DIGITAL FORENSICS 'ASSIGNMENT 2: MAJOR ASSIGNMENT'

Name: Thomas Rutt

Scenario

You work as a digital forensic investigator for the European Law Enforcement Agency (ELEA). It is an unusually quiet period. Your friend Benoit Blanc has returned from a holiday in Greece where he has had an interesting adventure with famous billionaire Miles Bron. Benoit attended a party at Miles Bron's island holiday estate. One of the guests at the party, Youtuber Duke Cody, died in spectacular circumstances. Also a fire on the last day of the weekend has burnt the estate mansion to the ground. Benoit suspects that several crimes have been committed and that Miles Bron is responsible for perjury regarding the flagship product "Klear", a hydrogen-based alternative fuel that his company Alpha will soon launch. [1].

Task 1

Your immediate supervisor has agreed to allow you to assist Benoit in his investigation. Your supervisor has asked you to determine if there is evidence to charge Miles. Benoit has been able to collect various pieces of digital evidence for you to examine. Your supervisor suggests you address the following questions related to each piece of evidence.

Contents

Task 1

Evidence A - A disk image of an old desktop computer found in Andi Brand’s villa on the estate.

Task 1 involved obtaining the '3906ICT-EvidenceA.zip' file from ***'http://3906ictassignment.griffith.internal/'*** and moving the file to the relevant ***'cases/MilesBron'*** directory. From there I unzipped the ***'3906ICT-EvidenceA.zip'*** file and concatenated all of the raw data into one .dd file called 'miles.dd', this made investigating the raw data exceptionally easier as I could then do further research into the evidence as one data file. Once I had the data concatenated into one '.dd' file, I had a look at the image statistics using the ***'img_stat'*** command, this tells me the characteristics of the file, like the following:

```
--------------------------------------------

Image Type: raw

Size in bytes: 10737418240

Sector size: 512

--------------------------------------------
```

Another command I used is ***'mmls'***, a part of the sleuth kit, it is used for examining and analysing disk images. This displays the following when outputted:

```
DOS Partition Table

Offset Sector: 0

Units are in 512-byte sectors

 -----------------------------------------------------------------------------------------------------------


    Slot     Start       End        Length      Description

000:  Meta     0000000000   0000000000   0000000001   Primary Table (#0)


001:  -------   0000000000   0000000055   0000000056   Unallocated


002:  000:000   0000000056   0020948759   0020948704   NTFS / exFAT (0x07)


003:  -------   0020948760   0020971519   0000022760   Unallocated
```

Next I mounted the 'miles.dd' file to '/mnt/windows_mount' using the following command:

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

The above command is run as 'sudo' which enables it to be run as root user, mount command mounts the 'miles.dd' file as read only at the specified offset to '/mnt/windows_mount'.

The information displayed from this command tells us partition information, Disk layout analysis, File system analysis and Sector information.

Another command I ran to research information on the disk image was,

```
'fsstat -o 56 miles.dd'
```

The command above provides the below output:

```
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: 64CC5169CC513710
OEM Name: NTFS
Version: Windows XP
METADATA INFORMATION
--------------------------------------------

First Cluster of MFT: 786432
First Cluster of MFT Mirror: 1309293
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
```

```
Range: 0 - 13536
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
Cluster Size: 4096
Total Cluster Range: 0 - 2618586
Total Sector Range: 0 - 20948702

$AttrDef Attribute Values:

$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident

$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
```

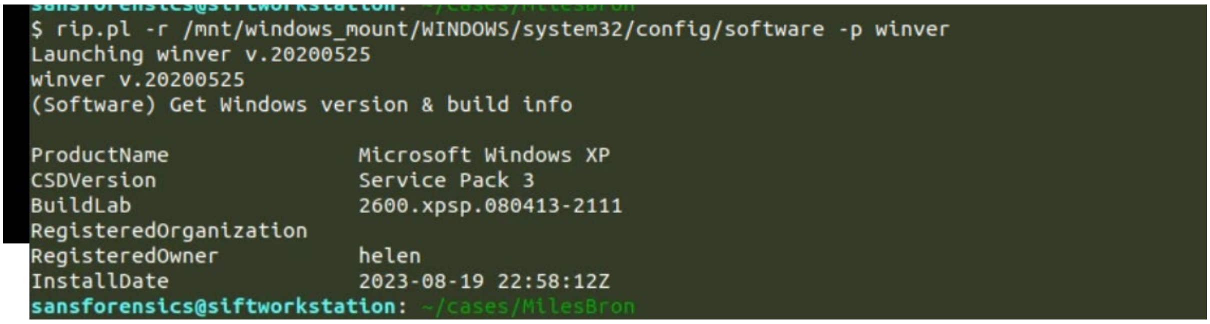
The information shown provides additional information about the miles.dd image, such as the 'File system type' and 'Version' which can be helpful in further investigation of the image.

Evidence 1
Who is the owner of the desktop?

The next step of the investigation process was to use the 'rip.pl' command to extract the first answer to "TASK 1":

'rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/software -p winver'

The above command uses the rip.pl script which extracts information from the registry hive located at the specified path. This command provided the 'RegisteredOwner' of the machine 'helen'.



```
sansforensics@siftworkstation: ~/cases/MilesBron
$ rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/software -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName              Microsoft Windows XP
CSDVersion               Service Pack 3
BuildLab                 2600.xpsp.080413-2111
RegisteredOrganization
RegisteredOwner          helen
InstallDate              2023-08-19 22:58:12Z
sansforensics@siftworkstation: ~/cases/MilesBron
```

Evidence 2
What programs have been installed on the desktop?

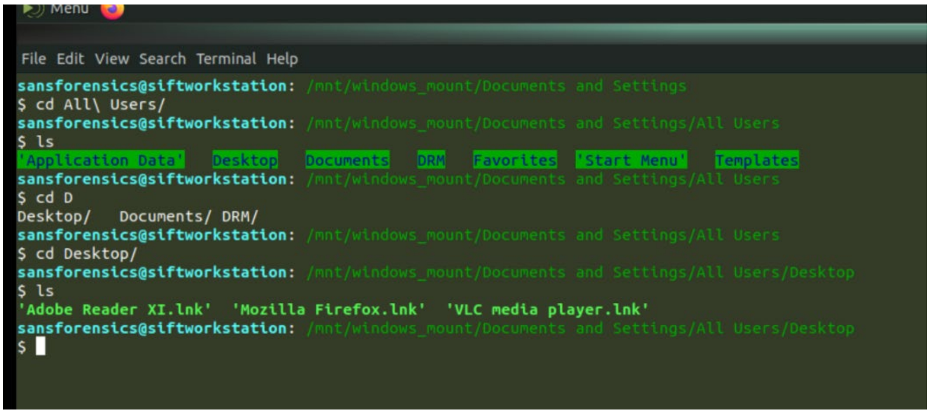
To locate the second piece of evidence for "Task 1", I looked in the following directory ***'/mnt/windows_mount/Documents_and_Settings/All_Users/Desktop'*** and found the following programs installed on the Desktop:

'Adobe Reader XI.lnk'

'Mozilla Firefox.lnk'

'VLC media player.lnk'

The directory displays the contents on the desktop for all users on the machine, the reason I looked in the ***"/All_users"*** directory is to ensure I am seeing all and any applications on the desktop for any user on the PC.



```
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings
$ cd All\ Users/
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/All Users
$ ls
'Application Data'   Desktop   Documents   DRM   Favorites  'Start Menu'   Templates
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/All Users
$ cd D
Desktop/   Documents/ DRM/
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/All Users
$ cd Desktop/
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/All Users/Desktop
$ ls
'Adobe Reader XI.lnk'  'Mozilla Firefox.lnk'  'VLC media player.lnk'
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/All Users/Desktop
$ 
```

Evidence 3

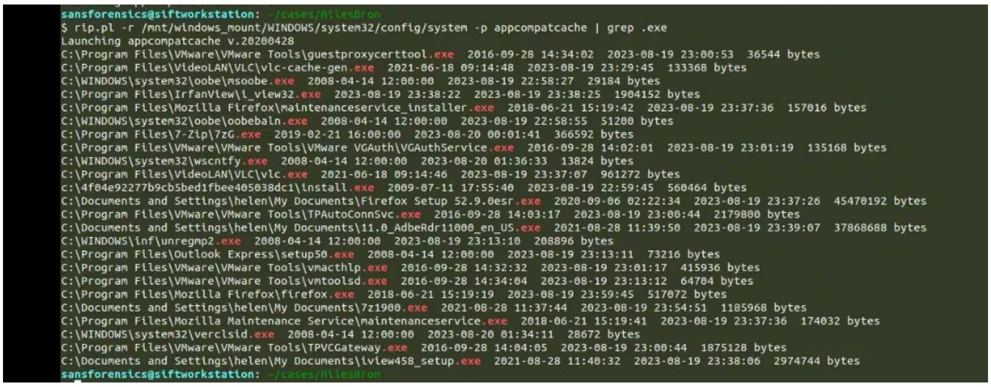
What recent programs have been run?

Evidence 3, I needed to find the most recent programs that were run on the computer, this can help identify what the applications the suspect was last running on the machine and may provide additional evidence for the case.

Using the following command ***"rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/system -p appcompatcache | grep .exe"***, I was able to list the recent programs that have been run, I found that the latest ran programs were:

"C:\WINDOWS\system32\wscntfy.exe" *which was last run on "2023-08-20 01:36:33".*

"C:\Documents and Settings\helen\My Documents\11.0_AdbeRdr11000_en_US.exe" last ran on "2023-08-19 23:39:07"



```
sansforensics@siftworkstation: ~/cases/MilesBron
$ rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/system -p appcompatcache | grep .exe
Launching appcompatcache v.20200428
C:\Program Files\VMware\VMware Tools\guestproxycerttool.exe  2016-09-28 14:34:02  2023-08-19 23:00:53  36544 bytes
C:\Program Files\VideoLAN\VLC\vlc-cache-gen.exe  2021-06-18 09:14:48  2023-08-19 23:29:45  133368 bytes
C:\WINDOWS\system32\oobe\msoobe.exe  2008-04-14 12:00:00  2023-08-19 22:58:27  29184 bytes
C:\Program Files\IrfanView\i_view32.exe  2023-08-19 23:38:22  2023-08-19 23:38:25  1904152 bytes
C:\Program Files\Mozilla Firefox\maintenanceservice_installer.exe  2018-06-21 15:19:42  2023-08-19 23:37:36  157016 bytes
C:\WINDOWS\system32\oobe\oobebaln.exe  2008-04-14 12:00:00  2023-08-19 22:58:55  51200 bytes
C:\Program Files\7-Zip\7zG.exe  2019-02-21 16:00:00  2023-08-20 00:01:41  366592 bytes
C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe  2016-09-28 14:02:01  2023-08-19 23:01:19  135168 bytes
C:\WINDOWS\system32\wscntfy.exe  2008-04-14 12:00:00  2023-08-20 01:36:33  13824 bytes
C:\Program Files\VideoLAN\VLC\vlc.exe  2021-06-18 09:14:46  2023-08-19 23:37:07  961272 bytes
c:\4f04e92277b9cb5bed1fbee405038dc1\install.exe  2009-07-11 17:55:40  2023-08-19 22:59:45  560464 bytes
C:\Documents and Settings\helen\My Documents\Firefox Setup 52.9.0esr.exe  2020-09-06 02:22:34  2023-08-19 23:37:26  45470192 bytes
C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe  2016-09-28 14:03:17  2023-08-19 23:00:44  2179800 bytes
C:\Documents and Settings\helen\My Documents\11.0_AdbeRdr11000_en_US.exe  2021-08-28 11:39:50  2023-08-19 23:39:07  37868688 bytes
C:\WINDOWS\inf\unregmp2.exe  2008-04-14 12:00:00  2023-08-19 23:13:10  208896 bytes
C:\Program Files\Outlook Express\setup50.exe  2008-04-14 12:00:00  2023-08-19 23:13:11  73216 bytes
C:\Program Files\VMware\VMware Tools\vmacthlp.exe  2016-09-28 14:32:32  2023-08-19 23:01:17  415936 bytes
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe  2016-09-28 14:34:04  2023-08-19 23:13:12  64704 bytes
C:\Program Files\Mozilla Firefox\firefox.exe  2018-06-21 15:19:19  2023-08-19 23:59:45  517072 bytes
C:\Documents and Settings\helen\My Documents\7z1900.exe  2021-08-28 11:37:44  2023-08-19 23:54:51  1185968 bytes
C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe  2018-06-21 15:19:41  2023-08-19 23:37:36  174032 bytes
C:\WINDOWS\system32\verclsid.exe  2008-04-14 12:00:00  2023-08-20 01:34:11  28672 bytes
C:\Program Files\VMware\VMware Tools\TPVCGateway.exe  2016-09-28 14:04:05  2023-08-19 23:00:44  1875128 bytes
C:\Documents and Settings\helen\My Documents\iview458_setup.exe  2021-08-28 11:40:32  2023-08-19 23:38:06  2974744 bytes
sansforensics@siftworkstation: ~/cases/MilesBron
```

Evidence 4

Recover details of any files in the recycle bin. Is there evidence that the owner of the desktop committed a crime?

To find evidence or the fourth question, I looked in the following directory:

'/mnt/windows_mount/RECYCLER/S-1-5-21-343818398-1563985344-725345543-1003'

Once I am in the correct location I use ***'recbin.pl -f INFO2'*** to find "Parse Windows Recycle Bin INFO2 & $Ixxxxx files in binary mode, translating the information listed; sends data to STDOUT, can also generate timeline data" according to the 'recbin.pl' help guide.

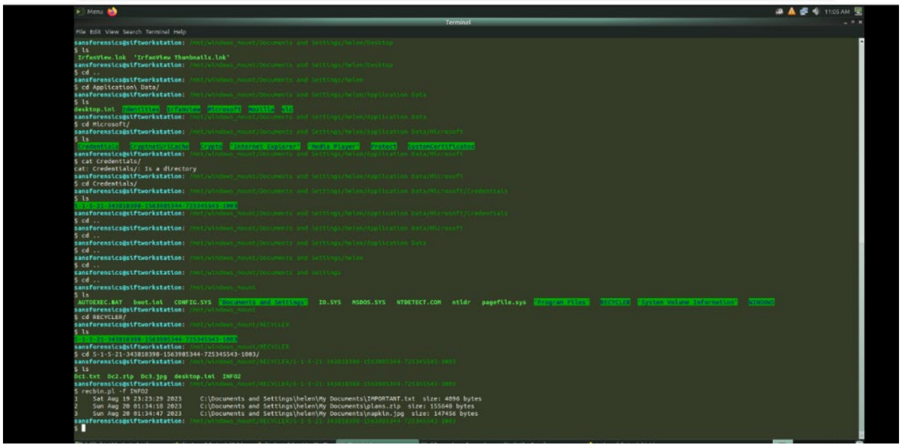
and found the following files:

'IMPORTANT.txt'

'Napkin.jpg'

'plans.zip'

The above files are interesting for two reasons, the first being the name of two of the files, 'IMPORTANT.txt' and 'plans.zip', the files tell me that this person may have had important plans that were tied to the investigation. The second reason being that the file extensions '.txt and .zip' are both files that could contain additional relevant information about the case.



```
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Desktop
$ ls
 IrfanView.lnk  'IrfanView Thumbnails.lnk'
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Desktop
$ cd ..
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen
$ cd Application\ Data/
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data
$ ls
desktop.ini  Identities  IrfanView  Microsoft  Mozilla  vlc
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data
$ cd Microsoft/
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data/Microsoft
$ ls
 Credentials   CryptnetUrlCache   Crypto  'Internet Explorer'  'Media Player'   Protect   SystemCertificates
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data/Microsoft
$ cat Credentials/
cat: Credentials/: Is a directory
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data/Microsoft
$ cd Credentials/
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data/Microsoft/Credentials
$ ls
S-1-5-21-343818398-1563985344-725345543-1003
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data/Microsoft/Credentials
$ cd ..
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data/Microsoft
$ cd ..
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen/Application Data
$ cd ..
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings/helen
$ cd ..
sansforensics@siftworkstation: /mnt/windows_mount/Documents and Settings
$ cd ..
sansforensics@siftworkstation: /mnt/windows_mount
$ ls
 AUTOEXEC.BAT   boot.ini   CONFIG.SYS  'Documents and Settings'   IO.SYS   MSDOS.SYS   NTDETECT.COM   ntldr   pagefile.sys  'Program Files'   RECYCLER  'System Volume Information'   WINDOWS
sansforensics@siftworkstation: /mnt/windows_mount
$ cd RECYCLER/
sansforensics@siftworkstation: /mnt/windows_mount/RECYCLER
$ ls
S-1-5-21-343818398-1563985344-725345543-1003
sansforensics@siftworkstation: /mnt/windows_mount/RECYCLER
$ cd S-1-5-21-343818398-1563985344-725345543-1003/
sansforensics@siftworkstation: /mnt/windows_mount/RECYCLER/S-1-5-21-343818398-1563985344-725345543-1003
$ ls
Dc1.txt  Dc2.zip  Dc3.jpg  desktop.ini  INFO2
sansforensics@siftworkstation: /mnt/windows_mount/RECYCLER/S-1-5-21-343818398-1563985344-725345543-1003
$ recbin.pl -f INFO2
1    Sat Aug 19 23:23:29 2023     C:\Documents and Settings\helen\My Documents\IMPORTANT.txt  size: 4096 bytes
2    Sun Aug 20 01:34:18 2023     C:\Documents and Settings\helen\My Documents\plans.zip  size: 155648 bytes
3    Sun Aug 20 01:34:47 2023     C:\Documents and Settings\helen\My Documents\napkin.jpg  size: 147456 bytes
sansforensics@siftworkstation: /mnt/windows_mount/RECYCLER/S-1-5-21-343818398-1563985344-725345543-1003
$ 
```

EVIDENCE B – Network capture of Miles Bron's estate network.

Evidence 5

Who are the people communicating in the transmission? When does the first transmission begin and the last transmission finish?

The evidence B task required me to obtain evidence within a .pcap file. In order to do this, I first downloaded the relevant ***"EvidenceB.pcap"*** file located at ***http://3906ictassignment.griffith.internal/.***

Once the file was downloaded, I moved the file to ***cases/MilesBron*** and unzipped using ***"unzip"***. I then loaded up wireshark using ***'wireshark &'*** to open in a separate browser. I started sifting through the streams of 'tcp' packets by right clicking on the most recent 'tcp' packet and clicking on 'follow' > 'follow stream'.

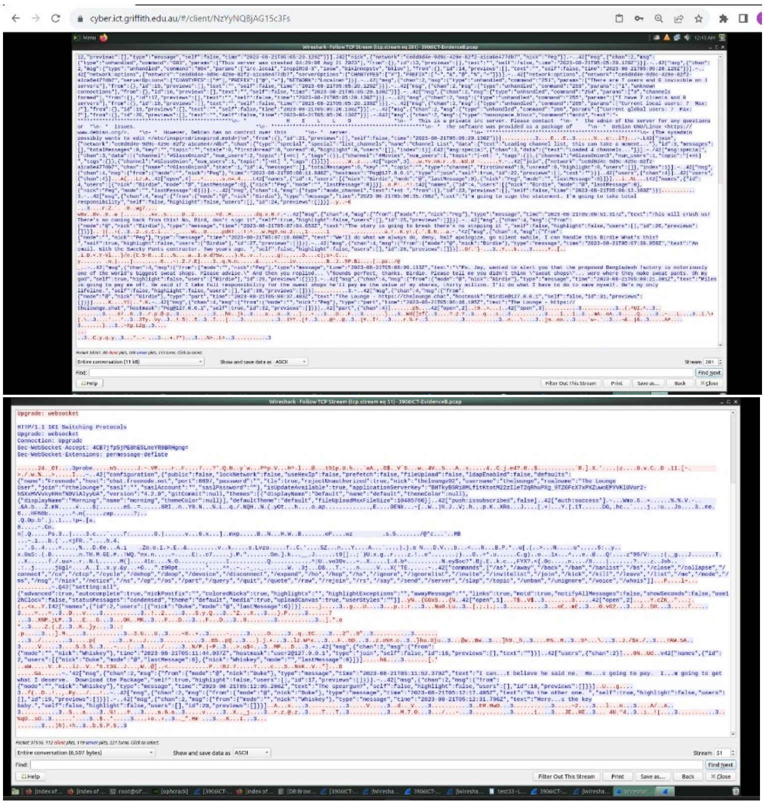
The first transmission started on 'stream 51' and last one on 'stream 281'.

I have identified the following “nicknames” within the multiple websocket packets that hold detailed conversions between the users:

- Miles
- Duke
- Peg
- Birdie
- Claire
- Lionel
- Andi
- Whiskey

This was located by opening ‘wireshark’ using ***‘wireshark &***’, than by opening the correct .pka file and applying a display filter to only filter for web socket packets.

The following are screenshots of only the first and last transmission between the users, as there were in total more than 6 different conversions.



cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs
Wireshark · Follow TCP Stream (tcp.stream eq 281) · 3906ICT-EvidenceB.pcap
Wireshark · Follow TCP Stream (tcp.stream eq 51) · 3906ICT-EvidenceB.pcap
Entire conversation (11 kB)
Entire conversation (6,507 bytes)
Show and save data as ASCII
Stream 281
Stream 51
Find:
Find Next
Help
Filter Out This Stream
Print
Save as…
Back
Close

```
Upgrade: websocket

HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: 4CB7jfp5jPE8hEGLneYR8BRHgng=
Sec-WebSocket-Extensions: permessage-deflate
```

Evidence 6

What browsers, operating systems and IP addresses are used by the communication endpoints?

The browsers used are, 'Mozilla Firefox' and 'Safari'

The operating systems used are, 'Ubuntu, linux' and Mac OS

Scanning through the Wireshark ‘websocket’ layers , I have discovered the following IP addresses:

10.10.10.1

10.10.10.254

10.10.10.56

10.10.10.22

10.10.10.33

10.10.10.44

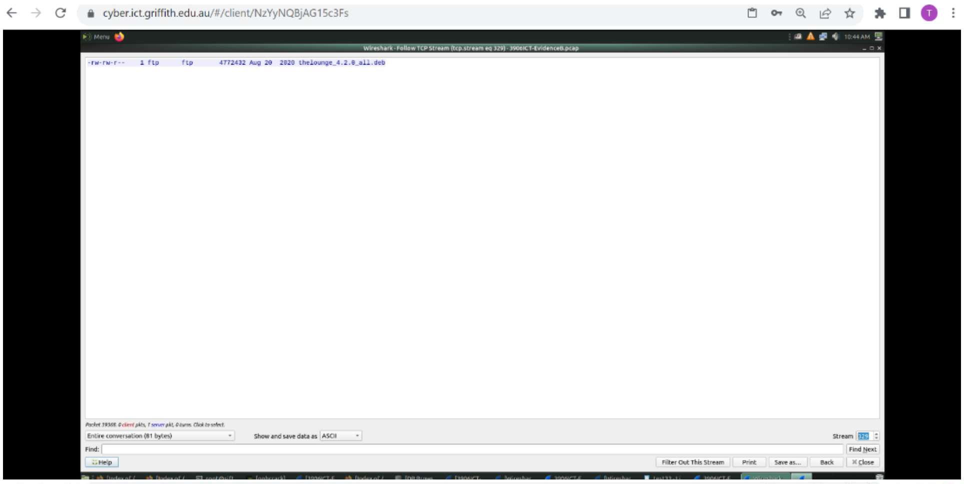
10.10.10.1

220.233.6.3

Evidence 7

What was the package that was sent on the internal network?

The package being sent across the network is called “thelounge_4.2.0_all.deb” and was sent on Aug 20th, this may have been the package “Duke Cody” was in communication about with “Whiskey”



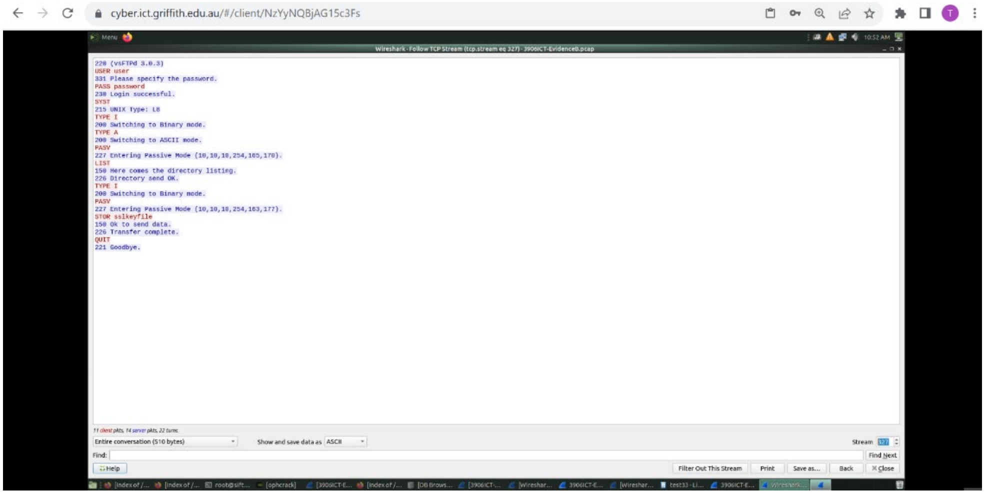
cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs

Wireshark · Follow TCP Stream (tcp.stream eq 329) · 3906ICT-Evidence8.pcap

```
-rw-rw-r--    1 ftp      ftp       4772432 Aug 20  2020 thelounge_4.2.0_all.deb
```

Packet 39568. 0 client pkts, 1 server pkt, 0 turns. Click to select.

Entire conversation (81 bytes) Show and save data as ASCII



cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs

Wireshark · Follow TCP Stream (tcp.stream eq 327) · 3906ICT-Evidence8.pcap

```
220 (vsFTPd 3.0.3)
USER user
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
TYPE I
200 Switching to Binary mode.
TYPE A
200 Switching to ASCII mode.
PASV
227 Entering Passive Mode (10,10,10,254,165,170).
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (10,10,10,254,163,177).
STOR sslkeyfile
150 Ok to send data.
226 Transfer complete.
QUIT
221 Goodbye.
```

11 client pkts, 14 server pkts, 22 turns.

Entire conversation (510 bytes) Show and save data as ASCII

Evidence 8 - Does the network capture reveal the relationship between Miles Bron and the people participating in the intercepted communications?

Answer:

The relationship between “Miles Bron” and the other people participating in the intercepted communications looks suspicious, however it does not uncover anything directly towards the murder, although there is some animosity between “Duke Cody” and “Miles Bron”, by the looks of it, duke saying to “Whiskey” that he will get payback to “Miles Bron” as “Miles Bron” did not give “Duke Cody” the chance to be on his news channel. However, “Miles Bron” did say that “Duke” Cody was a loyal friend, “Whiskey” said “Duke Cody” deserves the chance due to him doing something, I am assuming for “Miles Bron”. “Duke Cody” then tells “Whiskey” to download a package.

The messages between “lIonel” and “Claire” are very suspicious, they are talking about “Claire” signing off on a power plant, using the “klear” energy, “Lionel” is saying that “Andi” is correct about it being dangerous, and it will blow the house up if it is used, as the particles are too small and will leak. There is no mention of “Miles Bron” in this conversation apart from the beginning, where “Whiskey” says “This is the only messaging available on the island, typical Miles”, this uncovers that they are already on the island.

There was also another conversation between “Birdie” and “Peg” discussing the sweat shop, “Birdie” says he is going to sign a statement and take full responsibility for it, saying “Miles Bron” will pay him the value of his shares, being $30 million. “Peg” says it will crush them and not to sign it.

Evidence C – A disk image of a damaged mobile phone found near Duke Cody.

Evidence 9
What are the non-stock applications installed on the phone?

After downloading the ***'3906ICT-EvidenceD.7z'*** file and moving it to ***'cases/Milebron'*** and unzipping said file using ***'7za e 3906ICT-EvidenceD.7z'*** into ***the 'cases/Milesbron'*** directory. Once this was complete, I then mounted ***'dm-o'*** onto ***'/mnt/e01'*** directory and used ***'cd /mnt/e01'*** to go into this directory. I then searched around and concluded that it makes sense for apps to be within the ***'/mnt/e01/app'*** directory, which was correct.

'bubbleshooter' 'com.rovio.angrybirds' 'com.twitter.android

'com.facebook.katana 'com.tencent'   'stericson.busybox'

Evidence 10
Who is in the contacts list? What messages and calls have been sent and received by the phone?

I firstly mounted the two files that read data (vda and vde) to ‘***/mnt/e01***’ and activated ***'sudo su'*** to have full access, then went into the ***‘/mnt/e01’*** directory to locate some data. I went into ***'/mnt/e01/data/com.android.providers.contacts/databases'***, and used ***'cp contacts2.db /cases'*** to copy ***the 'contacts2.db'*** file to the ‘***/cases***’ directory for easy finding later on. I then redirected to ***‘/cases’*** and used ***'chown sansforensics:sansforensics contacts2.db'*** to give full permissions to this file. I then opened 'DB Browser for SQLite' and loaded the 'contacts2.db' databse file and looked within the 'view contacts' tale which dispalys the following:

Contacts:

Ma Cody

Whiskey

Miles Bron

Lalo

Gus Fring

Mike

Recent phone calls:

1888777666

1888777666

1888777666

1222333444

1555666777

Recent sms messages:

1222333444 2 1692792086496 1692792086000 0 1 -1 1 0 **Hey babe I tried.**

1222333444 2 1692792120218 1692792120000 0 1 -1 1 0 **It was all for you.**

1888777666 1 1692792170024 1692792170000 0 1 -1 1 0 **Why don?t you pick up when I call**

1888777666 1 1692792198903 1692792199000 0 1 -1 1 0 **You take care of yourself, you are still my baby. You keep away from that pineapple. That?s where they come from you know.**

1888777666 1 1692792226997 1692792227000 0 1 -1 1 0 **Don?t you sass your mum.**

1555666777 3 1692792524432 1692792524000 0 1 -1 1 0 **No she?s not I can see her right now.**

1555666777 3 1692792548672 1692792549000 0 1 -1 1 0 **Yes let?s talk.**

1222333444 1692792108417 0 1 -1 2 **That?s OK babe, I know.**

1222333444 1692792139753 0 1 -1 2 **I only need that one break and I know I can make it even bigger on Alpha News.**

1888777666 1692792187969 0 1 -1 2 **Ma!!!**

1888777666 1692792216481 0 1 -1 2 **Ma, pineapples come from the tropics. Not Greece.**

1555666777 1692792501000 0 1 -1 2 **Miles don?t you forget I saw you that afternoon leaving Andi?s house. Now I see that Alpha News is reporting Andi is dead.**

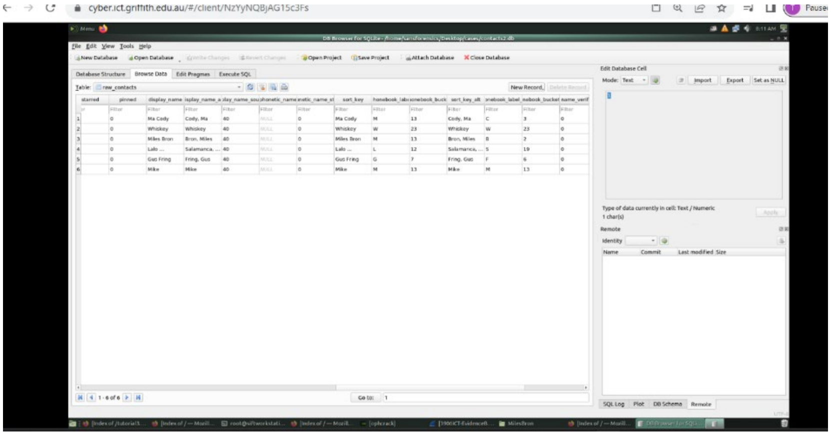
1555666777 1692792538763 0 1 -1 2 **We need to talk. You owe me.**

The above files were located within

/mnt/e01/user_de/0/com.android.providers.telephony/databases

I then used 'cp mmssms.db /cases' to copy the file to the /cases directory, and 'chown sansforensics:sansforensics mmssms.db' to give full access.

The table within the 'DB Browser for SQLite' was 'sms_restricted'.



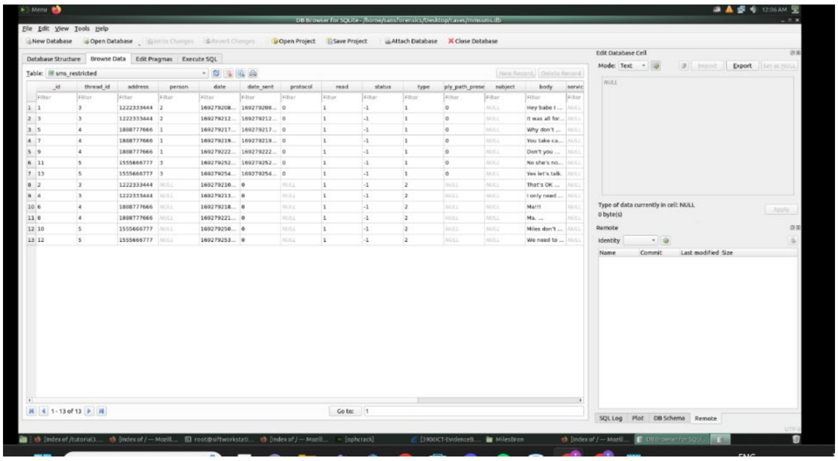
cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs

DB Browser for SQLite - /home/sansforensics/Desktop/cases/contacts2.db

Table: raw_contacts

	starred	pinned	display_name	isplay_name_a	play_name_sou	phonetic_name	netic_name_st	sort_key	honebook_lab	onebook_buck	sort_key_alt	onebook_label	nebook_bucket	name_verif
1		0	Ma Cody	Cody, Ma	40	NULL	0	Ma Cody	M	13	Cody, Ma	C	3	0
2		0	Whiskey	Whiskey	40	NULL	0	Whiskey	W	23	Whiskey	W	23	0
3		0	Miles Bron	Bron, Miles	40	NULL	0	Miles Bron	M	13	Bron, Miles	B	2	0
4		0	Lalo ...	Salamanca, ...	40	NULL	0	Lalo ...	L	12	Salamanca, ...	S	19	0
5		0	Gus Fring	Fring, Gus	40	NULL	0	Gus Fring	G	7	Fring, Gus	F	6	0
6		0	Mike	Mike	40	NULL	0	Mike	M	13	Mike	M	13	0

1 - 6 of 6

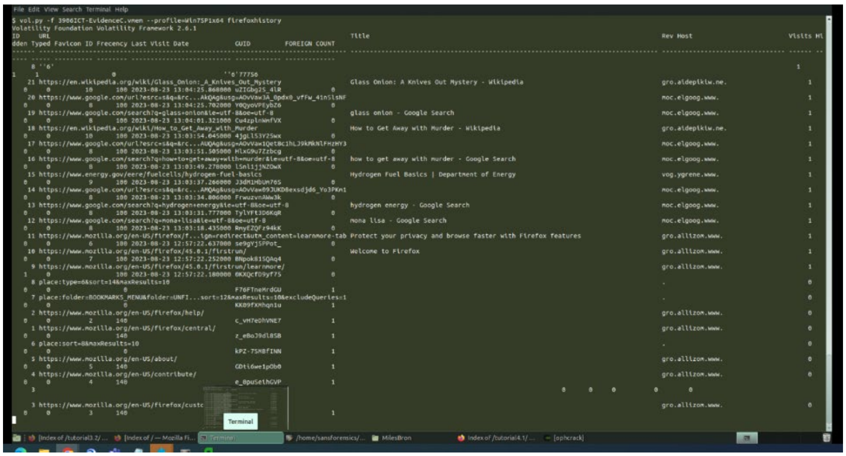


DB Browser for SQLite - /home/sansforensics/Desktop/cases/mmssms.db

Table: sms_restricted

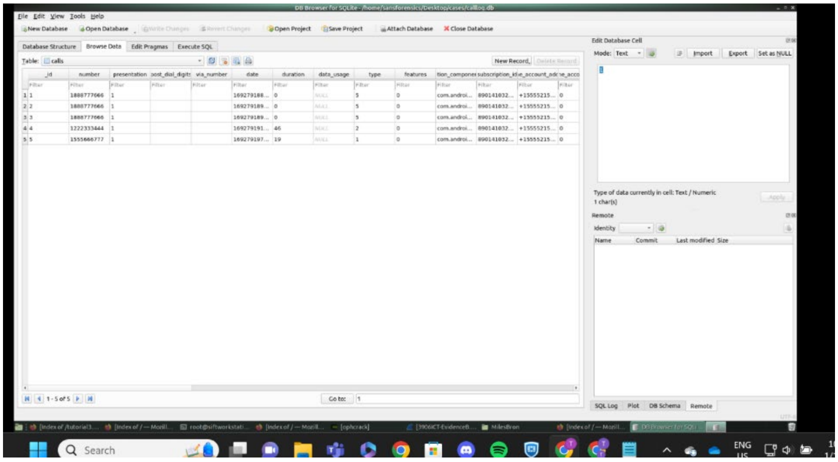
	_id	thread_id	address	person	date	date_sent	protocol	read	status	type	ply_path_prese	subject	body	servic
1	1	3	1222333444	2	169279208...	169279208...	0	1	-1	1	0	NULL	Hey babe I ...	NULL
2	3	3	1222333444	2	169279212...	169279212...	0	1	-1	1	0	NULL	It was all for...	NULL
3	5	4	1888777666	1	169279217...	169279217...	0	1	-1	1	0	NULL	Why don't ...	NULL
4	7	4	1888777666	1	169279219...	169279219...	0	1	-1	1	0	NULL	You take ca...	NULL
5	9	4	1888777666	1	169279222...	169279222...	0	1	-1	1	0	NULL	Don't you ...	NULL
6	11	5	1555666777	3	169279252...	169279252...	0	1	-1	1	0	NULL	No she's no...	NULL
7	13	5	1555666777	3	169279254...	169279254...	0	1	-1	1	0	NULL	Yes let's talk.	NULL
8	2	3	1222333444	NULL	169279210...	0	NULL	1	-1	2	NULL	NULL	That's OK ...	NULL
9	4	3	1222333444	NULL	169279213...	0	NULL	1	-1	2	NULL	NULL	I only need ...	NULL
10	6	4	1888777666	NULL	169279218...	0	NULL	1	-1	2	NULL	NULL	Ma!!!	NULL
11	8	4	1888777666	NULL	169279221...	0	NULL	1	-1	2	NULL	NULL	Ma. ...	NULL
12	10	5	1555666777	NULL	169279250...	0	NULL	1	-1	2	NULL	NULL	Miles don't ...	NULL
13	12	5	1555666777	NULL	169279253...	0	NULL	1	-1	2	NULL	NULL	We need to ...	NULL

1 - 13 of 13



```
$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 firefoxhistory
Volatility Foundation Volatility Framework 2.6.1
ID     URL                                                                        Title                                                          Rev Host                     Visits Hi
dden Typed Favicon ID Frecency Last Visit Date            GUID         FOREIGN COUNT
------ -------------------------------------------------------------------------- -------------------------------------------------------------- ---------------------------- ------ --
---- ----- ---------- -------- -------------------------- ------------ -------------
    0 ''6'                                                                                                                                                                  1
1     1                0                              ''6'77756
  21 https://en.wikipedia.org/wiki/Glass_Onion:_A_Knives_Out_Mystery           Glass Onion: A Knives Out Mystery - Wikipedia                  gro.aidepikiw.ne.             1
   0     0          10       100 2023-08-23 13:04:25.868000 uZIGbg2S_4lR            0
  20 https://www.google.com/url?esrc=s&q=&rc...AkQAg&usg=AOvVaw3A_0pdx0_vfFw_41nSlsNF                                                                 moc.elgoog.www.               1
   0     0           8       100 2023-08-23 13:04:25.702000 Y0QyoVPEybZ6            0
  19 https://www.google.com/search?q=glass+onion&ie=utf-8&oe=utf-8             glass onion - Google Search                                    moc.elgoog.www.               1
   0     0           8       100 2023-08-23 13:04:01.321000 Cu4zplnWmfVX            0
  18 https://en.wikipedia.org/wiki/How_to_Get_Away_with_Murder                 How to Get Away with Murder - Wikipedia                        gro.aidepikiw.ne.             1
   0     0          10       100 2023-08-23 13:03:54.045000 4jgLl53Y25wx            0
  17 https://www.google.com/url?esrc=s&q=&rc...AUQAg&usg=AOvVaw1Qet8c1hLJ9kMkNlFHzHY3                                                                 moc.elgoog.www.               1
   0     0           8       100 2023-08-23 13:03:51.505000 HlxG9u7Zzbcg            0
  16 https://www.google.com/search?q=how+to+get+away+with+murder&ie=utf-8&oe=utf-8   how to get away with murder - Google Search              moc.elgoog.www.               1
   0     0           8       100 2023-08-23 13:03:49.278000 lSnl1jjNZOwX            0
  15 https://www.energy.gov/eere/fuelcells/hydrogen-fuel-basics                Hydrogen Fuel Basics | Department of Energy                    vog.ygrene.www.               1
   0     0           9       100 2023-08-23 13:03:37.266000 J3dM1MbUm76S            0
  14 https://www.google.com/url?esrc=s&q=&rc...AMQAg&usg=AOvVaw09JUKD8exsdjd6_Yo3PKm1                                                                 moc.elgoog.www.               1
   0     0           8       100 2023-08-23 13:03:34.806000 FrwuzvnAWw3k            0
  13 https://www.google.com/search?q=hydrogen+energy&ie=utf-8&oe=utf-8         hydrogen energy - Google Search                                moc.elgoog.www.               1
   0     0           8       100 2023-08-23 13:03:31.777000 TylYFt3D6KqR            0
  12 https://www.google.com/search?q=mona+lisa&ie=utf-8&oe=utf-8               mona lisa - Google Search                                      moc.elgoog.www.               1
   0     0           8       100 2023-08-23 13:03:18.435000 RmyEZQFz94kK            0
  11 https://www.mozilla.org/en-US/firefox/f...ign=redirect&utm_content=learnmore-tab Protect your privacy and browse faster with Firefox features gro.allizom.www.     1
   0     0           6       100 2023-08-23 12:57:22.637000 se9gYj5PPot_            0
  10 https://www.mozilla.org/en-US/firefox/45.0.1/firstrun/                    Welcome to Firefox                                             gro.allizom.www.              1
   0     0           7       100 2023-08-23 12:57:22.252000 BNpok81SQAq4            0
   9 https://www.mozilla.org/en-US/firefox/45.0.1/firstrun/learnmore/                                                                            gro.allizom.www.              1
   1     0                   100 2023-08-23 12:57:22.180000 0KXQcfD9yf75            0
   8 place:type=6&sort=14&maxResults=10                                                                                                          .                             0
   0     0           0                                  F76FTneMrdGU            1
   7 place:folder=BOOKMARKS_MENU&folder=UNFI...sort=12&maxResults=10&excludeQueries=1                                                            .                             0
   0     0           0                                  KK09fXMhqn1u            1
   2 https://www.mozilla.org/en-US/firefox/help/                                                                                                 gro.allizom.www.              0
   0     0           2       140                        c_vM7eDhVNE7            1
   1 https://www.mozilla.org/en-US/firefox/central/                                                                                              gro.allizom.www.              0
   0     0                   140                        z_eBoJ9dl8SB            1
   6 place:sort=8&maxResults=10                                                                                                                  .                             0
   0     0           0                                  kPZ-7SMBfINN            1
   5 https://www.mozilla.org/en-US/about/                                                                                                        gro.allizom.www.              0
   0     0           5       140                        GDti6we1pOb0            1
   4 https://www.mozilla.org/en-US/contribute/                                                                                                   gro.allizom.www.              0
   0     0           4       140                        e_0puSeihGVP            1
   3                                                                                          0      0     0          0         0

   3 https://www.mozilla.org/en-US/firefox/custc                                                                                                 gro.allizom.www.              0
   0     0           3       140                                                1
```

File Edit View Search Terminal Help
Terminal
[Index of /tutorial3.2/ ...
[Index of / — Mozilla Fi...
Terminal
/home/sansforensics/...
MilesBron
Index of /tutorial4.1/ ...
[ophcrack]



DB Browser for SQLite - /home/sansforensics/Desktop/cases/calllog.db

Table: calls

	_id	number	presentation	post_dial_digits	via_number	date	duration	data_usage	type	features	tion_componen	subscription_id	e_account_adc	e_acco
1	1	1888777666	1			169279188...	0	NULL	5	0	com.androi...	890141032...	+15555215...	0
2	2	1888777666	1			169279189...	0	NULL	5	0	com.androi...	890141032...	+15555215...	0
3	3	1888777666	1			169279189...	0	NULL	5	0	com.androi...	890141032...	+15555215...	0
4	4	1222333444	1			169279191...	46	NULL	2	0	com.androi...	890141032...	+15555215...	0
5	5	1555666777	1			169279197...	19	NULL	1	0	com.androi...	890141032...	+15555215...	0

Type of data currently in cell: Text / Numeric
1 char(s)

Evidence 11

What Internet searches has the owner of the phone made?

The internet searches that were made on the phone are listed below:

https://www.google.com/search?q=how+to+blackmail&oq=how+to+blackmail&aqs=chrome..69i57j0l3.3266j0j7&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8

https://www.google.com/search?client=ms-unknown&sca_esv=559361602&sxsrf=AB5stBgXAc3-aY8VDppBJuONOjkwgnbENg%3A1692792599506&q=Andi+Brand&oq=Andi+Brand&aqs=heirloom-srp..015?

https://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mystery/1Geek

https://www.geekgirlauthority.com/movie-review-glass-onion-a-knives-out-mystery-rian-johnson-daniel-craig-monae-bautista/embed/#?secret=HHRUCF0RPk#?secret=gdkGkfmzG?

https://www.google.com/search?q=miles+bron&oq=Miles+Bron&aqs=chrome.0.0l3.1874j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF80?

https://movieweb.com/glass-onion-parallells-between-miles-bronn-and-elon-musk6https://www.google.c808?

https://www.google.com/search?q=men%27s+rights&oq=men%27s+rights&aqs=chrome..69i57j0l3.2828j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8men

https://en.m.wikipedia.org/wiki/Men%27s_rights_movement!Men

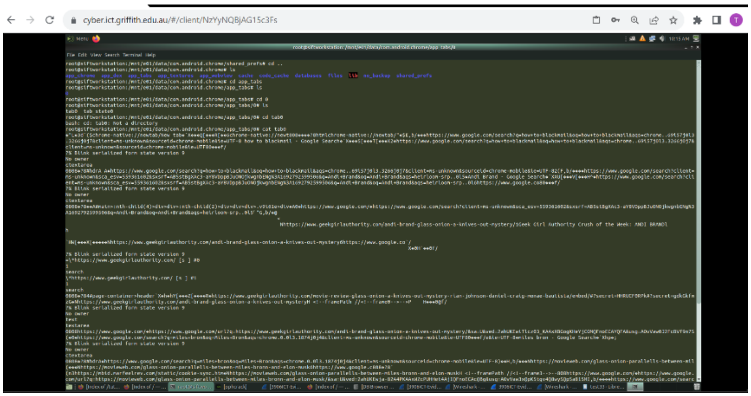
https://www.google.com/url?q=https://en.m.wikipedia.org/wiki/Men%2527s_rights_movement&sa=U&ved=2ahUKEwjq_KWI4PKAAxVG_2EKHbBFDFYQFnoECAAQAg&usg=AOvVaw0w-nTN-1yglc83bbpRvNqB

The above google searches were located in the following directory:

/mnt/e01/data/com.android.chrome/app_tabs/0/tab0

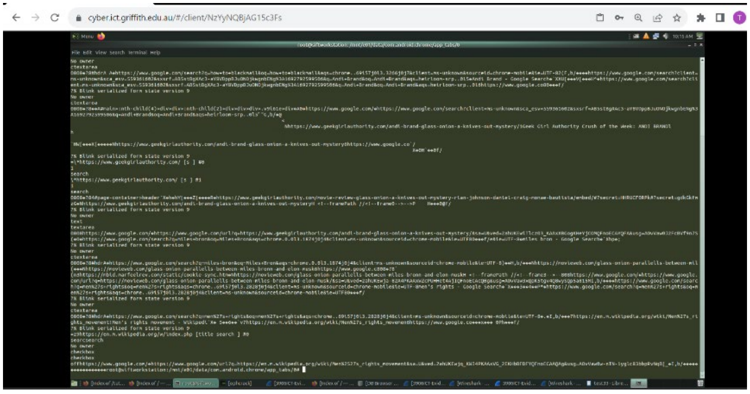
I followed the obvious path, this being the /com.android.chrome directory and searched within this file until I eventually came across the correct file with the evidence.

The following are screenshots of the recent google searches found in the chrome application:



cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs

```
root@siftworkstation:/mnt/e01/data/com.android.chrome/shared_prefs# cd ..
root@siftworkstation:/mnt/e01/data/com.android.chrome# ls
app_chrome  app_dex  app_tabs  app_textures  app_webview  cache  code_cache  databases  files  lib  no_backup  shared_prefs
root@siftworkstation:/mnt/e01/data/com.android.chrome# cd app_tabs
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_tabs# ls
0
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_tabs# cd 0
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_tabs/0# ls
tab0  tab_state0
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_tabs/0# cd tab0
bash: cd: tab0: Not a directory
root@siftworkstation:/mnt/e01/data/com.android.chrome/app_tabs/0# cat tab0
*"L<3d`(Schrome-native://newtab/New tab`X***Q[***R[**chrome-native://newtab0****?8htmlchrome-native://newtab/"*5E,b/***https://www.google.com/search?q=how+to+blackmail&oq=how+to+blackmail&aqs=chrome..69i57j0l3.3266j0j7&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8 how to blackmail - Google Search`X***S[***T[***X2ehttps://www.google.com/search?q=how+to+blackmail&oq=how+to+blackmail&aqs=chrome..69i57j0l3.3266j0j7&client=ms-unknown&sourceid=chrome-mobile&ie=UTF80***f/
7% Blink serialized form state version 9
No owner
ctextarea
0808*?8#hdrA A*https://www.google.com/search?q=how+to+blackmail&oq=how+to+blackmail&aqs=chrome..69i57j0l3.3266j0j7&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-82(F,b/****https://www.google.com/search?client=ms-unknown&sca_esv=559361602&sxsrf=AB5stBgXAc3-aY8VDppBJuDN0jkwgnbENg%3A1692792599506&q=Andi+Brand&oq=Andi+Brand&aqs=heirloom-srp..0l5*Andi Brand - Google Search`XXU[***V[***^*https://www.google.com/search?client=ms-unknown&sca_esv=559361602&sxsrf=AB5stBgXAc3-aY8VDppBJuDN0jkwgnbENg%3A1692792599506&q=Andi+Brand&oq=Andi+Brand&aqs=heirloom-srp..0l6https://www.google.co80***f/
7% Blink serialized form state version 9
No owner
ctextarea
0808*?8**A#main>:nth-child(4)>div>div>:nth-child(2)>div>div>div>.v9i61e>div*A6*https://www.google.com/*https://www.google.com/search?client=ms-unknown&sca_esv=559361602&sxsrf=AB5stBgXAc3-aY8VDppBJuDN0jkwgnbENg%3A1692792599506&q=Andi+Brand&oq=Andi+Brand&aqs=heirloom-srp..0l5`"G,b/*@
                                        Nhttps://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mystery/1Geek Girl Authority Crush of the Week: ANDI BRAND1
h

`HN[***X[*****Nhttps://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mystery8https://www.google.co`/
                                                                                       X*0H`**0f/
7% Blink serialized form state version 9
=\*https://www.geekgirlauthority.com/ [s ] #0
1
search
\*https://www.geekgirlauthority.com/ [s ] #1
1
search
0808*?84#page-container>header`XehehY[***Z[****Rehttps://www.geekgirlauthority.com/movie-review-glass-onion-a-knives-out-mystery-rian-johnson-daniel-craig-monae-bautista/embed/#?secret=HNRUCFORPkA?secret=gdkGkfmzGeNhttps://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mysteryH <!--framePath //<!--frame0-->-->P    Heee0@f/
7% Blink serialized form state version 9
No owner
text
textarea
0808https://www.google.com/*https://www.google.com/url?q=https://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mystery/&sa=U&ved=2ahUKEwiTlcz03_KAAxXBGogKHeYjCONQFnoECAYQFA&usg=AOvVaw0J2FcBVf9n7S(e0ehttps://www.google.com/search?q=miles+bron&oq=Miles+Bron&aqs=chrome.0.0l3.1874j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF80***f/e8ie=UTF-8emiles bron - Google Search`Xhpe;
7% Blink serialized form state version 9
No owner
ctextarea
0808*?8#hdrA*https://www.google.com/search?q=miles+bron&oq=Miles+Bron&aqs=chrome.0.0l3.1874j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8)**H,b/***Nhttps://movieweb.com/glass-onion-parallells-between-mil(***Nhttps://movieweb.com/glass-onion-parallells-between-miles-bronn-and-elon-musk8https://www.google.c808*?8`
(n3https://mbid.marfeelrev.com/static/cookie-sync.htm*Nhttps://movieweb.com/glass-onion-parallells-between-miles-bronn-and-elon-muskH <!--framePath //<!--frame1-->--808https://www.google.com/*https://www.google.com/url?q=https://movieweb.com/glass-onion-parallells-between-miles-bronn-and-elon-musk/&sa=U&ved=2ahUKEwja-8Z4PKAAxWZcPUHHet4AjIQFnoECAcQBg&usg=AOvVaw3xQpK5tqv4QBwySQp5a815HI,b/****https://www.google.com/searc
```



cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs

```
No owner
ctextarea
0808*?8#hdrA A*https://www.google.com/search?q=how+to+blackmail&oq=how+to+blackmail&aqs=chrome..69i57j0l3.3266j0j7&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-82(F,b/****https://www.google.com/search?client=ms-unknown&sca_esv=559361602&sxsrf=AB5stBgXAc3-aY8VDppBJuDN0jkwgnbENg%3A1692792599506&q=Andi+Brand&oq=Andi+Brand&aqs=heirloom-srp..0l5*Andi Brand - Google Search`XXU[***V[***^*https://www.google.com/search?client=ms-unknown&sca_esv=559361602&sxsrf=AB5stBgXAc3-aY8VDppBJuDN0jkwgnbENg%3A1692792599506&q=Andi+Brand&oq=Andi+Brand&aqs=heirloom-srp..0l6https://www.google.co80***f/
7% Blink serialized form state version 9
No owner
ctextarea
0808*?8**A#main>:nth-child(4)>div>div>:nth-child(2)>div>div>div>.v9i61e>div*A6*https://www.google.com/*https://www.google.com/search?client=ms-unknown&sca_esv=559361602&sxsrf=AB5stBgXAc3-aY8VDppBJuDN0jkwgnbENg%3A1692792599506&q=Andi+Brand&oq=Andi+Brand&aqs=heirloom-srp..0l5`"G,b/*@
                                        Nhttps://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mystery/1Geek Girl Authority Crush of the Week: ANDI BRAND1
h

`HN[***K[*****Nhttps://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mystery8https://www.google.co`/
                                                                                       X*0H`**0f/
7% Blink serialized form state version 9
=\*https://www.geekgirlauthority.com/ [s ] #0
1
search
\*https://www.geekgirlauthority.com/ [s ] #1
1
search
0808*?84#page-container>header`XehehY[***Z[****Rehttps://www.geekgirlauthority.com/movie-review-glass-onion-a-knives-out-mystery-rian-johnson-daniel-craig-monae-bautista/embed/#?secret=HNRUCFORPkA?secret=gdkGkfmzGeNhttps://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mysteryH <!--framePath //<!--frame0-->-->P    Heee0@f/
7% Blink serialized form state version 9
No owner
text
textarea
0808https://www.google.com/*https://www.google.com/url?q=https://www.geekgirlauthority.com/andi-brand-glass-onion-a-knives-out-mystery/&sa=U&ved=2ahUKEwiTlcz03_KAAxXBGogKHeYjCONQFnoECAYQFA&usg=AOvVaw0J2FcBVf9n7S(e0ehttps://www.google.com/search?q=miles+bron&oq=Miles+Bron&aqs=chrome.0.0l3.1874j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF80***f/e8ie=UTF-8emiles bron - Google Search`Xhpe;
7% Blink serialized form state version 9
No owner
ctextarea
0808*?8#hdrA*https://www.google.com/search?q=miles+bron&oq=Miles+Bron&aqs=chrome.0.0l3.1874j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8)**H,b/***Nhttps://movieweb.com/glass-onion-parallells-between-mil(***Nhttps://movieweb.com/glass-onion-parallells-between-miles-bronn-and-elon-musk8https://www.google.c808*?8`
(n3https://mbid.marfeelrev.com/static/cookie-sync.htm*Nhttps://movieweb.com/glass-onion-parallells-between-miles-bronn-and-elon-muskH <!--framePath //<!--frame1-->--808https://www.google.com/*https://www.google.com/url?q=https://movieweb.com/glass-onion-parallells-between-miles-bronn-and-elon-musk/&sa=U&ved=2ahUKEwja-8Z4PKAAxWZcPUHHet4AjIQFnoECAcQBg&usg=AOvVaw3xQpK5tqv4QBwySQp5a815HI,b/****https://www.google.com/search?q=men%27s+rights&oq=men%27s+rights&aqs=chrome..69i57j0l3.2828j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8men's rights - Google Search`X***3***P*https://www.google.com/search?q=men%27s+rights&oq=men%27s+rights&aqs=chrome..69i57j0l3.2828j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF80***f/
7% Blink serialized form state version 9
No owner
ctextarea
0808*?8#hdrA*https://www.google.com/search?q=men%27s+rights&oq=men%27s+rights&aqs=chrome..69i57j0l3.2828j0j4&client=ms-unknown&sourceid=chrome-mobile&ie=UTF-8e.eI,b/***7https://en.m.wikipedia.org/wiki/Men%27s_rights_movement!Men's rights movement - Wikipedi`X* 5***`v7https://en.m.wikipedia.org/wiki/Men%27s_rights_movemen8https://www.google.co****X***  0f***f/
7% Blink serialized form state version 9
=29https://en.m.wikipedia.org/w/index.php [title search ] #0
searcsearch
No owner
checkbox
checkbox
offhttps://www.google.com/*https://www.google.com/url?q=https://en.m.wikipedia.org/wiki/Men%2527s_rights_movement&sa=U&ved=2ahUKEwjq_KWI4PKAAxVG_2EKHbBFDFYQFnoECAAQAg&usg=AOvVaw0w-nTN-1yglc83bbpRvNqB]_eI,b/************************root@siftworkstation:/mnt/e01/data/com.android.chrome/app_tabs/0#
```

Evidence 12

Is there other evidence on the phone that might indicate the role of the owner in criminal activity?

Their email is sr8640171@gmail.com

Evidence D - a memory dump of a personal laptop found in the remains of the estate fire.

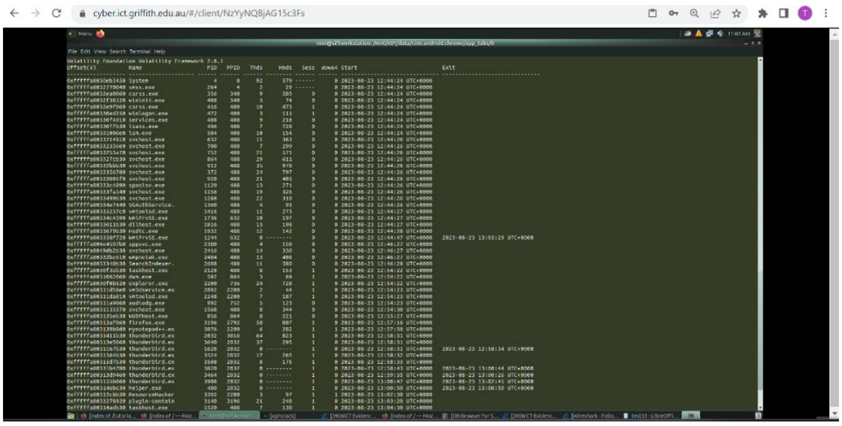
For this piece of evidence I firstly *visited* ***'http://3906ictassignment.griffith.internal/'*** to download the relevant ***"EvidenceD.vnem"*** file and moved it to the ***'cases/MilesBron'*** directory, and unzipped the folder to find a ***'.vnem***' file.

I then did a ***'Md5sum'*** hash of the ***"EvidenceD.vnem"*** file.

Evidence 13

What applications are running on the memory dump computer?

The following command was used ***"$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 pslist"*** to find that Miles has been running the following programs:



cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs

root@siftworkstation: /mnt/e01/data/com.android.chrome/app_tabs/0

```
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8030eb3450 System                    4      0     92      579 ------      0 2023-08-23 12:44:24 UTC+0000
0xfffffa8032770040 smss.exe                264      4      2       29 ------      0 2023-08-23 12:44:24 UTC+0000
0xfffffa8032ea0060 csrss.exe               356    340      9      503      0      0 2023-08-23 12:44:24 UTC+0000
0xfffffa8032f38120 wininit.exe             408    340      3       74      0      0 2023-08-23 12:44:24 UTC+0000
0xfffffa8032e9f060 csrss.exe               416    400     10      473      1      0 2023-08-23 12:44:24 UTC+0000
0xfffffa80330ed250 winlogon.exe            472    400      3      111      1      0 2023-08-23 12:44:24 UTC+0000
0xfffffa80330f4910 services.exe            488    408      9      218      0      0 2023-08-23 12:44:24 UTC+0000
0xfffffa80330ffb30 lsass.exe               496    408      7      728      0      0 2023-08-23 12:44:24 UTC+0000
0xfffffa8033100e0 lsm.exe                  504    408     10      154      0      0 2023-08-23 12:44:24 UTC+0000
0xfffffa8033214910 svchost.exe             632    488     11      363      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa80332336e0 svchost.exe             700    488      7      299      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa8033253a70 svchost.exe             752    488     21      571      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa803327cb30 svchost.exe             864    488     29      611      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa803332bbb30 svchost.exe            912    488     35      978      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa8033356780 svchost.exe             372    488     24      797      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa80333805f0 svchost.exe             920    488     21      401      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa80333c4890 spoolsv.exe            1120    488     13      271      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa80333fa140 svchost.exe            1156    488     19      326      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa8033499b30 svchost.exe            1288    488     22      310      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa80334e7440 VGAuthService.         1360    488      4       93      0      0 2023-08-23 12:44:26 UTC+0000
0xfffffa80335237c0 vmtoolsd.exe           1416    488     11      273      0      0 2023-08-23 12:44:27 UTC+0000
0xfffffa80334c4590 WmiPrvSE.exe           1736    632     10      197      0      0 2023-08-23 12:44:27 UTC+0000
0xfffffa8033611b30 dllhost.exe            1816    488     13      198      0      0 2023-08-23 12:44:27 UTC+0000
0xfffffa8033679b30 msdtc.exe              1932    488     12      142      0      0 2023-08-23 12:44:28 UTC+0000
0xfffffa803358f720 WmiPrvSE.exe           1244    632      0 --------      0      0 2023-08-23 12:44:47 UTC+0000  2023-08-23 13:05:29 UTC+0000
0xfffffa804e4597b0 sppsvc.exe             2300    488      4      150      0      0 2023-08-23 12:46:27 UTC+0000
0xfffffa8049db2b30 svchost.exe            2416    488     14      330      0      0 2023-08-23 12:46:27 UTC+0000
0xfffffa80332be510 wmpnetwk.exe           2484    488     13      408      0      0 2023-08-23 12:46:27 UTC+0000
0xfffffa803340b30 SearchIndexer.          2608    488     11      580      0      0 2023-08-23 12:46:28 UTC+0000
0xfffffa8030f3eb30 taskhost.exe           2128    488      8      153      1      0 2023-08-23 12:54:22 UTC+0000
0xfffffa8031062060 dwm.exe                 592    864      3       69      1      0 2023-08-23 12:54:22 UTC+0000
0xfffffa8030f0b520 explorer.exe           2200    736     24      728      1      0 2023-08-23 12:54:22 UTC+0000
0xfffffa80311d58e0 vm3dservice.ex         2092   2200      2       44      1      0 2023-08-23 12:54:23 UTC+0000
0xfffffa80311da810 vmtoolsd.exe           2248   2200      7      187      1      0 2023-08-23 12:54:23 UTC+0000
0xfffffa80311a9060 audiodg.exe             992    752      5      123      0      0 2023-08-23 12:54:23 UTC+0000
0xfffffa8031133370 svchost.exe            1568    488      8      344      0      0 2023-08-23 12:54:30 UTC+0000
0xfffffa803135eb30 WUDFHost.exe            856    864      8      221      0      0 2023-08-23 12:55:27 UTC+0000
0xfffffa80313af060 firefox.exe            3196   2792     58      887      1      0 2023-08-23 12:57:16 UTC+0000
0xfffffa803139b9d0 mynotepad++.ex         3076   2200      6      282      1      1 2023-08-23 12:57:50 UTC+0000
0xfffffa8031411b30 thunderbird.ex         2032   3016     64      823      1      0 2023-08-23 12:58:31 UTC+0000
0xfffffa80313e50d0 thunderbird.ex         3640   2032     37      295      1      0 2023-08-23 12:58:31 UTC+0000
0xfffffa803116 7b30 thunderbird.ex        1628   2032      0 --------      1      0 2023-08-23 12:58:31 UTC+0000  2023-08-23 12:58:34 UTC+0000
0xfffffa8031564b30 thunderbird.ex         3524   2032     17      265      1      0 2023-08-23 12:58:32 UTC+0000
0xfffffa80315d7b30 thunderbird.ex         3508   2032      8      175      1      0 2023-08-23 12:58:33 UTC+0000
0xfffffa80311b4780 thunderbird.ex         3020   2032      0 --------      1      0 2023-08-23 12:58:43 UTC+0000  2023-08-23 13:00:44 UTC+0000
0xfffffa80313d9460 thunderbird.ex         3464   2032      0 --------      1      0 2023-08-23 12:59:35 UTC+0000  2023-08-23 13:00:26 UTC+0000
0xfffffa803155b060 thunderbird.ex         3988   2032      0 --------      1      0 2023-08-23 13:00:47 UTC+0000  2023-08-23 13:02:45 UTC+0000
0xfffffa803146b630 helper.exe              400   2032      0 --------      1      0 2023-08-23 13:00:50 UTC+0000  2023-08-23 13:00:50 UTC+0000
0xfffffa80312cbb30 ResourceHacker         3392   2200      3       97      1      1 2023-08-23 13:02:30 UTC+0000
0xfffffa8033276920 plugin-contain         3140   3196     21      248      1      0 2023-08-23 13:03:20 UTC+0000
0xfffffa80314adb30 taskhost.exe           1520    488      7      130      1      0 2023-08-23 13:04:30 UTC+0000
```

Evidence 14

What web pages has the memory dump computer visited recently?

To find the recent web pages that were visited, I used the following ***command "$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 firefoxhistory"*** and found the following search history:

"hydrogen energy - Google Search" (oldest)

"Hydrogen Fuel Basics | Department of Energy"

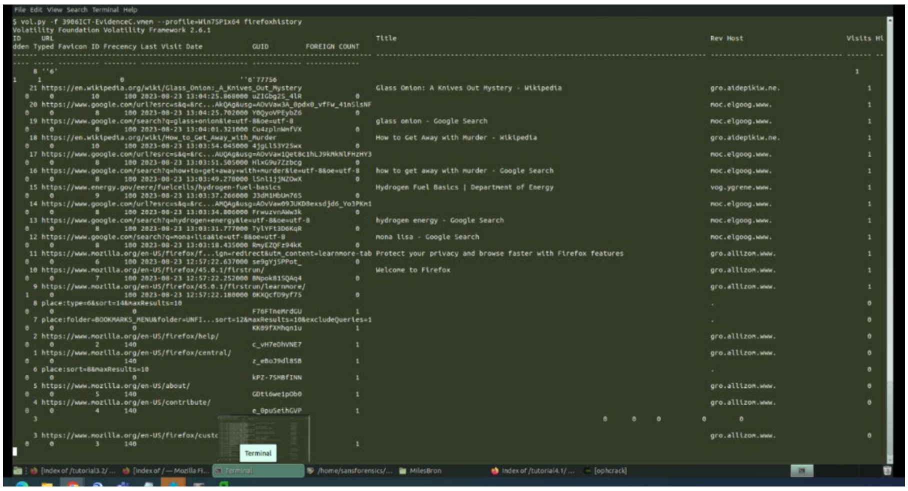
"how to get away with murder - Google Search "

"How to Get Away with Murder - Wikipedia"

"glass onion - Google Search "

" Glass Onion: A Knives Out Mystery - Wikipedia " (Latest)

As you can see, this search history is suspicious and should be taken seriously as it is relevant to the case at hand.



```
$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 firefoxhistory
Volatility Foundation Volatility Framework 2.6.1
ID     URL                                                                  Title                                                                        Rev Host                      Visits Hi
dden Typed Favicon ID Frecency Last Visit Date            GUID          FOREIGN COUNT
------ -------------------------------------------------------------------- ---------------------------------------------------------------------------- ----------------------------- ------ --
---- ----- ---------- -------- -------------------------- ------------ -------------
    8 ''6'                                                                                                                                                                           1
1     1           0                              ''6'77756
   21 https://en.wikipedia.org/wiki/Glass_Onion:_A_Knives_Out_Mystery       Glass Onion: A Knives Out Mystery - Wikipedia                                gro.aidepikiw.ne.                  1
 0     0          10       100 2023-08-23 13:04:25.868000 uZIGbg2S_4lR              0
   20 https://www.google.com/url?esrc=s&q=&rc...AkQAg&usg=AOvVaw3A_0pdx0_vfFw_41nSlsNF                                                                moc.elgoog.www.                    1
 0     0           8       100 2023-08-23 13:04:25.702000 Y0QyoVPEybZ6              0
   19 https://www.google.com/search?q=glass+onion&ie=utf-8&oe=utf-8         glass onion - Google Search                                                  moc.elgoog.www.                    1
 0     0           8       100 2023-08-23 13:04:01.321000 Cu4zplnWmfVX              0
   18 https://en.wikipedia.org/wiki/How_to_Get_Away_with_Murder             How to Get Away with Murder - Wikipedia                                      gro.aidepikiw.ne.                  1
 0     0          10       100 2023-08-23 13:03:54.045000 4jgLl53Y2Swx              0
   17 https://www.google.com/url?esrc=s&q=&rc...AUQAg&usg=AOvVaw1Qet8c1hLJ9kMkNlFHzHY3                                                                moc.elgoog.www.                    1
 0     0           8       100 2023-08-23 13:03:51.505000 HlxG9u7Zzbcg              0
   16 https://www.google.com/search?q=how+to+get+away+with+murder&ie=utf-8&oe=utf-8   how to get away with murder - Google Search                        moc.elgoog.www.                    1
 0     0           8       100 2023-08-23 13:03:49.278000 lSnl1jjNZOwX              0
   15 https://www.energy.gov/eere/fuelcells/hydrogen-fuel-basics            Hydrogen Fuel Basics | Department of Energy                                  vog.ygrene.www.                    1
 0     0           9       100 2023-08-23 13:03:37.266000 J3dM1HbUm76S              0
   14 https://www.google.com/url?esrc=s&q=&rc...AMQAg&usg=AOvVaw09JUKD8exsdjd6_Yo3PKm1                                                                moc.elgoog.www.                    1
 0     0           8       100 2023-08-23 13:03:34.806000 FrwuzvnAWw3k              0
   13 https://www.google.com/search?q=hydrogen+energy&ie=utf-8&oe=utf-8     hydrogen energy - Google Search                                              moc.elgoog.www.                    1
 0     0           8       100 2023-08-23 13:03:31.777000 TylYFt3D6KqR              0
   12 https://www.google.com/search?q=mona+lisa&ie=utf-8&oe=utf-8           mona lisa - Google Search                                                    moc.elgoog.www.                    1
 0     0           8       100 2023-08-23 13:03:18.435000 RmyEZQFz94kK              0
   11 https://www.mozilla.org/en-US/firefox/f...ign=redirect&utm_content=learnmore-tab Protect your privacy and browse faster with Firefox features  gro.allizom.www.                   1
 0     0           6       100 2023-08-23 12:57:22.637000 se9gYj5PPot_              0
   10 https://www.mozilla.org/en-US/firefox/45.0.1/firstrun/                Welcome to Firefox                                                           gro.allizom.www.                   1
 0     0           7       100 2023-08-23 12:57:22.252000 BNpok81SQAq4              0
    9 https://www.mozilla.org/en-US/firefox/45.0.1/firstrun/learnmore/                                                                                   gro.allizom.www.                   1
 1     0                   100 2023-08-23 12:57:22.180000 0KXQcfD9yf75              0
    8 place:type=6&sort=14&maxResults=10                                                                                                                 .                                  0
 0     0           0                                      F76FTneMrdGU              1
    7 place:folder=BOOKMARKS_MENU&folder=UNFI...sort=12&maxResults=10&excludeQueries=1                                                                   .                                  0
 0     0           0                                      KK89fXMhqn1u              1
    2 https://www.mozilla.org/en-US/firefox/help/                                                                                                        gro.allizom.www.                   0
 0     0           2       140                            c_vH7eDhVNE7              1
    1 https://www.mozilla.org/en-US/firefox/central/                                                                                                     gro.allizom.www.                   0
 0     0                   140                            z_eBoJ9dl8SB              1
    6 place:sort=8&maxResults=10                                                                                                                         .                                  0
 0     0           0                                      kPZ-7SMBfINN              1
    5 https://www.mozilla.org/en-US/about/                                                                                                               gro.allizom.www.                   0
 0     0           5       140                            GDti6we1pOb0              1
    4 https://www.mozilla.org/en-US/contribute/                                                                                                          gro.allizom.www.                   0
 0     0           4       140                            e_8puSethGVP              1
    3                                                                                                         0      0     0        0       0

    3 https://www.mozilla.org/en-US/firefox/custc                                                                                                        gro.allizom.www.                   0
 0     0           3       140                                                      1
```

File Edit View Search Terminal Help
Terminal
[index of /tutorial3.2/ ...
[index of / — Mozilla Fi...
Terminal
/home/sansforensics/...
MilesBron
Index of /tutorial4.1/ ...
[ophcrack]

Evidence 15

What is email address of the owner of the memory dump computer?

The email address of the owner of the PC is believed to be "ht317117@gmail.com” from the evidence that I have found in relation to this address.

In order to come to this conclusion I used the following command to list evidence against this address to see what it was possibly involved in.

The first step was to search ***using "$ strings 3906ICT-EvidenceC.vmem | grep username"***, however nothing came up with this search query, so I changed "username" to "mail" and then "yahoo" and lastly gmail", I found something with "@gmail". It was an address that seemed to appear a lot. I then did a search for the address ht317117@gmail.com and it showed contact with a "Dirk Gently" which was associated with demodan87@gmail.com.

Evidence 16

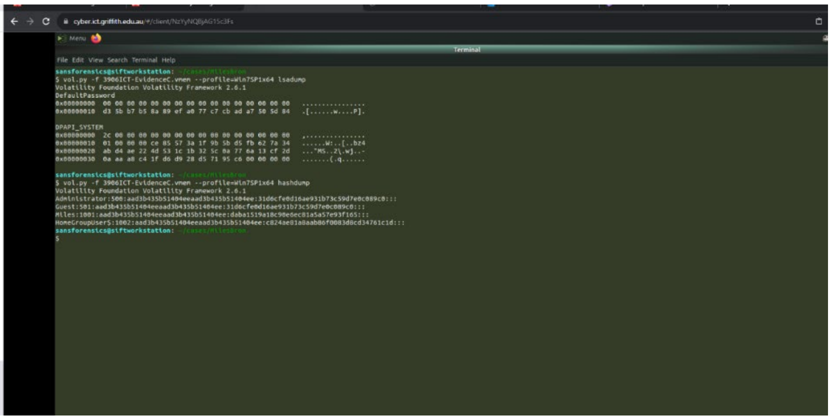
What is password of the memory dump computer?

Using ***"$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 hashdump"*** I uncovered the following password hashes:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Miles:1001:aad3b435b51404eeaad3b435b51404ee:daba1519a18c90e6ec81a5a57e93f165:::

HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:c824ae81a8aab86f0083d8cd34761c1d:::
```

The above are four password hashes for different user accounts for the windows xp computer.

The next step was to use "ophcrack" to crack the password hashes, however I could not do so as there were no "tables" loaded or installed to use with "ophcrack", I attempted downloading some, however there is no internet enabled on the virtual machine, I also attempted to use hashcat or another password cracking tool but unfortunately "ophcrack" is the only one installed, and with no tables to use.



cyber.ict.griffith.edu.au/#/client/NzYyNQBjAG15c3Fs
Menu
Terminal
File Edit View Search Terminal Help

```
sansforensics@siftworkstation: ~/cases/MilesBron
$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
DefaultPassword
0x00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00000010  d3 5b b7 b5 8a 89 ef a0 77 c7 cb ad a7 50 5d 84   .[......w....P].

DPAPI_SYSTEM
0x00000000  2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ,...............
0x00000010  01 00 00 00 ce 85 57 3a 1f 9b 5b d5 fb 62 7a 34   ......W:..[..bz4
0x00000020  ab d4 ae 22 4d 53 1c 1b 32 5c 0a 77 6a 13 cf 2d   ..."MS..2\.wj..-
0x00000030  0a aa a8 c4 1f d6 d9 28 d5 71 95 c6 00 00 00 00   .......(.q......

sansforensics@siftworkstation: ~/cases/MilesBron
$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Miles:1001:aad3b435b51404eeaad3b435b51404ee:daba1519a18c90e6ec81a5a57e93f165:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:c824ae81a8aab86f0083d8cd34761c1d:::
sansforensics@siftworkstation: ~/cases/MilesBron
$
```

Additional Questions

17. Conduct a timeline analysis of the pieces of evidence.

18. Provide a brief final analysis of the evidence and your conclusions.

The investigation into the ‘Miles Bron’ case has been successful, we have retrieved data from a multitude of devices from the suspect that tie’s Miles to the murder of ‘Duke Cody’ a youtuber who attended the party of ‘Benoit Blanc’. After careful steps to ensure the integrity of the data is kept un-damaged, we can see that the evidence collected shows ‘Miles Bron’ in communications with certain involved parties who are tied directly to the case. Messages/calls from the phone, data from the packets and search history from the ‘.vnem’ file off of ‘Mile Bron’s’ computer.

19. Provide advice to Benoit about the identification and collection methods for each specific evidence item.

The advice we have for ‘Benoit’ regarding the identification and collection methods for each specific item, are instructed below.

Evidence A review:

In the ‘Evidence A’ file, we had a disk image of an old desktop computer found in Andi Brand’s villa on the estate. This disk image contained important information about the owner of the desktop, programs that have been installed on the desktop, recent programs that have been run, and suspicious files in the recycle bin. More specific information on each of these items are as follows:

Owner of the desktop

The identification for this item was by using the following command to identify the owner of the desktop, for this to work correctly, the data file had to firstly be mounted into the

‘*/mnt/windows_mount/*’ directory and then use the rip.pl command to search for the windows version of the machine.

'rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/software -p winver'

Programs that have been installed on the desktop

This was found by firstly mounting the evidence onto ***‘/mnt/windows_mount/’*** and going into the correct file ***location ‘/mnt/windows_mount/Documents_and_Settings/All_Users/Desktop'*** which displayed a few suspicious files.

Recent programs that have been run

The recent programs that were run on the machine were identified by using the following command to find a detailed match for what I was searching for.

"rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/system -p appcompatcache | grep .exe"

This command searches within the ***‘/system32/config/system’*** location with the “appcompatcache” as the defining factor and lastly narrowing the search even more with ***“grep .exe”*** to specifically find data that ends with a ***“.exe”*** extension.

Files within the recycling bin

The last piece of evidence that was located in ***“Evidence A”*** was the data found in the recycling bin of the computer, which had a couple interesting file names. These were located in the following directory and could be accessed after mounting the data file to ***‘/mnt/windows_mount’.***

'/mnt/windows_mount/RECYCLER/S-1-5-21-343818398-1563985344-725345543-1003'

Evidence B review:

The evidence collected was in relation to the network capture of Miles Bron's estate network which provided evidence that Miles was indeed in contact with other people, as well as sharing a package across an FTP server, the communications between other members on the island prove that there were indeed some fishy activity going on, and it may require further analysis to find out how much “Miles Bron” has to do with these events. The data was found using an application called ‘Wireshark’, a well-known packet forensic application used to investigate data packets sent across the network.

Evidence C review:

The evidence collected in this section was in relation to a disk image of a damaged mobile phone found near Duke Cody. The first item of evidence was the non-stock applications currently installed on the phone, this was identified after mounting the dm-0 data file into ***‘/mnt/e01’*** and went into this location and chose the ‘app’ directory, this is where the apps were listed.

The second piece of evidence identified were the contact list, and messages/calls sent and received by the phone. This was located at **'/mnt/e01/data/com.android.providers.contacts/databases'**, where I copied the ***‘contacts2.db’*** file to the ***‘cases/MilesBron’*** directory and then opened in ‘DB Browser for SQLite' to search within *the* ***‘contacts2.db’*** file, where I located the contacts and recent phone calls. The messages were located within the

‘/mnt/e01/user_de/0/com.android.providers.telephony/databases’ directory, the file was named ‘mmssms’, this file held the recent messages received from the device, which proved to be very helpful in terms of evidence.

The third piece of evidence for ‘Evidence C’ is in relation to the internet searches that were done on the phone.

The fourth piece of evidence shows the email that was used.

Evidence D review:

The evidence collected within this data file was in relation to a memory dump of a personal laptop found in the remains of the estate fire. This memory dump provided us with crucial evidence that may tie ‘Miles Bron’ to the case. We were able to discover what applications were running on the memory dump computer by using ***the “vol.py”*** command ***("$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 pslist")***, which is a part of the sleuth kit, and used to find specific information, in this case, it being the applications that were running.

The second piece of evidence collected was the recently searched items on the clients ‘Firefox’ browser, this was identified by using **"$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 firefoxhistory"** command, this command also uses the vol.py option to do a precise search within the. vnem data file for anything with “firefoxhistory” attached.

The third piece of evidence we found within the .vnem file was the email address of the owner of the machine, this was identified by using **"$ strings 3906ICT-EvidenceC.vmem | grep gmail"** command, this command does a search for items listed with “@gmail”.

The fourth item of evidence was the password for the memory dump computer, this item of evidence was identified using **"$ vol.py -f 3906ICT-EvidenceC.vmem --profile=Win7SP1x64 hashdump",** which does a search for hashdumps of user profiles within the machine.