

Evidence C – A memory dump of a personal laptop found in Alex's bedroom.

Tool used: vol.py and rip.pl

First, I unzip the file and check md5sum.

```
sansforensics@siftworkstation: ~/Desktop/cases Apps-Poster.pdf Poster.pdf
$ unzip EvidenceC.zip
Archive: EvidenceC.zip
  inflating: EvidenceC.vmem
sansforensics@siftworkstation: ~/Desktop/cases
$ ls
Bob evidenceA EvidenceB.pcap EvidenceB.zip EvidenceC.vmem EvidenceC.zip
sansforensics@siftworkstation: ~/Desktop/cases
$ md5sum EvidenceC.vmem
610278c68947d89a587ea64987af5b85 EvidenceC.vmem
sansforensics@siftworkstation: ~/Desktop/cases
$
```

Determine the profile of the memory dump by using the imageinfo, profile, and hivelist command:

```
sansforensics@siftworkstation: ~/Desktop/cases
$ vol.py -f EvidenceC.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418
          AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
          AS Layer2 : FileAddressSpace (/cases/EvidenceC.vmem)
          caPAE type : NoPAEo-Unix-   iOS-3rd-Party-   SIFT-REMnux-
          DBT : 0x18760001df Apps-Poster.pdf Poster.pdf
          KDBG : 0xf800029f40a0L

          Number of Processors : 1
          Image Type (Service Pack) : 1
          KPCR for CPU 0 : 0xfffffff800029f5d00L
          KUSER_SHARED_DATA : 0xffffffff8000000000L
          Image date and time : 2024-09-08-12:26:34 UTC+0000
          Image local date and time : 2024-09-08 22:26:34 +1000
sansforensics@siftworkstation: ~/Desktop/cases
$ vol.py -f EvidenceC.vmem --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6.1
Virtual      Physical      Name
0xffffffff8a00000f010 0x00000000a96e4010 [no name]
0xffffffff8a000024010 0x00000000a972f010 \REGISTRY\MACHINE\SYSTEM
0xffffffff8a000061010 0x00000000a96ee010 \REGISTRY\MACHINE\HARDWARE
0xffffffff8a000b80410 0x00000000a6fd410 \Device\Harddisk\Volume1\Boot\BCD
0xffffffff8a000b98010 0x00000000a6520010 \SystemRoot\System32\Config\SOFTWARE
0xffffffff8a000dd7010 0x000000009ddbd010 \SystemRoot\System32\Config\SECURITY
0xffffffff8a000e43010 0x000000009d738010 \SystemRoot\System32\Config\SAM
0xffffffff8a000f5c410 0x000000009de6410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xffffffff8a000f62010 0x000000009d36c010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xffffffff8a0011ea010 0x0000000098c1d010 \??\C:\Users\Sophia Bennett\ntuser.dat
0xffffffff8a0013d4010 0x0000000095148010 \??\C:\Users\Sophia Bennett\AppData\Local\Microsoft\Windows\UsrClas.dat
0xffffffff8a001bf0370 0x000000007b1a9370 \??\C:\System Volume Information\Syscache.hve
0xffffffff8a0061af010 0x00000000a091c010 \SystemRoot\System32\Config\DEFAULT
sansforensics@siftworkstation: ~/Desktop/cases
$
```

What applications are running on the memory dump computer?

I run the following command to list processes running in the memory dump “vol.py -f EvidenceC.vmem --profile=Win7SP1x64 pslist” as show in below screenshot.

Windows Task Manager - Applications									
	Name	PID	PPID	Thds	Hnds	Sess	Wond4	Start	Exit
0xffffffffa8030eb2890	System	0	89	577	0	0	0	2024-09-08 07:08:05 UTC+0000	
0xffffffffa803251000	cases.exe	240	316	9	512	0	0	2024-09-08 07:08:11 UTC+0000	
0xffffffffa803ebd000	crss.exe	374	316	11	703	891	SUS-REMn	2024-09-08 07:08:11 UTC+0000	
0xffffffffa80324e1000	cases	376	368	1	0	0	0	2024-09-08 07:08:12 UTC+0000	
0xffffffffa80324e1000	wlinit.exe	384	316	3	111	1	0	2024-09-08 07:08:12 UTC+0000	
0xffffffffa803250b00	winlogon.exe	420	368	6	215	0	0	2024-09-08 07:08:13 UTC+0000	
0xffffffffa803252b00	services.exe	480	384	7	152	0	0	2024-09-08 07:08:13 UTC+0000	
0xffffffffa803254700	taskhost.exe	496	384	9	146	0	0	2024-09-08 07:08:14 UTC+0000	
0xffffffffa803260b30	svchost.exe	588	480	10	385	0	0	2024-09-08 07:08:20 UTC+0000	
0xffffffffa803262000	vndservice.exe	648	480	3	Window-43	0	0	2024-09-08 07:08:21 UTC+0000	
0xffffffffa803263700	svchost.exe	688	480	7	339	0	0	2024-09-08 07:08:21 UTC+0000	
0xffffffffa803263700	svchost.exe	700	480	2	388	0	0	2024-09-08 07:08:22 UTC+0000	
0xffffffffa8032638470	svchost.exe	816	480	23	469	0	0	2024-09-08 07:08:22 UTC+0000	
0xffffffffa8032692b30	svchost.exe	840	480	29	917	0	0	2024-09-08 07:08:22 UTC+0000	
0xffffffffa80326e7800	svchost.exe	992	480	18	773	0	0	2024-09-08 07:08:23 UTC+0000	
0xffffffffa803270e30	svchost.exe	328	480	19	495	0	0	2024-09-08 07:08:24 UTC+0000	
0xffffffffa803276960	spoils.exe	1632	480	13	272	0	0	2024-09-08 07:08:25 UTC+0000	
0xffffffffa803276960	spoils.exe	400	480	1	1	0	0	2024-09-08 07:08:27 UTC+0000	
0xffffffffa803276960	spoils.exe	1249	480	3	84	0	0	2024-09-08 07:08:27 UTC+0000	
0xffffffffa803276960	VAuthService	1384	480	9	195	1	0	2024-09-08 07:08:28 UTC+0000	
0xffffffffa80328d760c	taskhost.exe	1404	816	5	126	1	0	2024-09-08 07:08:28 UTC+0000	
0xffffffffa803291290	dwm.exe	1504	1456	21	962	1	0	2024-09-08 07:08:29 UTC+0000	
0xffffffffa803291290	explorer.exe	1580	480	11	272	0	0	2024-09-08 07:08:30 UTC+0000	
0xffffffffa8032925860	dhcpcsvc.exe	1876	480	13	159	0	0	2024-09-08 07:08:30 UTC+0000	
0xffffffffa8032a0b30	msdtc.exe	872	480	12	144	0	0	2024-09-08 07:08:34 UTC+0000	
0xffffffffa8032a2b800	vndservice.exe	1932	1504	2	53	1	0	2024-09-08 07:08:36 UTC+0000	
0xffffffffa8032b2a000	vtmtools.exe	2080	1504	214	1	0	0	2024-09-08 07:08:36 UTC+0000	
0xffffffffa8032b4030	vm3dservice.ex	2136	588	18	269	0	0	2024-09-08 07:08:37 UTC+0000	
0xffffffffa8032b4030	GeolocationService	2336	400	14	662	0	0	2024-09-08 07:08:37 UTC+0000	
0xffffffffa8032c6030	wpnnetwk.exe	2444	480	13	397	0	0	2024-09-08 07:08:43 UTC+0000	
0xffffffffa8032c9b30	svchost.exe	2556	480	21	333	0	0	2024-09-08 07:08:44 UTC+0000	
0xffffffffa8032d42000	svchost.exe	2780	480	9	364	0	0	2024-09-08 07:08:45 UTC+0000	
0xffffffffa803172d000	sppsvc.exe	2868	480	4	151	0	0	2024-09-08 07:08:45 UTC+0000	
0xffffffffa803172d000	sppsvc.exe	3180	480	33	320	0	0	2024-09-08 07:08:45 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	3512	3512	81	1838	1	0	2024-09-08 07:08:45 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	3748	3512	20	364	1	0	2024-09-08 08:00:31 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	3800	3512	1	148	1	0	2024-09-08 08:00:31 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	4080	3512	17	231	0	0	2024-09-08 08:00:32 UTC+0000	
0xffffffffa8031eeb730	firefox.exe	3088	3512	18	Window-239	0	0	2024-09-08 08:00:35 UTC+0000	
0xffffffffa8031eeb730	firefox.exe	4420	3512	245	1	0	0	2024-09-08 08:00:35 UTC+0000	
0xffffffffa8032ba0400	firefox.exe	4576	3512	8	164	1	0	2024-09-08 08:00:36 UTC+0000	
0xffffffffa803299aa060	taskhost.exe	5036	480	6	219	1	0	2024-09-08 08:03:37 UTC+0000	
0xffffffffa8031872510	thunderbird.exe	1892	4672	63	906	1	0	2024-09-08 12:02:41 UTC+0000	
0xffffffffa8031872510	thunderbird.exe	3412	1892	21	261	1	0	2024-09-08 12:02:42 UTC+0000	
0xffffffffa8032bcc30	thunderbird.exe	4476	1892	7	163	1	0	2024-09-08 12:02:46 UTC+0000	
0xffffffffa8031f0e06	Thunderbird.exe	780	1892	17	163	1	0	2024-09-08 12:02:50 UTC+0000	
0xffffffffa8031b1f30	thunderbird.exe	4988	1892	18	232	1	0	2024-09-08 12:02:58 UTC+0000	
0xffffffffa8031f4b30	thunderbird.exe	3268	1892	7	155	1	0	2024-09-08 12:10:21 UTC+0000	
0xffffffffa8031bbe30	helper.exe	4644	1892	0	-----	1	0	2024-09-08 12:11:01 UTC+0000	
0xffffffffa8031f0e06	mynotepad++.ex	4360	1504	5	247	1	1	2024-09-08 12:15:06 UTC+0000	
0xffffffffa8031b3b780	dhilst.exe	4332	588	8	249	1	0	2024-09-08 12:16:17 UTC+0000	
0xffffffffa8032b25060	firefox.exe	4040	3512	21	251	1	0	2024-09-08 12:24:41 UTC+0000	
0xffffffffa8031f32060	firefox.exe	2516	3512	22	257	1	0	2024-09-08 12:24:44 UTC+0000	
0xffffffffa803312ab30	firefox.exe	2432	3512	20	243	1	0	2024-09-08 12:24:57 UTC+0000	
0xffffffffa8033145b30	firefox.exe	2712	3512	20	245	1	0	2024-09-08 12:25:02 UTC+0000	
0xffffffffa803311fb30	firefox.exe	4256	3512	22	255	1	0	2024-09-08 12:25:15 UTC+0000	
0xffffffffa8032ad7060	firefox.exe	1724	3512	22	251	1	0	2024-09-08 12:25:31 UTC+0000	
0xffffffffa8032b089d0	firefox.exe	4108	3512	20	244	1	0	2024-09-08 12:25:31 UTC+0000	
0xffffffffa8031b3b830	firefox.exe	3436	3512	20	250	1	0	2024-09-08 12:25:42 UTC+0000	
0xffffffffa803321060	firefox.exe	4216	3512	20	247	1	0	2024-09-08 12:25:47 UTC+0000	
0xffffffffa803324f770	firefox.exe	1016	3512	20	249	1	0	2024-09-08 12:25:50 UTC+0000	
0xffffffffa8033309860	firefox.exe	1752	3512	20	247	1	0	2024-09-08 12:25:56 UTC+0000	
0xffffffffa80332b2530	firefox.exe	3024	3512	17	235	1	0	2024-09-08 12:25:58 UTC+0000	
0xffffffffa80332d4b30	firefox.exe	4176	3512	17	235	1	0	2024-09-08 12:26:01 UTC+0000	
0xffffffffa803326960	firefox.exe	4264	3512	17	235	1	0	2024-09-08 12:26:01 UTC+0000	

Windows Task Manager - Applications									
	Name	PID	PPID	Thds	Hnds	Sess	Wond4	Start	Exit
0xffffffffa8032a0b30	msdtc.exe	872	480	12	144	0	0	2024-09-08 07:08:34 UTC+0000	
0xffffffffa8032b2a000	vn3dservice.ex	1532	1504	2	Immers	53	1	0	2024-09-08 07:08:36 UTC+0000
0xffffffffa8032b4b30	vntools.exe	2000	1504	214	1	DPIR	Smartphone-1	2024-09-08 07:08:37 UTC+0000	
0xffffffffa8032b4b30	WniPrvSE.exe	2108	588	14	662	0	0	2024-09-08 07:08:37 UTC+0000	
0xffffffffa8032c3b30	SearchIndexer	2336	480	14	662	0	0	2024-09-08 07:08:42 UTC+0000	
0xffffffffa8032c9b30	wpnnetwk.exe	2444	480	13	397	0	0	2024-09-08 07:08:43 UTC+0000	
0xffffffffa8032d42000	svchost.exe	2556	480	21	333	0	0	2024-09-08 07:08:44 UTC+0000	
0xffffffffa803172d000	wlinit.exe	2780	480	9	364	0	0	2024-09-08 07:08:45 UTC+0000	
0xffffffffa803172d000	sppsvc.exe	2868	480	4	151	0	0	2024-09-08 07:08:45 UTC+0000	
0xffffffffa803172d000	sppsvc.exe	3180	480	33	320	0	0	2024-09-08 07:08:45 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	3512	3512	81	1838	1	0	2024-09-08 08:00:31 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	3748	3512	26	364	1	0	2024-09-08 08:00:31 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	3800	3512	6	148	1	0	2024-09-08 08:00:31 UTC+0000	
0xffffffffa8031c9b30	firefox.exe	4080	3512	17	231	1	0	2024-09-08 08:00:32 UTC+0000	
0xffffffffa8031eeb730	firefox.exe	3088	3512	18	Window-239	0	0	2024-09-08 08:00:35 UTC+0000	
0xffffffffa8031eeb730	firefox.exe	4420	3512	20	205	1	0	2024-09-08 08:01:47 UTC+0000	
0xffffffffa8032ba0400	firefox.exe	4576	3512	8	164	1	0	2024-09-08 08:01:48 UTC+0000	
0xffffffffa803299aa060	taskhost.exe	5036	480	6	219	1	0	2024-09-08 08:03:37 UTC+0000	
0xffffffffa8031872510	thunderbird.exe	1892	4672	63	906	1	0	2024-09-08 12:02:41 UTC+0000	
0xffffffffa8031872510	thunderbird.exe	3412	1892	21	261	1	0	2024-09-08 12:02:42 UTC+0000	
0xffffffffa8032bcc30	thunderbird.exe	4476	1892	7	163	1	0	2024-09-08 12:02:46 UTC+0000	
0xffffffffa8031f0e06	Thunderbird.exe	780	1892	17	163	1	0	2024-09-08 12:02:50 UTC+0000	
0xffffffffa8031b1f30	thunderbird.exe	4988	1892	18	232	1	0	2024-09-08 12:02:58 UTC+0000	
0xffffffffa8031f4b30	thunderbird.exe	3268	1892	7	155	1	0	2024-09-08 12:10:21 UTC+0000	
0xffffffffa8031bbe30	helper.exe	4644	1892	0	-----	1	0	2024-09-08 12:11:01 UTC+0000	
0xffffffffa8031f0e06	mynotepad++.ex	4360	1504	5	247	1	1	2024-09-08 12:15:06 UTC+0000	
0xffffffffa8031b3b780	dhilst.exe	4332	588	8	249	1	0	2024-09-08 12:16:17 UTC+0000	
0xffffffffa8032b25060	firefox.exe	4040	3512	21	251	1	0	2024-09-08 12:24:41 UTC+0000	
0xffffffffa8031f32060	firefox.exe	2516	3512	22	257	1	0	2024-09-08 12:24:44 UTC+0000	
0xffffffffa803312ab30	firefox.exe	2432	3512	20	243	1	0	2024-09-08 12:24:57 UTC+0000	
0xffffffffa8033145b30	firefox.exe	27							

Here is the screenshot showing the results:

What is email address of the owner of the memory dump computer and how are they connected to the case?

I used the command “strings EvidenceC.vmem | grep -i '@gmail.com'” to extract email addresses from the memory dump. The owner of the memory dump computer appears to be Sophia Bennett, as her email address, vb9945311@gmail.com, is repeatedly referenced in the email exchanges.

Message-ID: <de075ca0-905a-447a-aeb0-277965ddefe@gmail.com>
To: sr8640171@gmail.com
From: Sophia Bennett <vb994531@gmail.com>
 Jason Garrett - Glaser <darkshktkar@gmail.com>
From: Alex Marshall <sr8640171@gmail.com>
To: vb994531@gmail.com
-1725796979, https://accounts.google.com/v3/signIn/identifier?app_domain=http://localhost&client_id=406904057835-aq8lmtabj95dh1la2bvharmfk3t1hgqj.apps.googleusercontent.com&cor
auth/legacy/consent#&utmknow...partx3DAl1ahUmkd4XOU1zimEMNzU0UgPjwTRn7g8p8cExIbhKlnyGIClGhVlgxH2Tlwbp140h-99Zjwgh_x60moh9Y05BCPyv4rul8_Ct4t2Q5L
SPWhuempEWZhRhpR8Dp0Rkrksx1a_10t56P0CpNyKgTsaGHSy_miyXqcw5x42JWxmXA0B0k620DESe_EyexacHeJl07k1estlybvqkVQKov5f5xZxyR8bzIxKhQn38ycx17IBG_Eso0v5s07y_zJWLGR80vPGdP-GaykpoD7
35-aq8lmtabj95dh1la2bvharmfk3t1hgqj.apps.googleusercontent.com%23&domain=0&dsid=5-149152299-17257970194398638flowName=GeneralOAuthFlow2as%3DS-149195299%253A17257
tUGGdNkgQ5h1Q0lp5fgy1zE169QL-1720-uusy1Dy-sql_shZB0u3k1HEHS1z-Y8fpfjj_dnCfUM9bahDNowo4lrAy&redirrect_url=http://localhost&response_type=code&scope=https://mail.google.com
Return-Path: <vb994531@gmail.com>
 for <sr8640171@gmail.com>
Message-ID: <3971a057-5f43-ad53-ae04-f62bd82140d2@gmail.com>
To: sr8640171@gmail.com
From: Sophia Bennett <vb994531@gmail.com>
Return-Path: <vb994531@gmail.com>
 for <sr8640171@gmail.com>
 Copyright (c) 2006 Maxim Yegorushkin &maxim.yegorushkin@gmail.com>
sr8640171@gmail.com
vb994531@gmail.com
sr8640171@gmail.com
Sent Mail - vb994531@gmail.com
 Written by Harutyan Amirjanyan, (amirjanyan@gmail.com)
user_pref("mail.identity.id1.usernickname", "vb994531@gmail.com");
user_pref("mail.server.serverName", "vb994531@gmail.com");
user_pref("mail.server.serverUser", "vb994531@gmail.com");
Copyright (C) 2012 by Marlijn Haverbeke &marljnh@gmail.com>
sansforensics@workstation: /cases

What is password of the memory dump computer?

I used the command “vol.py -f EvidenceC.vmem --profile=Win7SP1x64 lsadump” to extract user account information from the memory dump, and the password obtained is “Alexisbeautiful”

```
sansforensics@siftworkstation: /cases Cheatsheet.pdf Tools-Poster.pdf Smartphone-F...
$ vol.py -f EvidenceC.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
DefaultPassword
0x00000000 1e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x00000010 41 00 6c 00 65 00 78 00 69 00 73 00 62 00 65 00 A..lex..is..be.
0x00000020 61 00 75 00 74 00 69 00 66 00 75 00 6c 00 00 00 OS-S...SETREMux-
Unix-Cheatshe... Apps-Poster.pdf Poster.pdf
DPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ,.....
0x00000010 01 00 00 00 f1 df 54 0f a8 3d 4d df e1 68 87 7b .....T..=M..h..I..
0x00000020 90 0a 0f 1b ee b0 ae 61 29 f9 b3 8b 25 49 e3 f9 .....a)..%!..
0x00000030 bd 9c 0d ec df c0 bc e0 c0 30 9c 8e 00 00 00 00 .....0.....
mount_points SIFT-Cheatsheet.pdf Windows-... Network-...
sansforensics@siftworkstation: /cases pdf Forensics-Post... Forensics-Post...

```