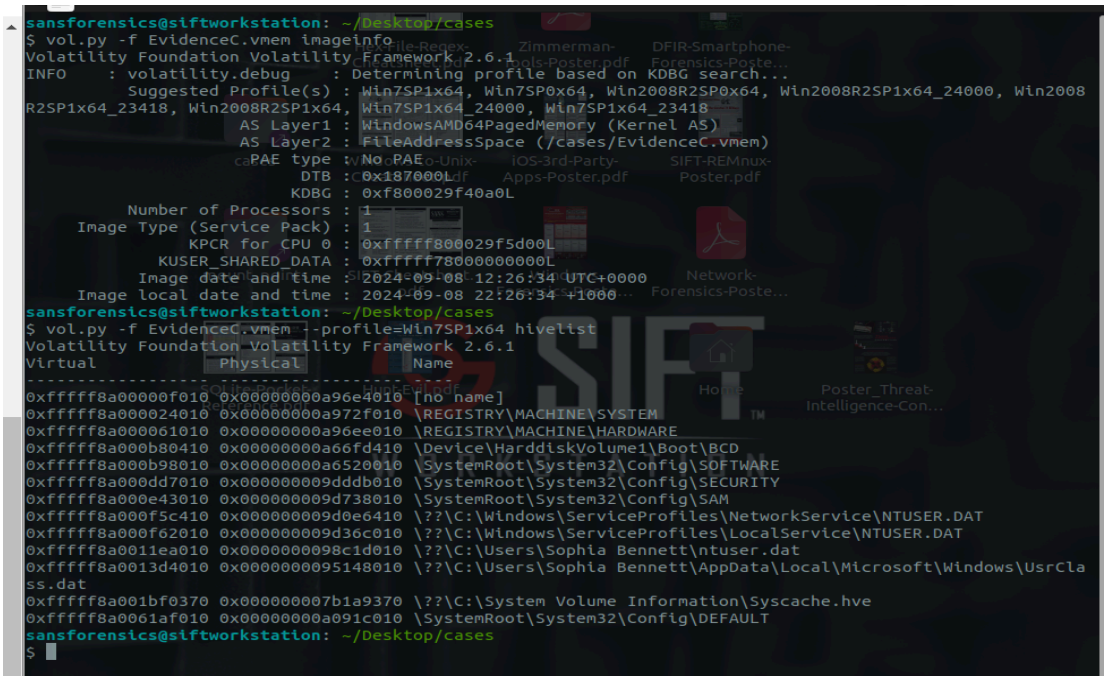
Evidence C – A memory dump of a personal laptop found in Alex's bedroom.

Tool used: vol.py and rip.pl

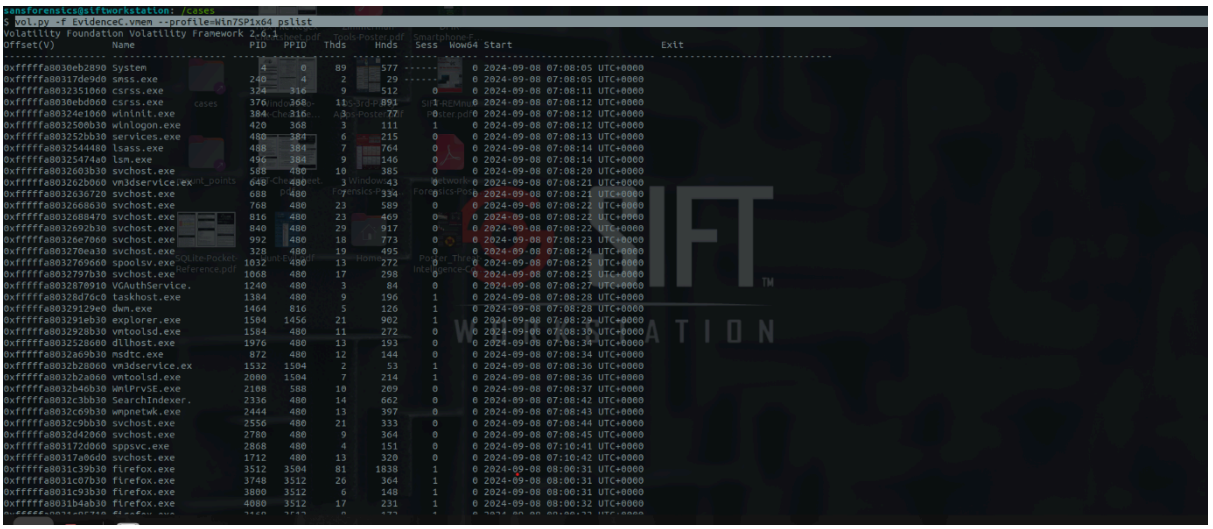
First, I unzip the file and check md5sum.

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



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.



```
sansforensics@siftworkstation: /cases
$ vol.py -f EvidenceC.vmem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8030eb2890 System                    4      0     89      577 ------      0 2024-09-08 07:08:05 UTC+0000
0xfffffa80317de9d0 smss.exe                240      4      2       29 ------      0 2024-09-08 07:08:05 UTC+0000
0xfffffa8032351060 csrss.exe               324    316      9      512      0      0 2024-09-08 07:08:11 UTC+0000
0xfffffa8030eb3060 csrss.exe               376    368     11      891      1      0 2024-09-08 07:08:12 UTC+0000
0xfffffa80324e1060 wininit.exe             384    316      3       77      0      0 2024-09-08 07:08:12 UTC+0000
0xfffffa8032500b30 winlogon.exe            420    368      3      111      1      0 2024-09-08 07:08:12 UTC+0000
0xfffffa8032520b30 services.exe            480    384      6      215      0      0 2024-09-08 07:08:13 UTC+0000
0xfffffa8032544480 lsass.exe               488    384      7      764      0      0 2024-09-08 07:08:14 UTC+0000
0xfffffa80325474a0 lsm.exe                 496    384      9      146      0      0 2024-09-08 07:08:14 UTC+0000
0xfffffa80326030b30 svchost.exe            588    480     10      385      0      0 2024-09-08 07:08:20 UTC+0000
0xfffffa8032620b060 vm3dservice.ex         648    480      3       43      0      0 2024-09-08 07:08:21 UTC+0000
0xfffffa8032636720 svchost.exe             688    480      7      334      0      0 2024-09-08 07:08:21 UTC+0000
0xfffffa8032668630 svchost.exe             768    480     23      589      0      0 2024-09-08 07:08:22 UTC+0000
0xfffffa8032688470 svchost.exe             816    480     23      469      0      0 2024-09-08 07:08:22 UTC+0000
0xfffffa80326920b30 svchost.exe            840    480     29      917      0      0 2024-09-08 07:08:22 UTC+0000
0xfffffa80326e7060 svchost.exe             992    480     18      773      0      0 2024-09-08 07:08:23 UTC+0000
0xfffffa8032700ea30 svchost.exe            328    480     19      495      0      0 2024-09-08 07:08:24 UTC+0000
0xfffffa8032769660 spoolsv.exe            1032    480     13      272      0      0 2024-09-08 07:08:25 UTC+0000
0xfffffa80327970b30 svchost.exe           1068    480     17      298      0      0 2024-09-08 07:08:25 UTC+0000
0xfffffa8032870910 VGAuthService.         1240    480      3       84      0      0 2024-09-08 07:08:27 UTC+0000
0xfffffa80328d76c0 taskhost.exe           1384    480      9      196      1      0 2024-09-08 07:08:28 UTC+0000
0xfffffa80329129e0 dwm.exe                1464    816      5      126      1      0 2024-09-08 07:08:28 UTC+0000
0xfffffa8032910b30 explorer.exe           1504   1456     21      902      1      0 2024-09-08 07:08:29 UTC+0000
0xfffffa80329280b30 vmtoolsd.exe          1584    480     11      272      0      0 2024-09-08 07:08:30 UTC+0000
0xfffffa8032528600 dllhost.exe            1976    480     13      193      0      0 2024-09-08 07:08:34 UTC+0000
0xfffffa8032a69b30 msdtc.exe               872    480     12      144      0      0 2024-09-08 07:08:34 UTC+0000
0xfffffa8032b28060 vm3dservice.ex         1532   1504      2       53      1      0 2024-09-08 07:08:36 UTC+0000
0xfffffa8032b2a060 vmtoolsd.exe           2000   1504      7      214      1      0 2024-09-08 07:08:36 UTC+0000
0xfffffa8032b46b30 WmiPrvSE.exe           2108    588     10      209      0      0 2024-09-08 07:08:37 UTC+0000
0xfffffa8032c3bb30 SearchIndexer.         2336    480     14      662      0      0 2024-09-08 07:08:42 UTC+0000
0xfffffa8032c69b30 wmpnetwk.exe           2444    480     13      397      0      0 2024-09-08 07:08:43 UTC+0000
0xfffffa8032c9bb30 svchost.exe            2556    480     21      333      0      0 2024-09-08 07:08:44 UTC+0000
0xfffffa8032d42060 svchost.exe            2780    480      9      364      0      0 2024-09-08 07:08:45 UTC+0000
0xfffffa803172d060 sppsvc.exe             2868    480      4      151      0      0 2024-09-08 07:10:41 UTC+0000
0xfffffa80317a06d0 svchost.exe            1712    480     13      320      0      0 2024-09-08 07:10:42 UTC+0000
0xfffffa8031c39b30 firefox.exe            3512   3504     81     1838      1      0 2024-09-08 08:00:31 UTC+0000
0xfffffa8031c07b30 firefox.exe            3748   3512     26      364      1      0 2024-09-08 08:00:31 UTC+0000
0xfffffa8031c93b30 firefox.exe            3800   3512      6      148      1      0 2024-09-08 08:00:31 UTC+0000
0xfffffa8031b4ab30 firefox.exe            4080   3512     17      231      1      0 2024-09-08 08:00:32 UTC+0000
0xfffffa8031c85710 firefox.exe            3168   3512      8      172      1      0 2024-09-08 08:00:32 UTC+0000
0xfffffa8031ee7b30 firefox.exe            3088   3512     18      239      1      0 2024-09-08 08:00:35 UTC+0000
0xfffffa8032b3a060 firefox.exe            4420   3512     20      245      1      0 2024-09-08 08:01:47 UTC+0000
0xfffffa8032ba4060 firefox.exe            4576   3512      8      164      1      0 2024-09-08 08:01:48 UTC+0000
0xfffffa803299a060 taskhost.exe           5036    480      6      219      1      0 2024-09-08 08:03:37 UTC+0000
0xfffffa8031872510 thunderbird.ex         1892   4672     63      906      1      0 2024-09-08 12:02:41 UTC+0000
0xfffffa8031eecb30 thunderbird.ex         3412   1892     21      261      1      0 2024-09-08 12:02:42 UTC+0000
0xfffffa8032bccb30 thunderbird.ex         4476   1892      7      163      1      0 2024-09-08 12:02:46 UTC+0000
0xfffffa8031f0e060 thunderbird.ex          780   1892     17      228      1      0 2024-09-08 12:02:50 UTC+0000
0xfffffa8031b3fb30 thunderbird.ex         4988   1892     18      232      1      0 2024-09-08 12:02:58 UTC+0000
0xfffffa8031f74b30 thunderbird.ex         3268   1892      7      155      1      0 2024-09-08 12:10:21 UTC+0000
0xfffffa8031bbe630 helper.exe             4644   1892      0 --------      1      0 2024-09-08 12:11:01 UTC+0000   2024-09-08 12:11:01 UTC+0000
0xfffffa8031f619e0 mynotepad++.ex         4360   1504      5      247      1      1 2024-09-08 12:15:06 UTC+0000
0xfffffa8031b3b780 dllhost.exe            4332    588      8      249      1      0 2024-09-08 12:16:17 UTC+0000
0xfffffa8032b25060 firefox.exe            4040   3512     21      251      1      0 2024-09-08 12:24:41 UTC+0000
0xfffffa8031f32060 firefox.exe            2516   3512     22      257      1      0 2024-09-08 12:24:44 UTC+0000
0xfffffa803312ab30 firefox.exe            2432   3512     20      243      1      0 2024-09-08 12:24:57 UTC+0000
0xfffffa8033145b30 firefox.exe            2712   3512     20      245      1      0 2024-09-08 12:25:02 UTC+0000
0xfffffa803311fb30 firefox.exe            4256   3512     22      255      1      0 2024-09-08 12:25:15 UTC+0000
0xfffffa8032ad7060 firefox.exe            1724   3512     22      251      1      0 2024-09-08 12:25:31 UTC+0000
0xfffffa8032b089d0 firefox.exe            4108   3512     20      244      1      0 2024-09-08 12:25:31 UTC+0000
0xfffffa8031f58b30 firefox.exe            3436   3512     20      250      1      0 2024-09-08 12:25:42 UTC+0000
0xfffffa8033210060 firefox.exe            4216   3512     20      247      1      0 2024-09-08 12:25:47 UTC+0000
0xfffffa803324f770 firefox.exe            1016   3512     20      249      1      0 2024-09-08 12:25:50 UTC+0000
0xfffffa8033098060 firefox.exe            1752   3512     20      247      1      0 2024-09-08 12:25:56 UTC+0000
0xfffffa80332b2b30 firefox.exe            3024   3512     17      235      1      0 2024-09-08 12:25:58 UTC+0000
0xfffffa80332d4b30 firefox.exe            4176   3512     17      235      1      0 2024-09-08 12:26:01 UTC+0000
0xfffffa8033266900 firefox.exe            4264   3512     17      235      1      0 2024-09-08 12:26:01 UTC+0000
sansforensics@siftworkstation: /cases
```

What web pages has the memory dump computer visited recently?

From the pslist output, I found that Firefox was used as the browser. I ran the command “strings EvidenceC.vmem | grep firefox | tail -n 200” to get the most recent entries related to Firefox. The output included URLs like:

“https://www.google.com/search?client=firefox-b-e&q=Emergency+therapy+services”

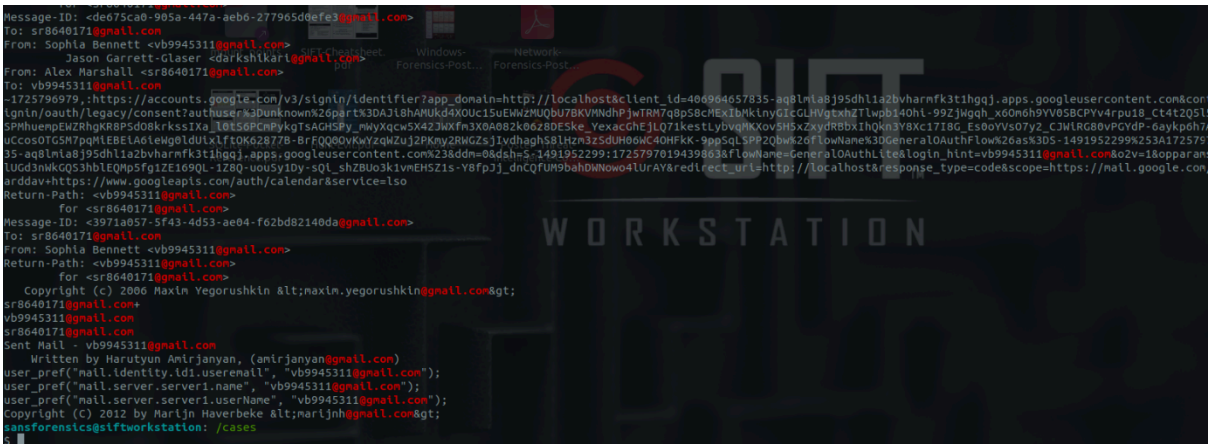
“https://www.google.com/search?client=firefox-b-e&q=Signs+someone+is+cheating”

“https://www.google.com/search?client=firefox-b-e&q=How+to+get+away+with+self-defense”

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.



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”.