real embassy.
2022-08-28T02:07:08.892Z	Benji	What are you talking Eason? Erika Sloane? That Erika Sloane?
2022-08-28T02:07:20.726Z	Eason	I have some insurance, in case this whole thing blows up. Its in the usual place. Promise me you will store it in a safe place.
2022-08-28T02:07:31.836Z	Benji	For sure my friend. I will upload it to my Onedrive. Stay safe
2022-08-28T02:07:42.549Z	Eason	Thx.
2022-08-28T02:09:28.542Z	Tony	Eason, the bioweapons came from a previous Soviet biological weapons program
2022-08-28T02:09:50.266Z	Eason	Thanks, Tony. I owe you one.
2022-08-28T02:10:21.807Z","	Tony	Buy me some KFC next time when you are in the office
2022-08-28T02:10:34.556Z	Eason	I don't know if I can come back
2022-08-28T02:10:46.128Z	Tony	Its just KFC. don't be stingy
2022-08-28T02:14:46.186Z	Tony	I just did Eason a favour but he is not willing to buy KFC for me
2022-08-28T02:14:58.511Z	Benji	idk. he sounds a bit under the weather today
2022-08-28T02:15:07.670Z	Tony	I know right
2022-08-28T02:15:27.217Z	Benji	He asked me to store something for him, but I dont know. I have no space on my one drive.

2022-08-28T02:15:41.093Z	Tony	Free for coffee?
2022-08-28T02:15:55.121Z	Tony	where to meet?
2022-08-28T02:16:13.317Z	Benji	where to meet indeed
2022-08-28T02:20:22.701Z	Syndicate1	Benji Dunn just downloaded something from the drop zone. Its encrypted.
2022-08-28T02:20:36.021Z	Syndicate2	Dont worry we are on the inside. I will upload the key.
2022-08-28T02:20:53.507Z	Syndicate1	From Dunn's PC?
2022-08-28T02:20:58.647Z	Syndicate2	Yes

After viewing the network traffic on wire shark, the mIRC chat structure was of messages stored was recolved. The following instruction was executed to retrieved all chats:

```
strings EvidenceC.pcap | grep -ic msg
strings EvidenceC.pcap | grep -C 9 msg | cat >
'/home/sansforensics/Downloads/evidence_C/msg.txt'
```

The participants of the chat are Benji Saulson, Tony, Eason, Syndicate1 and Syndicate2

i.III.2 Question 10: What browsers and operating systems are used by the communication endpoints?

The operating systems used are: Ubuntu, Windows NT 6.1, Macintosh. And the operating systems are: Firefox/91.0, Safari/537.36, Safari/601.3.9, Safari/537.36, Firefox/15.0.1.

This information can be gathered by tracing http GET headers on wireshark or doing a grep search on the EvidenceC.pcap file as follows:

```
strings EvidenceC.pcap | grep -iE "User-Agent:" | uniq
```

i.III.3 Question 11: What was sent for Benji to collect?

From the chat it is deducible that the item is a digital asset from Benji's dialog "For sure my friend. I will upload it to my Onedrive. Stay safe" and "He asked me to store something for him, but I dont know. I have no space on my one drive.". The item is of value as Eason refers to it as his "insurance" which is in its "usual place". This could be the bioweapon file in the recycling bin found on an old laptop on a boathouse near Hunter's house. This could be the bioweapon file found in the Recycle bin in EvidenceA as it too was encrypted as Syndicate1 says "Benji Dunn just downloaded something from the drop zone. Its encrypted."

As no explicit reference was made to the digital asset it is not clear what it may have been, however there is ground for suspicion it would be the file mentioned. As no context is given it could be some sort of leverage related to the case that is not the bioweapon file itself.

i.III.4 Question 12: Does the network capture reveal the relationship between Eason Hunter and the people participating in the intercepted communications?

The participants in the chat seem to be Mr. Hunters colleagues as the mIRC chat room is named “FederalLawEnforcementAgency ” see Appendix 3 for a full copy of the intercepted chat with the relevant meta-data. The chat was retrieved using the query in Question 9.

IV. Evidence D

i.IV.1 Question 13: What are the non-stock applications installed on the phone?

The non stock applications seem to be all the APK files in the dm-1 disk image, they are:

```
bubblesooter.orig-z8mJLeCzHzCg32ex5gy2aw==/base.apk
com.facebook.katana-o0Et3oUg_G0Le6fwo_Pb1A==/base.apk
com.rovio.angrybirds-d1xvsHqwbR3wyJJPUnfDA==/base.apk
com.tencent.mm-eJ99iI_SfXYx1pDwbXPjUg==/base.apk
com.twitter.android-ualDxAgdi2NTp6NucGhilA==/base.apk
```

The application files can be retrieved using `sudo mount -o loop,ro,noexec,noload <disk_img> /mnt/e01`

Where disk_img can be: dm-0, dm-1,vda1 or vde1.

The complete list of all applications can be found in Appendix 5.

i.IV.2 Question 14: Who is in the contacts list? What messages and calls have been sent and received by the phone?

Eason Hunter only has three contacts:

Name	Contact_last_updated_timestamp	X_last_time_contacted	Last_time_contacted	Times_contacted
Saulson, Benji	Wed 24 Aug 2022 04:41:30 AM UTC	Wed 24 Aug 2022 04:41:30 AM UTC	(1661316048.000) Wed 24 Aug 2022 04:40:48 AM UTC	2
Tony	Wed 24 Aug 2022 04:40:53 AM UTC		0	0
Sloane, Erika	Wed 24 Aug 2022 04:39:45 AM UTC		0	0

The data above was verified using the following queries:

```
sudo mount dm-1 /mnt/e01
sudo su
cd /mnt/e01/data/com.android.providers.contacts/databases/
cp contacts2.db '/home/sansforensics/Downloads/Evidence_D/Investigation/contacts/dm-1'
sudo chown sansforensics:sansforensics '/home/sansforensics/Downloads/Evidence_D/Investigation/contacts/dm-1/contacts2.db'
exit
sudo umount /mnt/e01
```

contacts2.db -> view_contacts

Only one call was made to the number 11188899966 on Wed 24 Aug 2022 04:40:48 AM UTC for 39 seconds as shown below:

ID	Number	Date	Duration
1	11188899966	(1661316048298) Wed 24 Aug 2022 04:40:48 AM UTC	39

This information was retrieved using the queries:

```
sudo mount dm-1 /mnt/e01
sudo su
cd /mnt/e01/data/com.android.providers.contacts/databases/calllog
cp calllog.db '/home/sansforensics/Downloads/ Evidence_D/Investigation/calllog/'
exit
sudo umount /mnt/e01
sudo chown sansforensics:sansforensics '/home/sansforensics/Downloads/
Evidence_D/Investigation/calllog/calllog.db'
```

Calllog.db -> calls

i.IV.3 Question 15: What Internet searches has the owner of the phone made?

According to the investigation no web searches were made. This conclusion was reached after accessing the “~data/com.android.chrome/app_chrome/Default/” directory:

```
$ sudo mount -o loop,ro,noexec,noload dm-1 /mnt/e01
$ sudo su
$ cd /mnt/e01/data/com.android.chrome/app_chrome/Default/
$ ls
blob_storage          Favicons-journal      NTPSnippets
previews_opt_out.db-journal 'Web Data'
Cookies              History                'Offline Pages'
README               'Web Data-journal'
Cookies-journal       History-journal        page_load_capping_opt_out.db
'Sync Data'
data_reduction_proxy_leveladb 'Local Storage'
page_load_capping_opt_out.db-journal 'Top Sites'
'Download Service'    'Login Data'          Preferences
'Top Sites-journal'
Favicons              'Login Data-journal'  previews_opt_out.db
'Visited Links'
$ cp -r . '/home/sansforensics/Downloads/ Evidence_D/Investigation/Search_History'
```

Question 16: Is there other evidence on the phone that might indicate the role of the owner in the bioweapon theft?

The following table shows the sms messages exchanged from Eason’s phone:

_id	Date	index_text
1	Wed 24 Aug 2022 04:42:53 AM UTC	Eason, we have a new mission for you. We will need you to deliver these three boxes to this address “6 Grosvenor Gardens, London SW1W 0DH” now

2	Wed 24 Aug 2022 04:43:38 AM UTC	Yes, ma'am
3	Wed 24 Aug 2022 04:43:55 AM UTC	The recipient is the "Syndicate", and the code is "Apostles"
4	Wed 24 Aug 2022 04:44:06 AM UTC	Yes ma'am
5	Wed 24 Aug 2022 04:44:18 AM UTC	Remember, you have to dress like a Uber delivery guy
6	Wed 24 Aug 2022 04:44:34 AM UTC	Yes ma'am
7	Wed 24 Aug 2022 04:44:51 AM UTC	May I know what's inside?
8	Wed 24 Aug 2022 04:45:04 AM UTC	You ask too much
9	Wed 24 Aug 2022 04:45:15 AM UTC	I am sorry ma'am
10	Wed 24 Aug 2022 04:46:50 AM UTC	Uber eats for Syndicate
11	Wed 24 Aug 2022 04:47:01 AM UTC	The code?
12	Wed 24 Aug 2022 04:47:11 AM UTC	Apostles
13	Wed 24 Aug 2022 04:47:22 AM UTC	Yes, that's my order
14	Wed 24 Aug 2022 04:47:40 AM UTC	Thanks, Enjoy your night, sir

The dates were derived from mmssms.db->sms

The fields _id and index_text were derived from mmssms.db->words

This data was obtained using the queries below:

```

sudo mount dm-1 /mnt/e01
sudo su
cd /mnt/e01/user_de/0/com.android.providers.telephony/databases
cp telephony.db '/home/sansforensics/Downloads/
Evidence_D/Investigation/sms/dm-1'
cp mmssms.db '/home/sansforensics/Downloads/
Evidence_D/Investigation/sms/dm-1'
exit
sudo umount /mnt/e01

sudo chown sansforensics:sansforensics '/home/sansforensics/Downloads/
Evidence_D/Investigation/sms/dm-1/telephony.db'
sudo chown sansforensics:sansforensics '/home/sansforensics/Downloads/
Evidence_D/Investigation/sms/dm-1/mmssms.db'

```

The sms messages captured, suggest a likelihood of the owner or the person managing the operation of a secret delivery operation, which could likely be the bioweapon. In the sms communication Eason is asked to deliver a package to London, in the mIRC chat Eason is asked to deliver a package from the Russian embassy in London to Morocco. There seems to be two deliveries handled by Eason.

The question for Eason is the texting Eason also Erika Sloane? The other important question is what is her role between the owners of the bioweapon and Eason? Is she a colleague of Eason in the Federal Law Enforcement Agency since she is in Eason's contact list on this Nexus phone? Another question that arises is, is she collaborating with fugitives?

i.IV.4 Question 17: Conduct a timeline analysis of the pieces of evidence.

The Table below shows the order of events as they occurred according to the forensic analysis of the laptop found on a boat house, Eason's work PC and his Android smartphone:

Order of Events	Date	Activity
1	24 Aug 2022 04:41:30	Eason receives a call that lasts for 39 seconds
2	24 Aug 2022 04:42:53 to 04:42:53	Eason is communicating with a female who is giving instructions to Eason regarding a delivery of a packet to London.
3	27 Aug 2022 12:13:00	Windows XP operating system is installed on a laptop found in the boat house. The laptop is Registered to a "Jim:
4	27 Aug 2022 12:25:06	An account is created on the Windows XP laptop.
5	27 Aug 2022 12:45:46 to 13:04:18	Web searches are made on Eason's work computer in the following order. <ol style="list-style-type: none"> 1. Flights to Morocco on the Flight Centre website 2. Searches the term "Syndicate" on Wikipedia after obtaining Google search query results. 3. A web search is made for "Sunscreen" on google search engine. Then he click a link that directs him to Chemist Warehouse. 4. Search for "Sunscreens, gels & lotions" on Chemist Warehouse 5. Searches "Sailing to Morocco" on the Bing search engine. 6. The same search ""Sailing to Morocco" is made on yatchingworld.com
6	28 Aug 2022 05:20:00	Two files are created in the laptop found in the boat house: note1.txt If I let you know where I'm going, I won't be on holiday note2.txt Desperate times, desperate measures.
7	28 Aug 2022 06:33:00 to 20:58:00	Eason appears to have a chat with his colleagues on mIRC with his work computer regarding a delivery he made of a "package" from the Russian Embassy in London. He also mentions the bioweapons and asks Benji for a favour to store a digital asset into a safe place. He refers to it as his "insurance".

i.IV.5 Question 18: Provide a brief final analysis of the evidence and your conclusions.

Eason receives a phone call that lasts for 39 seconds, after 44 minutes he receives instructions from a female that instructs Mr. Hunter to deliver a "package" to an address in London. He is instructed how to carry out the covert operation, the recipient, and the passcode to use during the exchange. The content of the package is kept secret from Mr Hunter. This could be the Russian Embassy.

Three days later Windows XP SP3 is stalled on a laptop under the name “Jim”. Two picture files are found locked with password protection in the Recycle bin named “bio-weapon.png” and “soviet-biological-warfare-installati.jpg”, a document with a string of unintelligible characters that may be an encryption or key.

On the same day twenty-five minutes later from 12:45 to 13:04, on Mr. Hunter's work computer, someone is searching for flights to Morocco, then searching the term “Syndicate”. Mr. Hunter then moves on to search for sunscreen, gels and lotion on the Chemist Warehouse website. Afterwards Mr Hunter is searching for a sailing option from London to Morocco.

Two days later at 5:20am, two files are created that writes “If I let you know where I’m going, I won’t be on holiday” and “Desperate times, desperate measures”. These files were created on a laptop that was found and seized on a boathouse near Mr. Hunter’s place of residence.

On the same day, on 28th August, an hour and thirty-three minutes later, Mr. Hunter is on a mIRC chat on his PC at work. The chat room seems to be among his colleagues at NACA.

A text document with a string of characters that is unintelligible, possibly a hash, a key. As well as a password protected file was found in the seized laptop. These items were created on the 20th of August.

An interesting finding observation was that two processes called “csrss.exe”, Windows 7 Enterprise operating systems are meant to contain only one instance of such process.

Further investigations are required about tasks conducted on Mr. Hunter’s work PC and further analysis is required to determine if a virus or malware could have been present that played a role in compromising the mission.

The Jury will need an extensive cross examination to determine who the lady on the phone was, was it Erika Sloane? Another pertinent question is how Mr. Hunter was given details of the “wrong” embassy; how can Erika make such a mistake? How Mr Eason make such a mistake? How can staff from NACA be so negligent?

Another important question is what is the contents of Dc.txt is it the key Syndicate2 mentioned in the online chat?

Why did Mr. Eason first look for flights to Morocco, then looked into travelling by Yacht? Were there such directives from the NACA or was it Mr. Hunter's prerogative?

The forensic evidence in this document begs for specific questions that need satisfactory testimonies. What was the “package” Erika asked Mr. Hunter to deliver to Morocco in Question? And what was in the three boxes that needed to be delivered to “6 Grosvenor Gardens, London SW1W 0DH”? And is the “package” and the three boxes related to the mission.

Regarding the laptop seized from the boathouse, another question arises, which is who is Jim? Or is it an Alias of one of the agents in NACA.

How can Erika and Mr. Hunter explain their version of event that aligns with the forensic evidence in question 17? Did they both make a mistake, or are they both accomplices or is one of them a corrupt agent?

In conclusion, the forensics analysis results elicit pertinent questions that require testimonies that align with the sequence of events in the timeline analysis.

Task II

V. Introduction

The purpose of memory forensics is to provide insights into the runtime system activity. Sometimes forensic memory analysis in volatile memory can reveal more than forensic disk analysis as programs and processes that

are run are put into memory. This means the candid true state of a process will be revealed as each running processes must show in memory as it is processed as they cannot be concealed from the operating system.

Memory analysis ensures a clear insight of the systems processes for when the memory snapshot was taken as all processes are revealed including encrypted documents of the drives that must be decrypted in order to run. For this reason, memory analysis can be the first step before forensic disk analysis as there are many ways of hiding or blocking access to data on the disk. Memory analysis can solve many such mysteries and provide directions for other digital forensic activities.

Memory analysis can also support a hypothesis about an event or sequence of events that is the subject of the investigation. Initial memory analysis can also assist in disk forensics as mentioned as there can be too much data in non-volatile memory, a live snapshot analysis may assist in identifying processes and their related activities such as executable files, devices associated to the process, shared memory used among processes, network connections established.

Analysing volatile memory allows the expert to understand how the process is running, it is an indispensable resource to investigate problems in two broad categories which are stealthy malicious code activity or causes of application or system failures.

A memory dump analysed in this analysis is only a snapshot of processes running when the memory snapshot was captured. This is analogous to capturing a frame in a video clip, meaning there were processes prior to the snapshot and the processes on the system will move on after the point in time the snapshot is taken.

Memory dumps obtained at the right time can reveal activities for debugging, such as incorrect configurations or malicious code activity, or for experience enhancement such as analysing crash dumps from page files.

Memory forensics is however particularly useful to analyse malicious code as traditional security software tools may struggle to identify stealthy malware written to volatile memory and uncover malicious activity such as fileless malware and RAM scrapers. These types of malicious activities are undetectable by traditional file-type based tools.

As such malicious codes are not stored on the systems file system, they are persistent on the host system through various means including remote exploitable systems, creating services that may run on bootup or login that in turn download a new piece of malware and run it on the machine, or create registry keys.

Memory analysis is most important forensics methods for fileless malwares as they not use the files system and operate on the computer's volatile memory to inject code using the tools trusted by the computers operating system.

VI. Evidence Acquisition

Volatile data is the data stored in temporary memory on a computer while its running. When a computer system is powered off, volatile data is lost almost immediately. Data that is relevant according to ISO2042 and to a broader investigation would ideally take place when the memory dump capture occurs at the right instant where the processes of interest occurred during memory capture.

A memory dump will always contain usernames and passwords, open clipboard or window contents at the time as well as fifty to ninety-eight percent of recent registry logs at the time.

The easiest memory acquisition process are conducted on virtual machines as the memory is readily stored in a ".vmem" file within the folder the virtual machine is running.

Acquisition of volatile memory is optimal when the system is up and running, however a full memory dump can also be obtained if the system crashes. This is because at that instant the computer takes a snapshot of memory for debugging and stores the last state into a crash dump file.

In cases where a device is put on hibernate, the hibernation file can be accessed if the system is not put on hibernate for a second time, hibernation files can be observed like memory.

However if the system is running the best case scenario is there is root access, for which there are command line tools in windows and Linux as well as downloadable non-stock application to perform memory dumps without interrupting ongoing processes.

For both Microsoft and Linux systems the built in command “dd” for disk dump can be used to acquire a memory dump. In Windows systems the command pmdump can be used for a particular process, or userdump which is Microsoft’s own internal suite. Linux also has the LiME memory extractor that allows acquiring memory either to the file system of the device or over a network. In Linux systems since everything is seen as a file including storage volumes, the memory can be found in /dev/fmem as a file.

Since digital artifacts are easier to tamper with compared to forensic artifacts in disciplines of natural sciences a digital signature of the memory dump using a hash function is required to verify clones of the original artifact before the examination phase of the digital forensics process.

VII. Forensic Analysis

After verifying the hash digest for data integrity in compliance with the chain of custody requirements. Process IDs help tracing sophisticated activities such as crashes occurring due to misconfigurations, the obscure activities of fileless malware that inject malicious code using tools whitelisted by the operating system can be investigated.

Processes can be linked with other processes, events, registry logs and networking activities through their process IDs.

Processes are programs what were captured at the instance the memory dump was taken. System activity can be traced through the application data and executable code related to the process ID.

The use of process handles revealed related artifacts to the process such as executable files, possible devices associated with the process such as pipes used as shared memory that may link how a process communicates, injects code into another process depending on the context.

Analysing environment variables can uncover how a process executes and the nature of the activity through its configuration settings.

Dll files associated to the process of interest can reveal what the process is doing. This is fileless malicious code is traced and exposed.

Packed executables can also be observed if identified in the process list, their activities can be examined as they are exposed after unpacking from the drive.

When a process is fully captured a process dump can be made to execute the process in virtual machine or a separate machine to observe the nature of the code.

Event logs can help expose activities and processes, possibly reveal process executions that may occurred before the memory capture.

Registries can reveal a wide scope of information of the state of the system, helping in reconstructing the activities. Registries captured would be recent data that can reveal recently instantiated programs, recently run applications, user account information, malware that may have tampered traces of memory.

Registry data can also reveal malware persistence, as fileless malicious code use system resources to persist in volatile memory. Looking into programs that run at system start-up or services run at user log in can reveal unusual activity. Such activities can also be uncovered by looking into changes in configuration files that may be logged to the registry.

Userassist key log programs run with the running count and execution times which may lead to traces of obfuscated activity in the RAM memory.

Analysis of networks captured in memory can reveal backdoors on the network connections such as remote exploits. The nature of network activities and their relations to processes can be uncovered by investigating network sockets that reveal ports addresses and protocols that can shed light in relation to processes under investigation.

Current and older connections can reveal the existing state of the system at the time of capture and may reveal preceding activities, such as the backdoors to remote attackers or bot process. Other user or malware activities can be explored through browser and DNS caches.

VIII. Forensic Tools

There are two aspects of memory forensics they are the acquisition of volatile memory and the second aspect is the memory analysis.

The first aspect is acquisition of a RAM dump before the memory analysis stage. Acquisition of volatile memory can be achieved using software process or using hardware devices. In instances where the system to be investigated is not a virtual machine, where it is a running system with no root access in these cases the only option is to capture volatile memory traffic using hardware. For RAM memory that is greater than 4GB the method is to use the PCI card slots on the motherboard to capture volatile memory data on the BUS between the RAM chip and the CPU chip. For RAM capacity that is greater than 4GB then a firewire is required to capture traffic of volatile memory. Fire wire can also be used to dump on a windows machine, however the windows machine needs to pretend to be an Apple proprietary product using tools such as “pythonraw1394” and its dependencies.

The easiest scenario of memory capture is when working with virtual machines as the investigator can take a snapshot of the VM that will create a vmem file or may even point to the directory where the VM is running and obtain the vmem file that contains the RAM dump.

Memory acquisitions can be achieved using command line tools for graphical user interface tools. It is best practice to capture memory of a running system from a separate USB device and dump the output of the memory capture across the network of a free volume on the loaded memory stick.

On a Windows system. Command line tools such as pmdump, userdump and dd (for disk dump) can be used. Other tools such as FTK imager KnTDD, MoonSols and F-Response can also be used.

FTK imager is a GUI tool, F-Response tools have two versions a GUI and a command line tool version. Using RAM dump tools on the target machine will also image its own process as it runs on the live system, as windows is a very popular Operating system for corporate and personal use there are a number of open source memory imaging tools such as Winpmem.

For Linux based systems there are two options they are LiME and the dd command line tool. The dd tool works with both Windows and Linux based systems.

Using the LiME tool requires the tools to be compiled for the suspect machine's architecture. If the examiner does not know the suspect machine's architecture this would mean the LiME would have to be compiled on the suspect system before acquiring memory. This can take a long time, secondly this process will change a lot of things in the suspect system's memory, compiling on the suspect machine will be much more destructive for potential evidence on the Linux host machine.

The second aspect is the memory analysis, a dedicated software tool is required to interpret the memory dump acquired from the first aspect discussed above. Running memory is not as structured as disk storage, RAM memory is a set of 1s or 0s that need to be interpreted and contextualised, different operating systems will sort and store memory in different ways. For this reason, forensics analysts need to understand the structure of how memory is stored in order to begin examination. Hence there is not an ideal memory forensics tool that catches all cases with greatest accuracy and precision the ideal digital forensic tool kit would possess.

There are various digital forensics tools for memory analysis, however most are not regularly updated or lack community support. The three top tools are Backlight, Volatility and Sans SIFT.

Backlight is ideal for companies and organisations as they are tailor made for quick and effective results in the field. Backlight details user actions and reports memory image analysis findings. It can analyse hibernation files, page files, raw dumps and crash dumps.

It can create bulk extraction contents searches of key details. It has a powerful file filter that is much faster than other open-source tools, and is available on all four major platforms. The downside is the very high price tag of the product.

Volatility is a cross platform tools written in python, it can extract useful information about network connections, open sockets, running processes, DLLs, cached registry hives, event logs and more. Volatility is available on Windows, MacOSX and Linux OS. Volatility is wise to keep as a staple tool as it is open source with potential to have more plugins added in future.

Sans SIFT is a popular toolkit that comes with all the essential features. It is an open-source tool for known for in-depth forensic investigations. Sans sift support AFF, dd and ewf file formats for deep analysis.

Sans Sift also comes with useful tools such as Rifiuti to examine the recycle bin, log2time to generate systems log based timelines, and scalpel used for file carving. It offers better memory utilisation, latest forensic techniques and cross compatibility between Linux and Windows.

There are other various tools that are not regularly updated or lack community support, however have a useful to employ to focus on certain aspects of memory analysis. PeStudio has entropy levels from 0 to 8 to indicate how packed malware is. Process Hacker is a useful tool to show how malware attempt to hide. Process Monitor or ProcMon records activities such as process creations and registry changes, it is very useful when used with Process hacker to examine new processes created by malware.

ProcDot is great tool for visualisation as it can take ProcMon output and visually represent malware activity.

Autoruns is an application to investigate software that launches on start-up. It is a tools that investigates malware persistence and highlight any new persistent software and techniques.

Fidler is tailored to investigate network activities for malwares that create backdoors or exfiltrate data.

Wireshark allows deep packet inspection of multiple protocols. It is an ideal tool for analysis of network packets, use of this program requires domain knowledge of network communication.

There are many more tools, however none which a is an all-in-one perfect suite of tools. Therefore, the best value for money for memory forensics tools is Volatility and Sans SIFT with all round understanding of digital forensics, that is the nature of running memory as mentioned above.

IX. Conclusions

The nature of program crashes and fileless malware is a system runtime activity that can only be resolved by analysing the state of a live system. Analysis of live system activity can also enlighten the direction of an investigation for other areas of digital forensic investigation such as disk analysis.

The best source of data for memory analysis is obtaining a memory dump with live memory capture, however if this this is not possible the next best alternative is to acquire the hibernation file if the system has been hibernated.

After capturing runtime processes the examiner can investigate for runtime environment variables to understand the nature of process execution, registries altered by the malware or bug, analysing network connections can reveal the nature of malicious code activity. However if the full process is captured then it is possible to dump the process as an executable to a virtual machine or a separate machine to examine the machinations of the process.

There is a wide range of forensics tolls to investigate RAM dump activity. The most effective and tailored solutions that report activity and are more automated are commercial products.

However there is not an ideal memory forensics tool that serves as a catch-all software solution for analysts that have limited understanding of computer systems and forensics analysis. The two main options for dealing with volatile memory security is to purchase specialised software such as Blacklist for forensic analysis or commercial security software products such as Guardian Digital EnGarde Cloud email security. The second option is to use regularly updated open source software such as Volatility and Sans Sift with a broad understanding of computer systems architecture and memory forensics concepts, and use other analyser software solutions (as mentioned previously) for particular needs of the analysiss.

ii. **Appendix**

ii.I.1.1 Appendix 1

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa8018da6040	System	4	0	89	560	-----	0	2022-08-28 06:42:08 UTC+0000	
0xfffffa80199a1950	smss.exe	244	4	2	29	-----	0	2022-08-28 06:42:08 UTC+0000	
0xfffffa8019ff4060	csrss.exe	328	320	9	508	0	0	2022-08-28 06:42:16 UTC+0000	
0xfffffa801a168b30	csrss.exe	380	372	11	457	1	0	2022-08-28 06:42:18 UTC+0000	
0xfffffa801a1914a0	wininit.exe	388	320	3	76	0	0	2022-08-28 06:42:18 UTC+0000	
0xfffffa80192a3060	winlogon.exe	424	372	4	112	1	0	2022-08-28 06:42:19 UTC+0000	
0xfffffa801a1e4b30	services.exe	484	388	8	215	0	0	2022-08-28 06:42:21 UTC+0000	
0xfffffa801a19fb30	lsass.exe	492	388	8	764	0	0	2022-08-28 06:42:22 UTC+0000	
0xfffffa801a1f5720	lsm.exe	500	388	9	148	0	0	2022-08-28 06:42:22 UTC+0000	
0xfffffa801a259690	svchost.exe	588	484	11	364	0	0	2022-08-28 06:42:27 UTC+0000	
0xfffffa801a27db30	vm3dservice.ex	648	484	4	45	0	0	2022-08-28 06:42:28 UTC+0000	
0xfffffa801a280870	svchost.exe	688	484	9	309	0	0	2022-08-28 06:42:29 UTC+0000	
0xfffffa801a2c4b30	svchost.exe	776	484	23	589	0	0	2022-08-28 06:42:30 UTC+0000	
0xfffffa801a2d9b30	svchost.exe	816	484	25	471	0	0	2022-08-28 06:42:30 UTC+0000	
0xfffffa801a2e09e0	svchost.exe	840	484	44	1038	0	0	2022-08-28 06:42:30 UTC+0000	
0xfffffa801a307060	audiodg.exe	920	776	5	124	0	0	2022-08-28 06:42:31 UTC+0000	
0xfffffa801a3349e0	svchost.exe	992	484	19	762	0	0	2022-08-28 06:42:32 UTC+0000	
0xfffffa801a35eb30	svchost.exe	324	484	18	479	0	0	2022-08-28 06:42:33 UTC+0000	
0xfffffa801a3b6b30	spoolsv.exe	672	484	13	270	0	0	2022-08-28 06:42:36 UTC+0000	
0xfffffa801a3db060	svchost.exe	1056	484	21	300	0	0	2022-08-28 06:42:36 UTC+0000	
0xfffffa801a4b9b30	VGAAuthService.	1240	484	4	82	0	0	2022-08-28 06:42:39 UTC+0000	
0xfffffa801a515450	taskhost.exe	1340	484	9	150	1	0	2022-08-28 06:42:40 UTC+0000	


0xfffffa801a545480 dwm.exe	1396	816	4	70	1	0	2022-08-28 06:42:40 UTC+0000
0xfffffa801a56a910 explorer.exe	1456	1388	27	814	1	0	2022-08-28 06:42:40 UTC+0000
0xfffffa801a582b30 vmtoolsd.exe	1496	484	11	270	0	0	2022-08-28 06:42:41 UTC+0000
0xfffffa801a676060 vm3dservice.ex	2044	1456	3	48	1	0	2022-08-28 06:42:47 UTC+0000
0xfffffa801a6779e0 vmtoolsd.exe	876	1456	9	189	1	0	2022-08-28 06:42:47 UTC+0000
0xfffffa801a484b30 dllhost.exe	1368	484	16	200	0	0	2022-08-28 06:42:48 UTC+0000
0xfffffa80197736f0 msdtc.exe	1160	484	15	155	0	0	2022-08-28 06:42:52 UTC+0000
0xfffffa801a76d060 SearchIndexer.	1088	484	14	639	0	0	2022-08-28 06:42:54 UTC+0000
0xfffffa801a78a3f0 WmiPrvSE.exe	2052	588	11	204	0	0	2022-08-28 06:42:55 UTC+0000
0xfffffa801a861b30 wmpnetwk.exe	2320	484	14	439	0	0	2022-08-28 06:42:59 UTC+0000
0xfffffa801a8c85f0 svchost.exe	2428	484	23	314	0	0	2022-08-28 06:43:00 UTC+0000
0xfffffa801a943950 svchost.exe	2600	484	10	352	0	0	2022-08-28 06:43:01 UTC+0000
0xfffffa801a9bdb30 WmiPrvSE.exe	2792	588	9	216	0	0	2022-08-28 06:43:04 UTC+0000
0xfffffa801aa68060 spspsvc.exe	2284	484	5	152	0	0	2022-08-28 06:44:44 UTC+0000
0xfffffa801a8ed060 svchost.exe	932	484	14	322	0	0	2022-08-28 06:44:45 UTC+0000
0xfffffa801aa49b30 chrome.exe	2892	1456	34	815	1	0	2022-08-28 06:47:04 UTC+0000
0xfffffa801a562060 chrome.exe	1960	2892	10	220	1	0	2022-08-28 06:47:31 UTC+0000
0xfffffa801a405060 thunderbird.ex	2776	772	65	859	1	0	2022-08-28 06:49:08 UTC+0000
0xfffffa801a6d5060 thunderbird.ex	3312	2776	39	308	1	0	2022-08-28 06:49:13 UTC+0000
0xfffffa801a9b7b30 thunderbird.ex	3568	2776	0	-----	1	0	2022-08-28 06:49:17 UTC+0000 2022-08-28 06:49:21 UTC+0000
0xfffffa801a9f6b30 thunderbird.ex	3972	2776	10	181	1	0	2022-08-28 06:49:19 UTC+0000
0xfffffa801aa2a060 thunderbird.ex	2136	2776	20	270	1	0	2022-08-28 06:49:22 UTC+0000
0xfffffa801aa31b30 thunderbird.ex	3508	2776	0	-----	1	0	2022-08-28 06:49:26 UTC+0000 2022-08-28 06:49:36 UTC+0000
0xfffffa801aa33b30 thunderbird.ex	3476	2776	21	278	1	0	2022-08-28 06:49:26 UTC+0000
0xfffffa801a9f3630 mynotepad++.ex	3948	1456	3	70	1	1	2022-08-28 06:50:21 UTC+0000

0xfffffa8018e7f6d0 iexplore.exe	2028	1456	12	409	1	1	2022-08-28 06:50:56 UTC+0000
0xfffffa801abb8b30 iexplore.exe	3656	2028	16	373	1	1	2022-08-28 06:50:57 UTC+0000
0xfffffa8019a075c0 chrome.exe	3808	2892	9	174	1	0	2022-08-28 06:51:16 UTC+0000

ii.I.1.2 Appendix 2

Procedure	vol.py -f Snapshot1.vmem --profile=Win7SP1x64 filescan grep -i Thunderbird		
	"0x000000007e258b70 16 0 RW-rw- \Device\HarddiskVolume1\Users\Eason\AppData\Roaming\Thunderbird\Profiles\nsxx2nq9.default-release\ImapMail\imap.gmail.com\[Gmail].sbd\All Mail"		
	vol.py -f Snapshot1.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007e258b70 -D '/home/sansforensics/Downloads/evidence_B/Email'		
Source:	file.None.0xfffffa801a4451e0.dat		
Email Messages			
Email #1			
Base64 Encoded		Base64 Decoded	
W2ItYWdlOiBHb29nbGVdDQpBIg5ldy BzaWduLWlulG9uIFdpbmRvd3MNCg0 KDQpodDMxNzExN0Bn bWFpbC5jb20NCldlIG5vdGljZWQgYSB uZXcgc2lnbi1pbiB0byB5b3VylEdvb2ds ZSBBY2NvdW50 IG9uIGEgV2luZG93cyBkZXZpY2UuEI mDQp0aGlzIHdhcyB5b3UsIHlvdSBkb2 7igJl0IG5lZWQg dG8gZG8gYW55dGhpbmculElmIG5vd Cwgd2XigJlsbCB0ZWxwIHlvdSBzZW50 1cmUNCnlvdXlgYWVjY291 bnRDZG9vc2VyP0VtYWlsPW50MzE3		[image: Google] A new sign-in on Windows ht317117@gmail.com We noticed a new sign-in to your Google Account on a Windows device. If this was you, you don't need to do anything. If not, we'll help you secure your account. Check activity <https://accounts.google.com/AccountChooser?Email=ht317117@gmail.com&continue=https:// myaccount.google.com/alert/nt/1661605003000?rfn%3D325%26rfnc%3D1%26eid %3D1063308458760514630%26et%3D0> You can also see security activity at	

<p>MTE3QGdtYWlsLmNvbSZjb250aW51Z T1odHRwczovL215YWNj</p> <p>b3VudC5nb29nbGUuY29tL2FsZXJ0L2 50LzE2NjE2MDUwMDMwMDA/ cmZuJTNEZl1JTl2cmZuYyUz</p> <p>RDEIMjZlaWQIM0QxMDYzMzA4NDU4 NzYwNTE0NjMwJTl2ZXQIM0QwPg0K WW91IGNhbiBhbHNvIHNI</p> <p>ZSBzZWN1cmI0eSBhY3Rpdml0eSBhd A0KaHR0cHM6Ly9teWFjY291bnQuZ2 9vZ2xlLmNvbS9ub3Rp</p> <p>ZmljYXRpb25zDQpZb3UgcmlvZjZWI2Z WQgdGhpcyBlbWFpbCB0byBsZXQge W91IGtub3cgYWJvdXQg</p> <p>aW1wb3J0YW50IGNoYW5nZXMgdG8 geW91cg0KR29vZ2xlIEFjY291bnQgY W5kiHNIcnZpY2VzLg0K</p> <p>wqkgMjAyMiBHb29nbGUgTExDLCAxN jAwIEFtcGhpdGhYXRYZSBQYXJrd2F 5LCBNb3VudGFpbiBW</p> <p>aWV3LCBDQSA5NDA0MywgVVNBBDQ o=</p>	<p>https://myaccount.google.com/notifications</p> <p>You received this email to let you know about important changes to your Google Account and services.</p> <p>© 2022 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA</p>
--	--

Email #2	
Base64 Encoded	Base64 Decoded
W2ltYWdlOiBHb29nbGVdDQpNb3ppb GxhIFRodW5kZXJiaXJkIEVtYWlsIHdhc yBncmFudGVkIGFj Y2VzcyB0byB5b3VylEdvb2dsZSBBY2 NvdW50DQoNCg0KaHQzMTcxMTdAZ 21haWwuY29tDQoNCklm IHlvdSBkaWQgbm90IGdyYW50IGFjY2 VzcywgeW91IHNo3VsZCBjaGVjayB0 aGlzIGFjdGl2aXR5 IGFuZCBzZW50cmUgeW91cg0KYWN jb3VudC4NCkNoZW50IGFjdGl2aXR5D Qo8aHR0cHM6Ly9hY2Nv dW50cy5nb29nbGUuY29tL0FjY291bn RDaG9vc2VyP0VtYWlsPW50MzE3MT E3QGdtYWlsLmNvbSZj b250aW51ZT1odHRwczovL215YWNjb 3VudC5nb29nbGUuY29tL2FsZXJ0L25 0LzE2NjE2MDUwNDkw MDA/ cmZuJTNETI3JTI2cmZuYyUzRDEIMj ZlaWQIM0QzMjA5OTA5ODEzODMxN DExMDAIMjZldCUz RDA+DQpZb3UgY2FuIGFsc28gc2VlIH NIY3VyaXR5IGFjdGl2aXR5IGF0DQpo	 Mozilla Thunderbird Email was granted access to your Google Account ht317117@gmail.com If you did not grant access, you should check this activity and secure your account. Check activity <https://accounts.google.com/AccountChooser?Email=ht317117@gmail.com&continue=https://myaccount.google.com/alert/nt/1661605049000?rfn%3D127%26rfnc%3D1%26eid%3D320990981383141100%26et%3D0> You can also see security activity at https://myaccount.google.com/notifications You received this email to let you know about important changes to your Google Account and services. © 2022 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA M4M4M4s9[?]{g

dHRwczovL215YWNj b3VudC5nb29nbGUuY29tL25vdGlma WNhdGlvbnMNCllvdSByZWNIaXZIZCB 0aGlzIGVtYWIsIHRv IGxldCB5b3Uga25vdyBhYm91dCBpbX BvcnRhbnQgY2hhbmdlcyB0byB5b3Vy DQpHb29nbGUgQWNj b3VudCBhbmQgc2VydmljZXMuDQrCq SAyMDIyIEdivb2dsZSBMTEMsIDE2MD AgQW1waGl0aGVhdHJl IFBhcmt3YXksIE1vdW50YWluIFZpZXc slENBIDk0MDQzLCBVU0ENCg== --0000000000000c9694105e73892ee	
Email #3	
Base64 Encoded	Base64 Decoded
SGkgRWFzb24sDQoNCkEgYmV0dGV yIEFuZHJvaWQgZXhwZXJpZW5jZSBp cyB3YWl0aW5nDQoNCIRh a2Ugb25lIG1pbmV0ZSB0byBzZXQgdX AgeW91ciBwaG9uZSB3aXRoIEdivb2ds ZQ0KDQpHZXQgc3Rh cnRIZCAgDQo8aHR0cHM6Ly9ub3RpZ mljYXRpb25zLmdvb2dsZS5jb20vZy9w L0FQTkwxVGk1RHZf NTZRRjBEdjNZMzNxaDNfRnNlcEFFN 3JBTk83V2VIM08yRlFCMmJVMHpTTk VwQIB1TE9QNkpTU3Va d3AzNmpfZlYyOUtjRGJMa0V4MlIDbjN vSnowT0tyQ0JZa0ZKMxhPUUYzTG12	<p>Hi Eason,</p> <p>A better Android experience is waiting</p> <p>Take one minute to set up your phone with Google</p> <p>Get started</p> <p><https://notifications.google.com/g/p/APNL1Ti5Dv_56QF0Dv3Y33qh3_FsepAE7rANO7Wee3O2FQB2bU0zSNEpBPuLOP6JSSuZwp36j_fv29KcDbLkEx2YCn3oJz0OKrCBYkFJ1xOQF3Lb69WlpVjd58aXbpoCS7lptwXoOX4YoV2ZflzSA5tdtUXBndBRVo1b2KZhQ4TpREFm8hlg4mV5ufe0RG9F1W-HHsgU4-VoP_AaxC9VJKb9Qk6IBwOpw5yflyWJOK4nzD-></p>

<p>OVdscFZqZDU4YVhi</p> <p>cG9DUzdschHR3WG9PWDRZb1YyWmZJeINBNXRkdFVYQm5kQIJWbzFiMktaFE0VHBSRUZtOGhsZzRt</p> <p>VjV1ZmUwUkc5RjFXLUhlc2dVNC1Wb1BfQWF4QzIWSktiOVFrNkICd09wdzV5Zkl5V0pPSzRuekQt</p> <p>bTF3bWITakJBTHM2Y21tWDAzMDRWb0MybFFMNkdUamhEMjl6SnI5aTNWX19RSm5QQTJwc3FibHIJ</p> <p>N2VNTFJjUXdtbmpRNVp4aHREaUJjeHU1ME0xcG1uTmZFaW5tVkp0SmNqTE40ZHdHRIZNWUlpTmMx</p> <p>VmxZWDdpSTRMX1IMdmszWnp3WG8wTkY0RIBYMKloOUpXeHJwd3Nkd2F3SWtzaE13Q0R2c1M2Mkhu</p> <p>UFk1SWp0RWZsN0VfS1NqYVpIRnJBbGZHVBzNmhBRWVMMDIIU0dIRXpXa3F1QWp3UU1RX08yQUxT</p> <p>eFgwZ3NoWTktV00tTzEzUnB3V0M2cEg3MFhKZy15RERyUm10NDJ4TFISdmVsZnVKZlpHYnk0QVJJ</p> <p>LUVhRVdwNHJxU2RzeU9vbFBhM1IFQkg4SThHM2NyMDhGZ0VFMWw3dm dXaEVxLVBoYXgwQXhZd0JC</p> <p>NnJoMW1uVDRITVlqVGp6T2h6NFloT0pnOTBVTINOTkxxT3IFa3I2YmYtRzh0Mk9vRGxrb1VOU0hl</p> <p>Nmo3VHUxWC14c3FDYXFXWEVWdUpCMUdQU21Lb3d3SWhQUUtWX1NJMzFFb2ZXOU1fZkZoT2NvdWw2</p>	<p>m1wmiSjBALs6cmmX0304VoC2IQL6GTjhD29zJr9i3V__QJnPA2psqHlyl7eMLRcQwmnjQ5ZxhtDiBcxu50M1pmnNfEinmVJtJcjLN4dwGFVMYliNc1VIYX7iI4L_YLvk3ZzwXo0NF4FPX2Ih9JWxrpwsdwawlkshMwCDvsS62HnPY5IjtEfI7E_KSjaZeFrAlfGePs6hAEeL09eSGHEzqkquAjwQMQ_O2ALSxX0gshY9-WM-O13RpwWC6pH70XJg-yDDrRmt42xLYRvelfuJfZGby4ARl-EaEWp4rqSdsyOolPa3YEBH8I8G3cr08FgEE1I7vgWhEq-Phax0AxYwBB6rh1mnT4HMYjTjzOhz4YhOJg90UNSNNLqOyEkr6bf-G8t2OoDIkoUNSHe6j7Tu1X-xsqCaqWXEvuJB1GPSmKowwlhPQKV_Si31EofW9M_fFhOcoul6Ya73YOJDIXo91G7zl1a5ISYAJRnnWdbliBBLzp2GMkAg10Q7T-vcdNWT1fcF-1tIBDhKzf7vx46-2J7t7SlqoGxhz></p> <p>This email was sent to ht317117@gmail.com <ht317117@gmail.com> because you recently signed into your Google Account on your Google Emualtor device. If you do not wish to receive emails to help you set up your device with Google when you sign into your account on the device for the first time, please unsubscribe</p> <p><<a 901="" 914="" 938"="" 968="" data-label="Page-Footer" href="https://notifications.google.com/g/p/APNL1TiIKagTMrmbgX8_Vlh24ym9sDJBZW5BW8CEnApXNwKyIBABNvBBZhGDkh1vW1MFAI5K0jgNCZ4XL_SK7bUHTFCjM9tHVo5jUkVqQfHjGgb_rOfyNDWz9xHPQWLG0-EZUE7cqnyaZZSMQXoJTUHbyFStnHIBW_Mh2BFZ98rBF6td5CfXqW5XOhplK5eIS4q5kuXyBcXcRboWD2_gR-POdHuPHJ3TQQfWbYFX6RXsRC7j1GAhliWRMqseMzO3kQAQujhfbmJ64HnjpdVMA-EkB6shgVKxzlpamWHcsVe__4>.</p> <p>© 2022 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043</p> <p>4M4M4N[1wě -u</p> </td></tr> </table> </div> <div data-bbox="> <p>Page 33</p> </p>
---	--

<p>WWE3M1IPSkRJWG85MUc3ekkxYTV sU1IBSIJubldkYklpQkJMenAyR01rQW cxMFE3VC12Y2ROV1Qx</p> <p>ZmNGLTF0SUJESEt6Zjd2eDQ2LTJK N3Q3U0lxb0d4aHo+DQoNCIRoaXMgZ W1haWwgd2FzIHNIbnQg</p> <p>dG8gaHQzMTcxMTdAZ21haWwuY29tI DxodDMxNzExN0BnbWFpbC5jb20+IG JIY2F1c2UgeW91ICAN</p> <p>CnJIY2VudGx5IHNPZ25lZCBpbmRvIH vdXlR29vZ2x1IEFjY291bnQgb24geW9 1ciBHb29nbGUg</p> <p>RW11YWx0b3lgZGV2aWNiLiBJZiAgD Qp5b3UgZG8gbm90IHdpc2ggdG8gcm VjZWl2ZSBibWFpbHMg</p> <p>dG8gaGVscCB5b3Ugc2V0IHVwIHlvdX lgZGV2aWNlIHdpcGggIA0KR29vZ2x1 HdoZW4geW91IHNP</p> <p>Z24gaW50byB5b3VyIGFjY291bnQgb2 4gdGhlIGRldmJjZSBmb3lgaGhlIGZpcn N0IHRpbWUsICAN</p> <p>CnBsZWZzZSB1bnN1YnNjcmlhZSAgD Qo8aHR0cHM6Ly9ub3RpZmljYXRpb2 5zLmdvb2dsZS5jb20v</p> <p>Zy9wL0FQTkwxVGJJS2FnVE1ybWJn WDhfVkl0MjR5bTlZREpCWlc1Qlc4Q0V uQXBYTndLeWICQUJO</p> <p>dkJCWmhHRGtoMXZXMU1GQWw1Sz BqZ05DWjRYTF9TSzdiVUhURkNqTTI 0SFZvNWpVa1ZxUWZlakdn</p> <p>YI9yT2Z5TkRXejl4SFBRV0xHMC1FWI</p>	
--	--

<p>VFN2NxbnlhWlpTTVFYb0pUVUhieUZT dG5lbEJXX01oMkJG</p> <p>Wjk4ckJGNnRkNUNmWHFXNVhPaHB sSzVISUITNHE1a3VYeUJjWGNSYm9 XRDJfZ1ltUE9kSHVQSEoz</p> <p>VFFRZldiWUZYNlJYc1JDN2oxR0FoS WIXUk1xc2VNek8za1FBUXVqaGZibU o2NEhuanBkVk1BLUVr</p> <p>QjZzaGdWS3h6SXBhbVdlY3NWZV9f ND4uDQoNCsKpIDlwMjlgR29vZ2xllEx MQyAxNjAwIEFtcGhp</p> <p>dGhYXRyZSBQYXJrd2F5LCBNb3Vud GFpbiBWaWV3LCBDQSA5NDA0Mw0 K</p> <p>--0000000000005b35d305e6f58eda</p>	
Email #4	
Base64 Encoded	Base64 Decoded
<p>W2ltYWdlOiBHb29nbGVdDQpBIG5ldy BzaWduLWlulG9uIFdpbmRvd3MNCg0 KDQpodDMxNzExN0Bn</p> <p>bWFpbC5jb20NCldlIG5vdGljZWQgYSB uZXcgc2lnbi1pbiB0byB5b3VyIEdivb2ds ZSBBY2NvdW50</p> <p>IG9uIGEgV2luZG93cyBkZXZpY2UuIEI mDQp0aGlzIHdhcyB5b3UsIHlvdSBkb2 7igJl0IG5lZWQg</p> <p>dG8gZG8gYW55dGhpbmculElmIG5vd Cwg2XigJlsbCB0ZWxwIHlvdSBzZW50 1cmUNCnlvdXlgYWNj</p>	<p>[image: Google]</p> <p>A new sign-in on Windows</p> <p>ht317117@gmail.com</p> <p>We noticed a new sign-in to your Google Account on a Windows device. If this was you, you don't need to do anything. If not, we'll help you secure your account.</p> <p>Check activity</p>

b3VudC4NCkNoZWNrIGFjdGI2aXR5D Qo8aHR0cHM6Ly9hY2NvdW50cy5nb2 9nbGUuY29tL0FjY291 bnRDaG9vc2VyP0VtYWIsPWh0MzE3 MTE3QGdtYWIsLmNvbSZjb250aW51Z T1odHRwczovL215YWNj b3VudC5nb29nbGUuY29tL2FsZXJ0L2 50LzE2NjEYnJjA1ODEwMDA/ cmZuJTNEZl11JTl2cmZuYyUz RDEIMjZlaWQIM0QxODQxMDk1MzA3 ODU4OTE5MTUIMjZldCUzRDA+DQpZ b3UgY2FuIGFsc28gc2VI IHNIY3VyaXR5IGFjdGI2aXR5IGF0DQp odHRwczovL215YWNjb3VudC5nb29n bGUuY29tL25vdGlm aWNhdGlbnMNCllvdSBYZWNIaXZIZC B0aGlzIGVtYWIsIHRvIGxldCB5b3Uga2 5vdyBhYm91dCBp bXBvcnRhbnQgY2hhbmdlcyB0byB5b3 VyDQpHb29nbGUgQWNjb3VudCBhb mQgc2VydmljZXMuDQrC qSAyMDIyIEdvb2dsZSBMTEMsIDE2M DAgQW1waGl0aGVhdHJlIFBhcmt3YX ksIE1vdW50YWluIFZp ZXcsiENBIDk0MDQzLCBVU0ENCg== --000000000000ec690e05e6e85ee2	< https://accounts.google.com/AccountChooser?Email=ht317117@gmail.com&continue=https://myaccount.google.com/alert/nt/1661260581000?rfn%3D325%26rfnc%3D1%26eid%3D184109530785891915%26et%3D0 > You can also see security activity at https://myaccount.google.com/notifications You received this email to let you know about important changes to your Google Account and services. © 2022 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA M4M4M4yv9{
Email #5	
Base64 Encoded	Base64 Decoded
W2ltYWdlOiBHb29nbGVdDQpBIG5ldy	[image: Google]

<p>BzaWduLWlulG9uIEdvb2dsZSBFbXVh bHRvcg0KDQoNCmh0</p> <p>MzE3MTE3QGdtYWlsLmNvbQ0KV2U gbm90aWNIZCBhIG5ldyBzaWduLWlul HRvIHlvdXlR29vZ2xl</p> <p>IEFjY291bnQgb24gYSBhb29nbGUgR W11YWx0b3INCmRldmJjZS4gSWYgd GhpcyB3YXMgeW91LCB5</p> <p>b3UgZG9u4oCZdCBuZWVklHRvIGRvI GFueXRoaW5nLiBJZiBub3QsIHdl4oC ZbGwgaGVscA0KeW91</p> <p>IHNiY3VyZSB5b3VyIGFjY291bnQuDQ pDaGVjayBhY3Rpdml0eQ0KPGh0dHB zOi8vYWNjb3VudHMu</p> <p>Z29vZ2xlLmNvbS9BY2NvdW50Q2hvb 3Nlcj9FbWFpbD1odDMxNzExN0BnbW FpbC5jb20mY29udGlu</p> <p>dWU9aHR0cHM6Ly9teWFjY291bnQuZ 29vZ2xlLmNvbS9hbGVydC9udC8xNjY xMzE1MzUwMDAwP3Jm</p> <p>biUzRDMyNSUyNnJmbmMIM0QxJTl2 ZWlkJTNELTI1MTk3NDEyNTQ1OTQ0 ODU4MTkIMjZldCUzRDA+</p> <p>DQpZb3UgY2FuIGFsc28gc2VIIHNiY3V yaXR5IGFjdGI2aXR5IGF0DQpodHRwc zovL215YWNjb3Vu</p> <p>dC5nb29nbGUuY29tL25vdGlmaWNhd GlvbnMNCllvdSBYZWNIaXZIZCB0aGlz IGVtYWlsIHRvIGxl</p> <p>dCB5b3Uga25vdyBhYm91dCBpbXBvc nRhbnQgY2hhbmdlcYB0byB5b3VyDQ</p>	<p>A new sign-in on Google Emualtor</p> <p>ht317117@gmail.com</p> <p>We noticed a new sign-in to your Google Account on a Google Emualtor device. If this was you, you don't need to do anything. If not, we'll help you secure your account.</p> <p>Check activity</p> <p><https://accounts.google.com/AccountChooser?Email=ht317117@gmail.com&continue=https://myaccount.google.com/alert/nt/1661315350000?rfn%3D325%26rfnc%3D1%26eid%3D-2519741254594485819%26et%3D0></p> <p>You can also see security activity at</p> <p>https://myaccount.google.com/notifications</p> <p>You received this email to let you know about important changes to your Google Account and services.</p> <p>© 2022 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA</p> <p>M4M4M49معرش</p>
--	---

<p>pHb29nbGUgQWNjb3Vu</p> <p>dCBhbmQgc2VydmljZXMuDQrCqSAy</p> <p>MDIyIEdvb2dsZSBMTEMsIDE2MDAg</p> <p>QW1waGl0aGVhdHJlIFBh</p> <p>cmt3YXksIE1vdW50YWluIFZpZXcsIEN</p> <p>BIDk0MDQzLCBVU0ENCg==</p> <p>--00000000000006d6b3b05e6f51ff1</p>	
--	--

ii.I.1.3 Appendix 4

```
42["commands",["/as","/away","/back","/ban","/banlist","/bs","/close","/collapse","/connect","/cs","/ctcp","/cycle","/dehop","/deop","/devoice","/disconnect","/expand","/ho","/hop","/hs","/ignore","/ignorelist","/invite","/invitelist","/join","/kick","/kill","/leave","/list","/me","/mode","/ms","/msg","/nick","/notice","/ns","/op","/os","/part","/query","/quit","/quote","/raw","/rejoin","/rs","/say","/send","/server","/slap","/topic","/unban","/unignore","/voice","/whois"]]

R42["setting:all",
{"advanced":false,"autocomplete":true,"nickPostfix":"","coloredNicks":true,"highlights":"","highlightExceptions":"","awayMessage":"","links":true,"motd":true,"notifyAllMessages":false,"showSeconds":false,"use12hClock":false,"statusMessages":"condensed","theme":"default","media":true,"uploadCanvas":true,"userStyles":""}]

42["join",{"network":"439dd4e3-b6f7-4cad-ab28-b2d35de10533","chan":
{"name":"#FederalLawEnforcementAgency","state":1,"id":5,"messages":
[],"totalMessages":0,"key":"","topic":"","type":"channel","firstUnread":0,"unread":0,"highlight":0,"users":
[]},"index":1}]P

42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Eason"},"time":"2022-08-28T02:05:04.352Z","hostmask":"user1@127.0.0.1","type":"join","self":true,"id":38,"previews":
[],"text":""}}]P

42["users",{"chan":5}]P
42["users",{"chan":5}]P
42["open",5]P

J42["names",{"id":5,"users":[{"nick":"Eason","mode":"@","lastMessage":0}]]P

42["msg",{"chan":5,"msg":{"type":"mode_channel","text":"+nt ","from":{"id":39,"previews":
[],"self":false,"time":"2022-08-28T02:05:06.356Z"}}]R

42["join",{"network":"9a5ab82b-ec8c-4582-9b47-0730a8deaff2","chan":
{"name":"#FederalLawEnforcementAgency","state":1,"id":3,"messages":
[],"totalMessages":0,"key":"","topic":"","type":"channel","firstUnread":0,"unread":0,"highlight":0,"users":
[]},"index":1}]m

42["msg",{"chan":3,"msg":{"from":{"mode":"","nick":"Benji"},"time":"2022-08-28T02:05:33.419Z","hostmask":"user2@127.0.0.1","type":"join","self":true,"id":22,"previews":
[],"text":""}}]m

42["users",{"chan":3}]m
42["users",{"chan":3}]m

42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Benji"},"time":"2022-08-28T02:05:33.420Z","hostmask":"user2@127.0.0.1","type":"join","self":false,"id":40,"previews":
[],"text":""}}]m

42["users",{"chan":5}]m

u42["names",{"id":5,"users":[{"nick":"Eason","mode":"@","lastMessage":0},
{"nick":"Benji","mode":"","lastMessage":0}]]m

42["msg",{"chan":3,"msg":{"type":"mode_channel","text":"+nt ","from":{"id":23,"previews":
[],"self":false,"time":"2022-08-28T02:05:35.425Z"}}]o

L42["join",{"network":"fbf22ec7-012d-4e49-87e5-40046557dd7d","chan":
{"type":"special","special":"list_channels","name":"Channel List","data":{"text":"Loading channel list, this can take a moment..."},"id":3,"messages":
[],"totalMessages":0,"key":"","topic":"","state":0,"firstUnread":0,"unread":0,"highlight":0,"users":
```

```

[], "index": 1}}
C42["msg:special", {"chan": 3, "data": {"text": "Loaded 2 channels..."}}]
42["msg:special", {"chan": 3, "data":
[{"channel": "#FederalLawEnforcementAgency", "num_users": 2, "topic": "[+nt] ", "tags": {}},
{"channel": "#thelounge", "num_users": 1, "topic": "[+nt] ", "tags": {}}]]
42["msg", {"chan": 5, "msg": {"from": {"mode": "", "nick": "Tony"}, "time": "2022-08-
28T02:06:03.738Z", "hostmask": "user3@127.0.0.1", "type": "join", "self": false, "id": 41, "previews":
[], "text": ""}}}
42["users", {"chan": 5}]
42["msg", {"chan": 3, "msg": {"from": {"mode": "", "nick": "Tony"}, "time": "2022-08-
28T02:06:03.738Z", "hostmask": "user3@127.0.0.1", "type": "join", "self": false, "id": 24, "previews":
[], "text": ""}}}
42["users", {"chan": 3}]
42["join", {"network": "fbf22ec7-012d-4e49-87e5-40046557dd7d", "chan":
{"name": "#FederalLawEnforcementAgency", "state": 1, "id": 4, "messages":
[], "totalMessages": 0, "key": "", "topic": "", "type": "channel", "firstUnread": 0, "unread": 0, "highlight": 0, "users":
[]}, "index": 1}}
42["msg", {"chan": 4, "msg": {"from": {"mode": "", "nick": "Tony"}, "time": "2022-08-
28T02:06:03.739Z", "hostmask": "user3@127.0.0.1", "type": "join", "self": true, "id": 25, "previews":
[], "text": ""}}}
42["users", {"chan": 4}]
42["users", {"chan": 4}]
42["msg", {"chan": 4, "msg": {"type": "mode_channel", "text": "+nt ", "from": {}, "id": 26, "previews":
[], "self": false, "time": "2022-08-28T02:06:05.742Z"}}]
42["msg", {"chan": 5, "msg": {"from": {"mode": "@", "nick": "Eason"}, "type": "message", "time": "2022-08-
28T02:06:33.050Z", "text": "Benji, read this message carefully. I might not have much time
left", "self": true, "highlight": false, "users": ["Benji"], "id": 42, "previews": []}}}
42["msg", {"chan": 3, "msg": {"from": {"mode": "@", "nick": "Eason"}, "type": "message", "time": "2022-08-
28T02:06:33.094Z", "text": "Benji, read this message carefully. I might not have much time
left", "self": false, "highlight": true, "users": ["Benji"], "id": 25, "previews": []}}}
42["msg", {"chan": 4, "msg": {"from": {"mode": "@", "nick": "Eason"}, "type": "message", "time": "2022-08-
28T02:06:33.095Z", "text": "Benji, read this message carefully. I might not have much time
left", "self": false, "highlight": false, "users": ["Benji"], "id": 27, "previews": []}}}
42["msg", {"chan": 3, "msg": {"from": {"mode": "", "nick": "Benji"}, "type": "message", "time": "2022-08-
28T02:06:46.030Z", "text": "Whats wrong Eason?", "self": true, "highlight": false, "users":
["Eason"], "id": 26, "previews": []}}}
42["msg", {"chan": 5, "msg": {"from": {"mode": "", "nick": "Benji"}, "type": "message", "time": "2022-08-
28T02:06:46.030Z", "text": "Whats wrong Eason?", "self": false, "highlight": true, "users":
["Eason"], "id": 43, "previews": []}}}
42["msg", {"chan": 4, "msg": {"from": {"mode": "", "nick": "Benji"}, "type": "message", "time": "2022-08-
28T02:06:46.031Z", "text": "Whats wrong Eason?", "self": false, "highlight": false, "users":
["Eason"], "id": 28, "previews": []}}}
642["msg", {"chan": 5, "msg": {"from": {"mode": "@", "nick": "Eason"}, "type": "message", "time": "2022-08-
28T02:06:58.107Z", "text": "Erika Sloane asked me to deliver a package from the Russian embassy in
London to Morocco. But it wasnt the real embassy.", "self": true, "highlight": false, "users":

```


[{"id":44,"previews":[]}]

742["msg",{"chan":3,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:06:58.107Z","text":"Erika Sloane asked me to deliver a package from the Russian embassy in London to Morocco. But it wasnt the real embassy.","self":false,"highlight":false,"users":

[{"id":27,"previews":[]}]

742["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:06:58.108Z","text":"Erika Sloane asked me to deliver a package from the Russian embassy in London to Morocco. But it wasnt the real embassy.","self":false,"highlight":false,"users":

[{"id":29,"previews":[]}]

42["msg",{"chan":3,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-28T02:07:08.892Z","text":"What are you talking Eason? Erika Sloane? That Erika Sloane?","self":true,"highlight":false,"users":["Eason"],"id":28,"previews":[]}]

42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-28T02:07:08.893Z","text":"What are you talking Eason? Erika Sloane? That Erika Sloane?","self":false,"highlight":true,"users":["Eason"],"id":45,"previews":[]}]

42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-28T02:07:08.893Z","text":"What are you talking Eason? Erika Sloane? That Erika Sloane?","self":false,"highlight":false,"users":["Eason"],"id":30,"previews":[]}]

?42["msg",{"chan":5,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:07:20.726Z","text":"I have some insurance, in case this whole thing blows up. Its in the usual place. Promise me you will store it in a safe place. ","self":true,"highlight":false,"users":

[{"id":46,"previews":[]}]

@42["msg",{"chan":3,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:07:20.727Z","text":"I have some insurance, in case this whole thing blows up. Its in the usual place. Promise me you will store it in a safe place. ","self":false,"highlight":false,"users":

[{"id":29,"previews":[]}]

@42["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:07:20.727Z","text":"I have some insurance, in case this whole thing blows up. Its in the usual place. Promise me you will store it in a safe place. ","self":false,"highlight":false,"users":

[{"id":31,"previews":[]}]

42["msg",{"chan":3,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-28T02:07:31.836Z","text":"For sure my friend. I will upload it to my Onedrive. Stay safe","self":true,"highlight":false,"users":[],"id":30,"previews":[]}]

42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-28T02:07:31.837Z","text":"For sure my friend. I will upload it to my Onedrive. Stay safe","self":false,"highlight":false,"users":[],"id":47,"previews":[]}]

42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-28T02:07:31.837Z","text":"For sure my friend. I will upload it to my Onedrive. Stay safe","self":false,"highlight":false,"users":[],"id":32,"previews":[]}]

42["msg",{"chan":5,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:07:42.549Z","text":"Thx. TTYL","self":true,"highlight":false,"users":[],"id":48,"previews":[]}]

42["msg",{"chan":3,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:07:42.549Z","text":"Thx. TTYL","self":false,"highlight":false,"users":[],"id":31,"previews":[]}]

42["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:07:42.554Z","text":"Thx. TTYL","self":false,"highlight":false,"users":[],"id":33,"previews":[]}]

42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-28T02:09:28.542Z","text":"Eason, the bioweapons came from a previous Soviet biological weapons

```

program","self":false,"highlight":true,"users":["Eason"],"id":49,"previews":[]}}X
42["msg",{"chan":3,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-28T02:09:28.542Z","text":"Eason, the bioweapons came from a previous Soviet biological weapons program","self":false,"highlight":false,"users":["Eason"],"id":32,"previews":[]}}]X
42["msg",{"chan":5,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:09:50.266Z","text":"Thanks, Tony. I owe you one.","self":true,"highlight":false,"users":["Tony"],"id":50,"previews":[]}}]n
42["msg",{"chan":3,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:09:50.267Z","text":"Thanks, Tony. I owe you one.","self":false,"highlight":false,"users":["Tony"],"id":33,"previews":[]}}]n
42["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:09:50.267Z","text":"Thanks, Tony. I owe you one.","self":false,"highlight":true,"users":["Tony"],"id":35,"previews":[]}}]n
42["msg",{"chan":3,"msg":{"from":{"mode":"","nick":"Benji"},"type":"part","time":"2022-08-28T02:10:13.335Z","text":"The Lounge - https://thelounge.chat","hostmask":"user2@127.0.0.1","self":true,"id":34,"previews":[]}}]
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Benji"},"type":"part","time":"2022-08-28T02:10:13.335Z","text":"The Lounge - https://thelounge.chat","hostmask":"user2@127.0.0.1","self":false,"id":51,"previews":[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Benji"},"type":"part","time":"2022-08-28T02:10:13.336Z","text":"The Lounge - https://thelounge.chat","hostmask":"user2@127.0.0.1","self":false,"id":36,"previews":[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-28T02:10:21.807Z","text":"Buy me some KFC next time when you are in the office","self":true,"highlight":false,"users":["Tony"],"id":37,"previews":[]}}]
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-28T02:10:21.807Z","text":"Buy me some KFC next time when you are in the office","self":false,"highlight":false,"users":["Tony"],"id":52,"previews":[]}}]
42["msg",{"chan":5,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:10:34.556Z","text":"I dont know if I can come back","self":true,"highlight":false,"users":["Eason"],"id":53,"previews":[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"message","time":"2022-08-28T02:10:34.556Z","text":"I dont know if I can come back","self":false,"highlight":false,"users":["Eason"],"id":38,"previews":[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-28T02:10:46.128Z","text":"Its just KFC. dont be stingy","self":true,"highlight":false,"users":["Tony"],"id":39,"previews":[]}}]
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-28T02:10:46.129Z","text":"Its just KFC. dont be stingy","self":false,"highlight":false,"users":["Tony"],"id":54,"previews":[]}}]
42["msg",{"chan":5,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"part","time":"2022-08-28T02:11:31.165Z","text":"The Lounge - https://thelounge.chat","hostmask":"user1@127.0.0.1","self":true,"id":55,"previews":[]}}]
42["part",{"chan":5}]
42["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Eason"},"type":"part","time":"2022-08-28T02:11:31.167Z","text":"The Lounge -

```

```

https://thelounge.chat","hostmask":"user1@127.0.0.1","self":false,"id":40,"previews":[]}]
L42["join",{"network":"9a5ab82b-ec8c-4582-9b47-0730a8deaff2","chan":
{"type":"special","special":"list_channels","name":"Channel List","data":{"text":"Loading channel list, this
can take a moment..."},"id":4,"messages":
[],"totalMessages":0,"key":"","topic":"","state":0,"firstUnread":0,"unread":0,"highlight":0,"users":
[],"index":1}}{
42["join",{"network":"9a5ab82b-ec8c-4582-9b47-0730a8deaff2","chan":
{"name":"#FederalLawEnforcementAgency","state":1,"id":5,"messages":
[],"totalMessages":0,"key":"","topic":"","type":"channel","firstUnread":0,"unread":0,"highlight":0,"users":
[],"index":1}}
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Benji"},"time":"2022-08-
28T02:14:24.383Z","hostmask":"user2@127.0.0.1","type":"join","self":true,"id":35,"previews":
[],"text":""}}]
42["users",{"chan":5}]
42["users",{"chan":5}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Benji"},"time":"2022-08-
28T02:14:24.384Z","hostmask":"user2@127.0.0.1","type":"join","self":false,"id":41,"previews":
[],"text":""}}]
42["users",{"chan":4}]
42["names",{"id":4,"users":[{"nick":"Benji","mode":"","lastMessage":0},
{"nick":"Tony","mode":"","lastMessage":1661652646128}]]
42["msg",{"chan":5,"msg":{"type":"mode_channel","text":"+nt ","from":{},"id":36,"previews":
[],"self":false,"time":"2022-08-28T02:14:26.387Z"}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-
28T02:14:46.186Z","text":"I just did Eason a favour but he is not willing to buy KFC for me
","self":true,"highlight":false,"users":[],"id":42,"previews":[]}]
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-
28T02:14:46.186Z","text":"I just did Eason a favour but he is not willing to buy KFC for me
","self":false,"highlight":false,"users":[],"id":37,"previews":[]}]
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-
28T02:14:58.511Z","text":"idk. he sounds a bit under the weather
today","self":true,"highlight":false,"users":[],"id":38,"previews":[]}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-
28T02:14:58.511Z","text":"idk. he sounds a bit under the weather
today","self":false,"highlight":false,"users":[],"id":43,"previews":[]}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-
28T02:15:07.670Z","text":"I know right","self":true,"highlight":false,"users":[],"id":44,"previews":[]}]
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Tony"},"type":"message","time":"2022-08-
28T02:15:07.671Z","text":"I know right","self":false,"highlight":false,"users":[],"id":39,"previews":[]}]
42["msg",{"chan":5,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-
28T02:15:27.217Z","text":"He asked me to store something for him, but I don
t know. I have no space on my one drive.","self":true,"highlight":false,"users":[],"id":40,"previews":[]}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Benji"},"type":"message","time":"2022-08-
28T02:15:27.218Z","text":"He asked me to store something for him, but I don

```

```

t know. I have no space on my one drive.", "self": false, "highlight": false, "users": [], "id": 45, "previews": []}]
42["msg", {"chan": 4, "msg": {"from": {"mode": "", "nick": "Tony"}, "type": "message", "time": "2022-08-28T02:15:41.093Z", "text": "Free for coffee?", "self": true, "highlight": false, "users": [], "id": 46, "previews": []}}]
42["msg", {"chan": 5, "msg": {"from": {"mode": "", "nick": "Tony"}, "type": "message", "time": "2022-08-28T02:15:41.093Z", "text": "Free for coffee?", "self": false, "highlight": false, "users": [], "id": 41, "previews": []}}]
42["msg", {"chan": 4, "msg": {"from": {"mode": "", "nick": "Tony"}, "type": "message", "time": "2022-08-28T02:15:55.121Z", "text": "where to meet?", "self": true, "highlight": false, "users": [], "id": 47, "previews": []}}]
42["msg", {"chan": 5, "msg": {"from": {"mode": "", "nick": "Tony"}, "type": "message", "time": "2022-08-28T02:15:55.122Z", "text": "where to meet?", "self": false, "highlight": false, "users": [], "id": 42, "previews": []}}]
42["msg", {"chan": 5, "msg": {"from": {"mode": "", "nick": "Benji"}, "type": "message", "time": "2022-08-28T02:16:13.317Z", "text": "where to meet indeed", "self": true, "highlight": false, "users": [], "id": 43, "previews": []}}]
42["msg", {"chan": 4, "msg": {"from": {"mode": "", "nick": "Benji"}, "type": "message", "time": "2022-08-28T02:16:13.318Z", "text": "where to meet indeed", "self": false, "highlight": false, "users": [], "id": 48, "previews": []}}]
42["join", {"network": "d0effdca-0c7f-425f-8829-f0f659a4f30e", "chan": {"name": "#Syndicate", "state": 1, "id": 7, "messages": [], "totalMessages": 0, "key": "", "topic": "", "type": "channel", "firstUnread": 0, "unread": 0, "highlight": 0, "users": [], "index": 1}}]
42["msg", {"chan": 7, "msg": {"from": {"mode": "", "nick": "Syndicate1"}, "time": "2022-08-28T02:16:39.484Z", "hostmask": "user4@127.0.0.1", "type": "join", "self": true, "id": 68, "previews": [], "text": ""}}]
42["users", {"chan": 7}]
42["users", {"chan": 7}]
42["open", 7]
O42["names", {"id": 7, "users": [{"nick": "Syndicate1", "mode": "@", "lastMessage": 0}]]]
O42["names", {"id": 7, "users": [{"nick": "Syndicate1", "mode": "@", "lastMessage": 0}]]]
O42["names", {"id": 7, "users": [{"nick": "Syndicate1", "mode": "@", "lastMessage": 0}]]]
42["msg", {"chan": 7, "msg": {"type": "mode_channel", "text": "+nt ", "from": {}, "id": 69, "previews": [], "self": false, "time": "2022-08-28T02:16:41.062Z"}}]
L42["join", {"network": "65167699-1c87-4cc5-ad52-fda442d06e36", "chan": {"type": "special", "special": "list_channels", "name": "Channel List", "data": {"text": "Loading channel list, this can take a moment..."}, "id": 3, "messages": [], "totalMessages": 0, "key": "", "topic": "", "state": 0, "firstUnread": 0, "unread": 0, "highlight": 0, "users": [], "index": 1}}]
C42["msg:special", {"chan": 3, "data": {"text": "Loaded 3 channels..."}}]
42["msg:special", {"chan": 3, "data": [{"channel": "#FederalLawEnforcementAgency", "num_users": 2, "topic": "[+nt] ", "tags": {}}, {"channel": "#thelounge", "num_users": 1, "topic": "[+nt] ", "tags": {}}, {"channel": "#Syndicate", "num_users": 1, "topic": "[+nt] ", "tags": {}}]] +@
42["msg", {"chan": 7, "msg": {"from": {"mode": "", "nick": "Syndicate2"}, "time": "2022-08-28T02:16:53.396Z", "hostmask": "user5@127.0.0.1", "type": "join", "self": false, "id": 70, "previews": [], "text": ""}}]
42["users", {"chan": 7}]

```

```

42["join",{"network":"65167699-1c87-4cc5-ad52-fda442d06e36","chan":
{"name":"#Syndicate","state":1,"id":4,"messages":
[],"totalMessages":0,"key":"","topic":"","type":"channel","firstUnread":0,"unread":0,"highlight":0,"users":
[]},"index":1}}
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Syndicate2"},"time":"2022-08-
28T02:16:53.401Z","hostmask":"user5@127.0.0.1","type":"join","self":true,"id":20,"previews":
[],"text":""}}]
42["users",{"chan":4}]
42["users",{"chan":4}]
42["names",{"id":7,"users":[{"nick":"Syndicate1","mode":"@","lastMessage":0},
{"nick":"Syndicate2","mode":"","lastMessage":0}]]
42["names",{"id":4,"users":[{"nick":"Syndicate1","mode":"@","lastMessage":0},
{"nick":"Syndicate2","mode":"","lastMessage":0}]]
42["names",{"id":4,"users":[{"nick":"Syndicate1","mode":"@","lastMessage":0},
{"nick":"Syndicate2","mode":"","lastMessage":0}]]
42["names",{"id":4,"users":[{"nick":"Syndicate1","mode":"@","lastMessage":0},
{"nick":"Syndicate2","mode":"","lastMessage":0}]]      ,@
42["msg",{"chan":4,"msg":{"type":"mode_channel","text":"+nt ","from":{},"id":21,"previews":
[],"self":false,"time":"2022-08-28T02:16:55.405Z"}}]
42["msg",{"chan":7,"msg":{"from":{"mode":"@","nick":"Syndicate1"},"type":"message","time":"2022-08-
28T02:20:22.701Z","text":"Benji Dunn just downloaded something from the drop zone. Its
encrypted.","self":true,"highlight":false,"users":[],"id":71,"previews":[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Syndicate1"},"type":"message","time":"2022-08-
28T02:20:22.702Z","text":"Benji Dunn just downloaded something from the drop zone. Its
encrypted.","self":false,"highlight":false,"users":[],"id":22,"previews":[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Syndicate2"},"type":"message","time":"2022-08-
28T02:20:36.021Z","text":"Dont worry we are on the inside. I will upload the
key.","self":true,"highlight":false,"users":[],"id":23,"previews":[]}}]
42["msg",{"chan":7,"msg":{"from":{"mode":"","nick":"Syndicate2"},"type":"message","time":"2022-08-
28T02:20:36.022Z","text":"Dont worry we are on the inside. I will upload the
key.","self":false,"highlight":false,"users":[],"id":72,"previews":[]}}]
42["msg",{"chan":7,"msg":{"from":{"mode":"@","nick":"Syndicate1"},"type":"message","time":"2022-08-
28T02:20:53.507Z","text":"From Dunn's PC?","self":true,"highlight":false,"users":[],"id":73,"previews":
[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"@","nick":"Syndicate1"},"type":"message","time":"2022-08-
28T02:20:54.509Z","text":"From Dunn's PC?","self":false,"highlight":false,"users":[],"id":24,"previews":
[]}}]
42["msg",{"chan":4,"msg":{"from":{"mode":"","nick":"Syndicate2"},"type":"message","time":"2022-08-
28T02:20:58.647Z","text":"Yes","self":true,"highlight":false,"users":[],"id":25,"previews":[]}}]
42["msg",{"chan":7,"msg":{"from":{"mode":"","nick":"Syndicate2"},"type":"message","time":"2022-08-
28T02:20:58.648Z","text":"Yes","self":false,"highlight":false,"users":[],"id":74,"previews":[]}}]

```