RETO 1:

El ordenador de mi hermana se estropeó. Tuvimos mucha suerte de recuperar este volcado de memoria. Tu trabajo es recuperar todos sus archivos importantes del sistema. Por lo que recordamos, de repente vimos aparecer una ventana negra en la que se ejecutaba algo. Cuando ocurrió el accidente, ella estaba intentando dibujar algo. Eso es todo lo que recordamos del momento del colapso.

Bien, una vez descargado el volcado de memoria, vamos a examinar la información de la imagen

Podemos encontrar el perfil sugerido usando el comando:

volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw imageinfo

A partir de aquí tenemos el perfil Win7SP1x64 como el sugerido a utilizar.

volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw — profile=Win7SP1x64 pslist

```
night-wolf@ubuntu:~/MemLabs$ volatility -f MemoryDump_Lab1.raw --profile Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca0040 System                    4      0     80      570 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800148f040 smss.exe                248      4      3       37 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800154f740 csrss.exe               320    312      9      457      0      0 2019-12-11 13:41:32 UTC+0000
0xfffffa8000ca81e0 csrss.exe               368    360      7      199      1      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c45060 psxss.exe               376    248     18      786      0      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c5f060 winlogon.exe            416    360      4      118      1      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c5f630 wininit.exe             424    312      3       75      0      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c98530 services.exe            484    424     13      219      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca0580 lsass.exe               492    424      9      764      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca4b30 lsm.exe                 500    424     11      185      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001cf4b30 svchost.exe             588    484     11      358      0      0 2019-12-11 13:41:39 UTC+0000
0xfffffa8001d327c0 VBoxService.ex          652    484     13      137      0      0 2019-12-11 13:41:40 UTC+0000
0xfffffa8001d49b30 svchost.exe             720    484      8      279      0      0 2019-12-11 13:41:41 UTC+0000
0xfffffa8001d8c420 svchost.exe             816    484     23      569      0      0 2019-12-11 13:41:42 UTC+0000
0xfffffa8001da5b30 svchost.exe             852    484     28      542      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001da96c0 svchost.exe             876    484     32      941      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001e1bb30 svchost.exe             472    484     19      476      0      0 2019-12-11 13:41:47 UTC+0000
0xfffffa8001e50b30 svchost.exe            1044    484     14      366      0      0 2019-12-11 13:41:48 UTC+0000
0xfffffa8001eba230 spoolsv.exe            1208    484     13      282      0      0 2019-12-11 13:41:51 UTC+0000
0xfffffa8001eda060 svchost.exe            1248    484     19      313      0      0 2019-12-11 13:41:52 UTC+0000
0xfffffa8001f58890 svchost.exe            1372    484     22      295      0      0 2019-12-11 13:41:54 UTC+0000
0xfffffa8001f91b30 TCPSVCS.EXE            1416    484      4       97      0      0 2019-12-11 13:41:55 UTC+0000
0xfffffa8000d3c400 sppsvc.exe             1508    484      4      141      0      0 2019-12-11 14:16:06 UTC+0000
0xfffffa8001c38580 svchost.exe             948    484     13      322      0      0 2019-12-11 14:16:07 UTC+0000
0xfffffa8002170630 wmpnetwk.exe           1856    484     16      451      0      0 2019-12-11 14:16:08 UTC+0000
0xfffffa8001d376f0 SearchIndexer.          480    484     14      701      0      0 2019-12-11 14:16:09 UTC+0000
0xfffffa8001eb47f0 taskhost.exe            296    484      8      151      1      0 2019-12-11 14:32:24 UTC+0000
0xfffffa8001dfa910 dwm.exe                1988    852      5       72      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa8002046960 explorer.exe            604   2016     33      927      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa80021c75d0 VBoxTray.exe           1844    604     11      140      1      0 2019-12-11 14:32:35 UTC+0000
0xfffffa80021da060 audiodg.exe            2064    816      6      131      0      0 2019-12-11 14:32:37 UTC+0000
0xfffffa80022199e0 svchost.exe            2368    484      9      365      0      0 2019-12-11 14:32:51 UTC+0000
0xfffffa8002222780 cmd.exe                1984    604      1       21      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa8002227140 conhost.exe            2692    368      2       50      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa80022bab30 mspaint.exe            2424    604      6      128      1      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8000eac770 svchost.exe            2660    484      6      100      0      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8001e68060 csrss.exe              2760   2680      7      172      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000ecbb30 winlogon.exe           2808   2680      4      119      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000f3aab0 taskhost.exe           2908    484      9      158      2      0 2019-12-11 14:37:13 UTC+0000
0xfffffa8000f4db30 dwm.exe                3004    852      5       72      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f4c670 explorer.exe           2504   3000     34      825      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f9a4e0 VBoxTray.exe           2304   2504     14      144      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000fff630 SearchProtocol         2524    480      7      226      2      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8000ecea60 SearchFilterHo         1720    480      5       90      0      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8001010b30 WinRAR.exe             1512   2504      6      207      2      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001020b30 SearchProtocol         2868    480      8      279      0      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001048060 DumpIt.exe              796    604      2       45      1      1 2019-12-11 14:37:54 UTC+0000
0xfffffa800104a780 conhost.exe            2260    368      2       50      1      0 2019-12-11 14:37:54 UTC+0000
```

Podemos ver que mspaint.exe (PID 2424), cmd.exe (PID 1984) y WinRAR.exe (PID 1512) despiertan interés, en parte por la escalada de privilegios y el acceso a la línea de comandos. Dumpit.exe también es bastante sospechoso, pero sin duda es la herramienta que se utilizó para generar el volcado de memoria, por lo que no nos preocupa demasiado. A continuación, inspeccionaremos si alguno de estos procesos está ocultando su existencia a pslist u otros plugins:

volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw — profile=Win7SP1x64 psxview

```
0x000000003ff671e0 csrss.exe               368 True   True   True     True   False True   True
0x000000003f74f740 csrss.exe               320 True   True   True     True   False True   True
0x000000003facd060 DumpIt.exe              796 False  True   False    False  False False  False
0x000000003facf780 conhost.exe            2260 False  True   False    False  False False  False
0x000000003fb54780 conhost.exe            2260 False  True   False    False  False False  False
0x000000003fb2ab30 SearchProtocol         2868 False  True   False    False  False False  False
0x000000003faa5b30 SearchProtocol         2868 False  True   False    False  False False  False
0x000000003fb52060 DumpIt.exe              796 False  True   False    False  False False  False
0x000000003fa95b30 WinRAR.exe             1512 False  True   False    False  False False  False
0x000000003fb1ab30 WinRAR.exe             1512 False  True   False    False  False False  False
```

Curiosamente WinRAR.exe (PID 1512) está oculto en pslist, thrdproc, pspcid, csrss, session y deskthrd.

Mirando el plugin netscan para el tráfico de red utilizando procesos:

volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw — profile=Win7SP1x64 netscan

Vemos, un par de procesos sospechosos aquí:

```
0x3efb0ad0         TCPv4    0.0.0.0:49153                0.0.0.0:0              LISTENING        816      svchost.exe
0x3efb0ad0         TCPv6    :::49153                     :::0                   LISTENING        816      svchost.exe
0x3ecb8cf0         TCPv6    -:0                          4800:ca00:80fa:ffff:4800:ca00:80fa:ffff:0 CLOSED          1        ?J30????
0x3ed4d610         TCPv6    ::1:49163                    ::1:2869               CLOSED           1856     wmpnetwk.exe
0x3eed7820         TCPv4    -:0                          56.155.212.1:0         CLOSED           1        ?J30????
0x3ef5baa0         TCPv6    -:0                          389b:d401:80fa:ffff:389b:d401:80fa:ffff:0 CLOSED          1        ?J30????
0x3ef80cf0         TCPv6    ::1:2869                     ::1:49163              CLOSED           4        System
0x3f63cd70         UDPv4    10.0.2.15:59433              *:*                                     1372     svchost.exe    2019-12-11 14:16:09 UTC+0000
0x3f63dc20         UDPv6    fe80::b137:133f:8d0b:8cfe:1900 *:*                                   1372     svchost.exe    2019-12-11 14:16:09 UTC+0000
0x3f63dec0         UDPv4    127.0.0.1:59434              *:*                                     1372     svchost.exe    2019-12-11 14:16:09 UTC+0000
0x3f794010         TCPv6    -:0                          4800:ca00:80fa:ffff:4800:ca00:80fa:ffff:0 CLOSED          1044     svchost.exe
0x3fcc4b60         UDPv4    0.0.0.0:0                    *:*                                     652      VBoxService.ex 2019-12-11 14:37:57 UTC+0000

C:\Users\DEEP\Documents\volatility_2.6_win64_standalone>
```

wmpnetwk.exe (PID 1856) y ?J3☺???? (PID 1). Vale la pena señalar aquí que Threatminer afirma que 10.0.2.15 está asociado con múltiples muestras de malware, en particular Worms. Teniendo esto en cuenta, merece la pena que vigilemos svchost.exe (PID 1372), sobre todo porque se abusa mucho de él.

A continuación, veremos las consolas:

Volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw — profile=Win7SP1x64 consoles

```
night-wolf@ubuntu:~/MemLabs$ volatility -f MemoryDump_Lab1.raw --profile Win7SP1x64 consoles
Volatility Foundation Volatility Framework 2.6.1
**************************************************
ConsoleProcess: conhost.exe Pid: 2692
Console: 0xff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe - St4G3$1
AttachedProcess: cmd.exe Pid: 1984 Handle: 0x60
----
CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x1de3c0: St4G3$1
----
Screen 0x1e0f70 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\SmartNet>St4G3$1
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=
Press any key to continue . . .
**************************************************
```

¿Y qué tenemos aquí? Parece que el plugin de consolas muestra un comando St4Ge$1 con una salida ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=

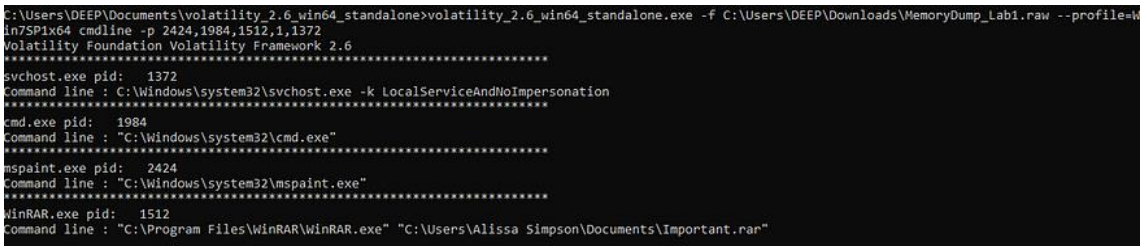
Si decodificamos esto desde base64, obtenemos nuestra primera bandera:

```
$ echo ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0= | base64 -d
flag{th1s_1s_th3_1st_st4g3!!}
```

Flag 1: flag{th1s_1s_th3_1st_st4g3!!}

Bien, si ahora miramos las líneas de comandos de los procesos sospechosos que hemos destacado:

volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw — profile=Win7SP1x64 cmdline -p 2424,1984,1512,1,1372

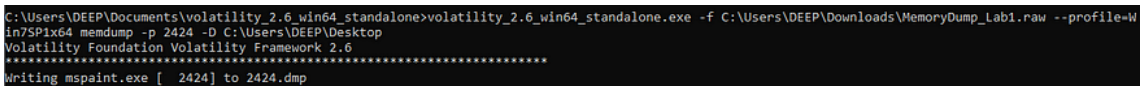


Tenga en cuenta svchost.exe cmdline 'LocalServiceAndNoImpersonation' en realidad está asociado con Windows App Locker y es seguro, aunque parece sospechoso a primera vista. El proceso que sobresale ahora es WinRAR.exe y el archivo C:\Users\Alissa Simpson\Documents\Important.rar.

Centrémonos en el proceso mspaint.exe, usando el plugin memdump para examinar los datos. El PID de este proceso es 2424.

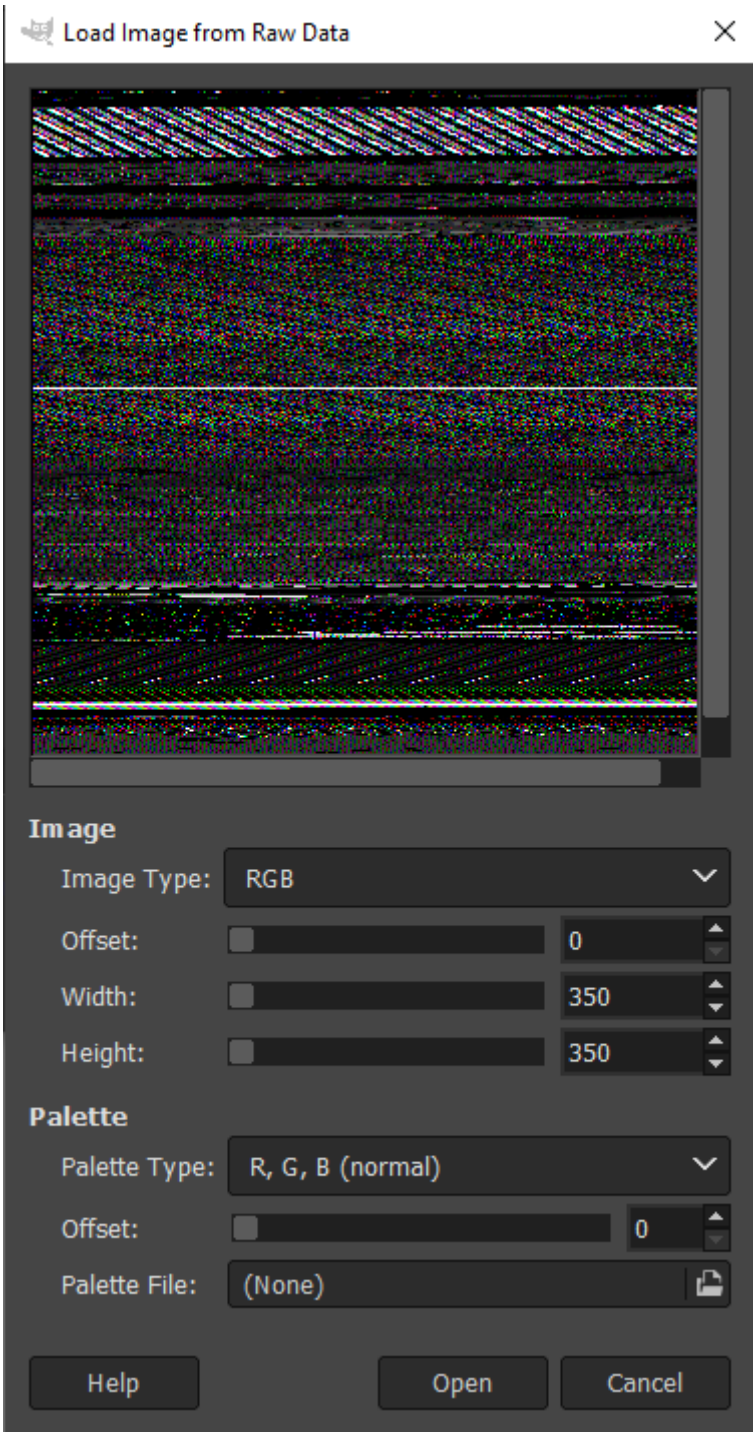
Si volvemos a la descripción del desafío, podemos ver que el usuario estaba dibujando algo (usando mspaint).

Así que vamos a utilizar el plugin memdump para extraer algunos datos.

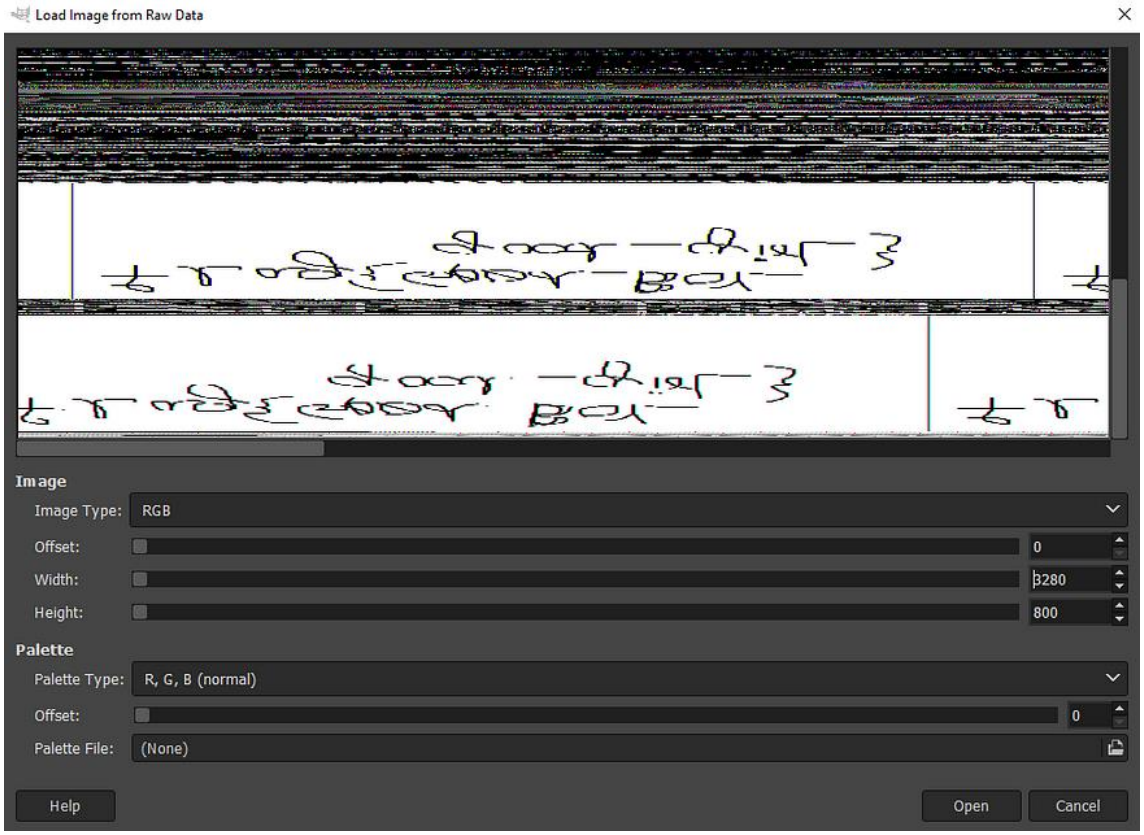


La salida se escribe en 2424.dmp. Tratando de abrir esto en WinDbg como se recomienda, conduce a fallos. Investigaciones posteriores recomiendan cambiar el nombre del archivo a .data y abrirlo con GIMP (GNU Image Manipulation Program).

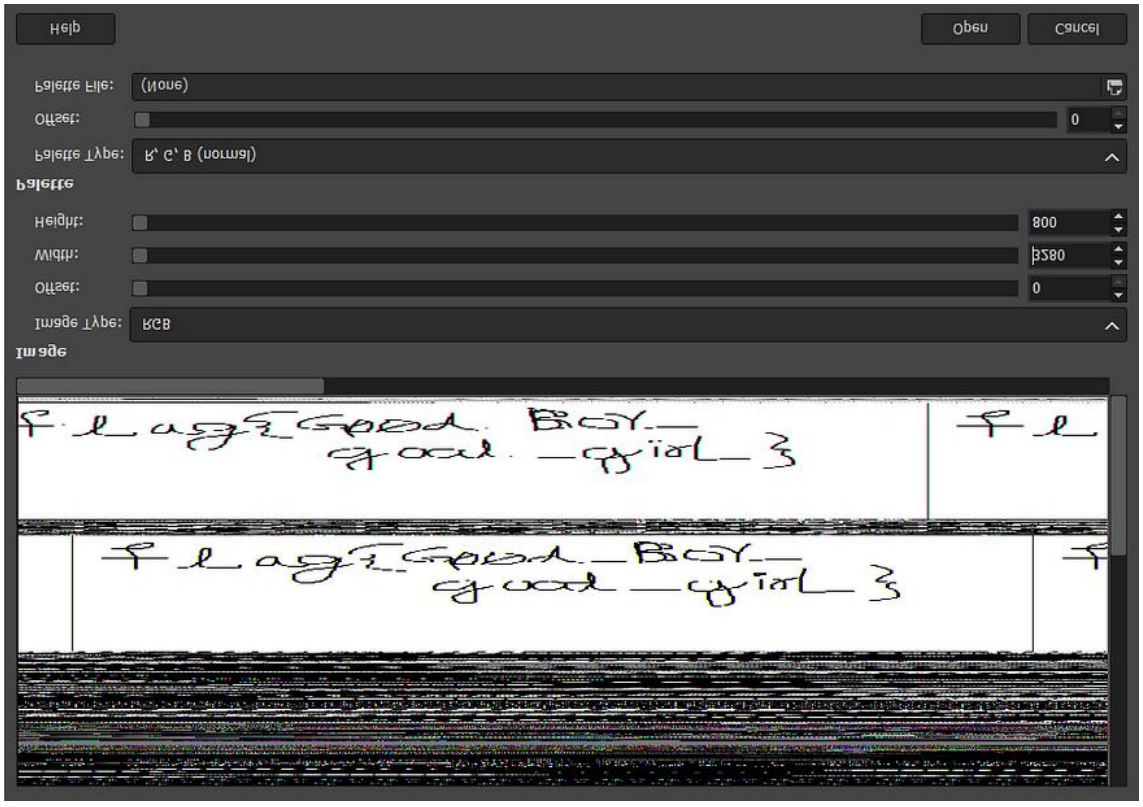
Después de jugar un poco con la anchura y el desplazamiento. Obtuve una imagen que está un poco volteada. La rote 180 grados y luego la voltee horizontalmente y Voila, obtuve la bandera.



Ajustando esta imagen, vemos lo que parece ser escritura:



Y ahí lo tenemos, utilizando Microsoft Paint para ajustar la imagen:



Flag 2: Flag{G00d_BoY_good_girL}

No es la bandera más sencilla teniendo en cuenta que este es el laboratorio 1 ... pero espero que tengamos una bandera bastante sencilla 3.

Creo que vale la pena volver a este archivo Important.rar usando el plugin filescan.

Volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw — profile=Win7SP1x64 filescan | findstr "Important.rar"

```
C:\Users\DEEP\Documents\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw --profile=W
in7SP1x64 filescan | findstr "Important.rar"
Volatility Foundation Volatility Framework 2.6
0x000000003fa3ebc0      1      0 R--r-- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
0x000000003fac3bc0      1      0 R--r-- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
0x000000003fb48bc0      1      0 R--r-- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
```

Bien sabemos que su hermana se llama Alissa Simpson y donde se encuentra este documento. Mirando el ID proporcionado, ahora podemos realizar un volcado de archivos:

volatility -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw — profile=Win7SP1x64 dumpfiles -Q 0x000000003fa3ebc0 -D C:\Users\DEEP\Desktop\

```
C:\Users\DEEP\Documents\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe -f C:\Users\DEEP\Downloads\MemoryDump_Lab1.raw --profile=W
in7SP1x64 dumpfiles -Q 0x000000003fa3ebc0 -D C:\Users\DEEP\Desktop\
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3fa3ebc0   None   \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
```

A continuación, cambie el nombre y el tipo de archivo a 'important.rar' y descomprímalo...

El archivo se descarga con el nombre file.None.0xfffffa8001034450.dat, vamos a renombrarlo y a descomprimirlo.

```
$ mv file.None.0xfffffa8001034450.dat Important.rar
$ unrar e Important.rar

UNRAR 5.61 beta 1 freeware      Copyright (c) 1993-2018 Alexander Roshal

Extracting from Important.rar

Password is NTLM hash(in uppercase) of Alissa's account passwd.

Enter password (will not be echoed) for flag3.png:
```

El archivo está protegido por contraseña, pero podemos ver un comentario que dice que la contraseña es el hash NTLM de la cuenta passwd de Alissa.

Para obtener el hash de la contraseña, podemos usar el plugin hashdump.

```
$ volatility -f MemoryDump_Lab1.raw --profile Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
SmartNet:1001:aad3b435b51404eeaad3b435b51404ee:4943abb39473a6f32c11301f4987e7
e0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f0fc3d257814e08fea06e63c
5762ebd5:::
Alissa
Simpson:1003:aad3b435b51404eeaad3b435b51404ee:f4ff64c8baac57d22f22edc681055ba
6:::
```

Windows almacena dos hashes con cada contraseña, delimitados por dos puntos. El primero es un hash extremadamente inseguro y obsoleto que utiliza el algoritmo LANMAN. Los sistemas operativos Windows

desde Vista ya no utilizan hashes LANMAN, por lo que se rellenan con un valor ficticio que empieza por "aad".

El segundo hash es el nuevo hash NTLM, que es mucho mejor que los hashes LANMAN, pero sigue siendo extremadamente inseguro y mucho más fácil de crackear que los hashes de Linux o Mac OS X.

El hash NTLM deseado es f4ff64c8baac57d22f22edc681055ba6 (recuerda que debe estar en mayúsculas).

Después de descomprimir el archivo, obtenemos una imagen con la bandera.

Flag 3: flag{w3ll)3rd_stage_was_easy}