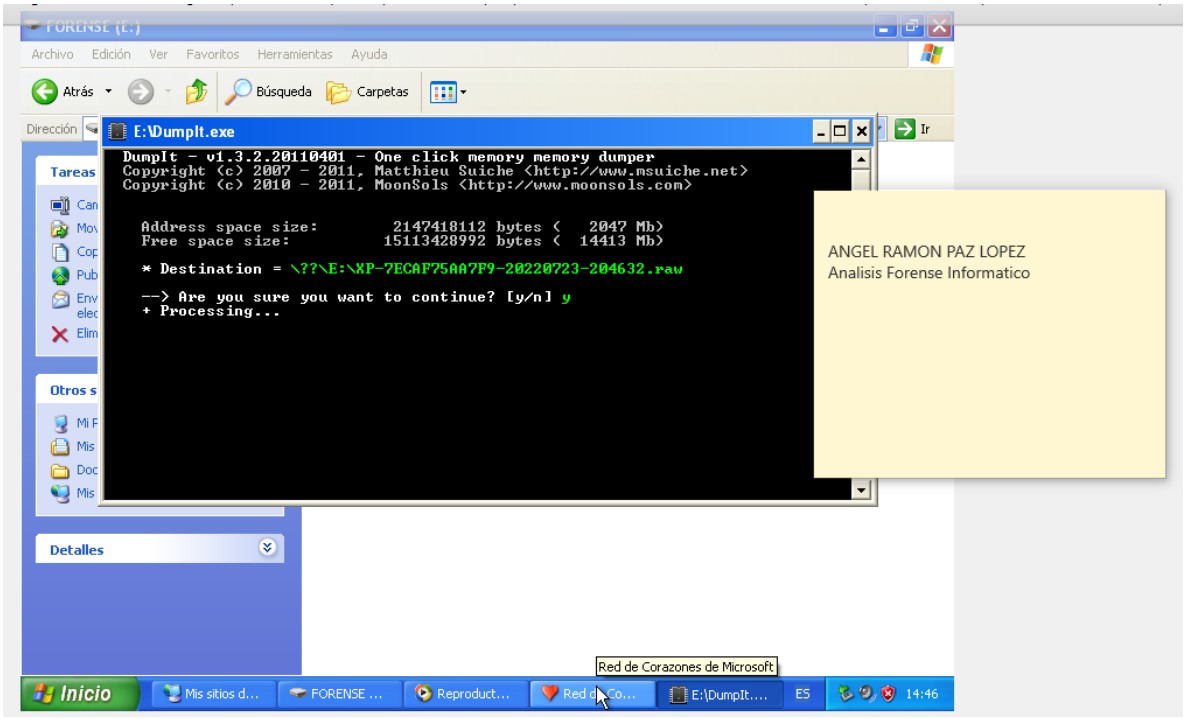
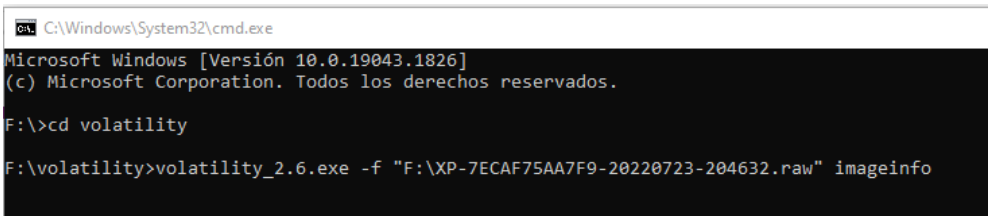
Asignatura	Datos del alumno	Fecha
Análisis forense	Apellidos: Paz López	23/07/2022
	Nombre: Angel Ramon	

Actividad: Obtención y análisis de un volcado de memoria de un equipo vivo.

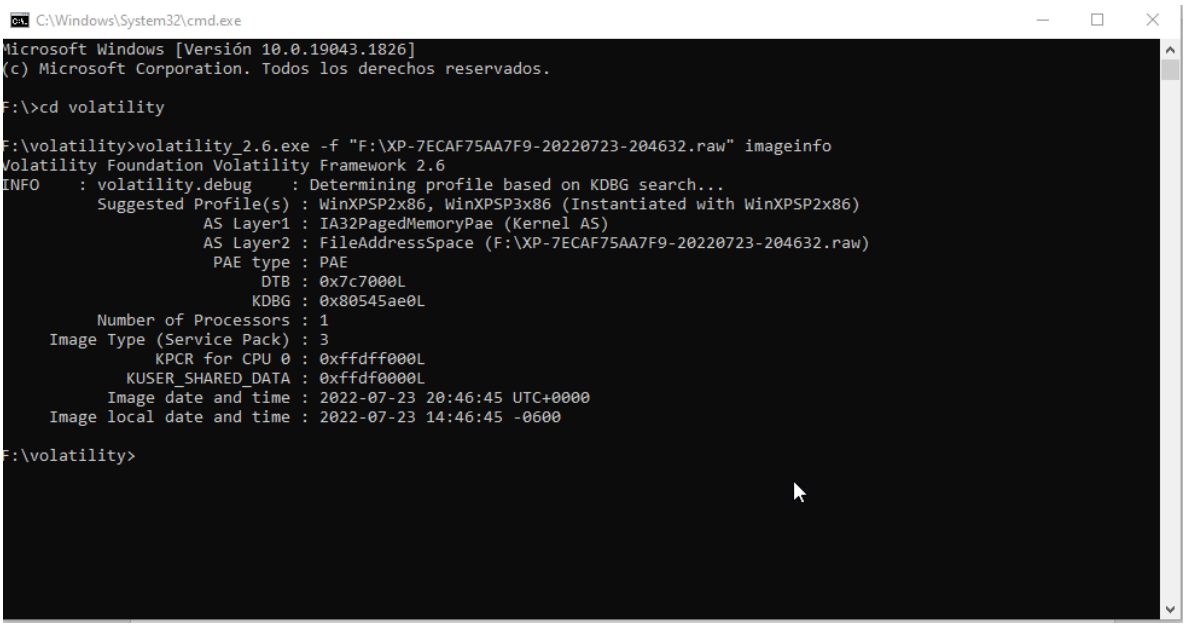
Creación del volcado de memoria con la herramienta DumpIt



Colocamos y (yes) para continuar y realizar el proceso de volcado de memoria, Analizamos el volcado a través de la herramienta volatility y usamos el plugin imageinfo para ver información importante del archivo de memoria.

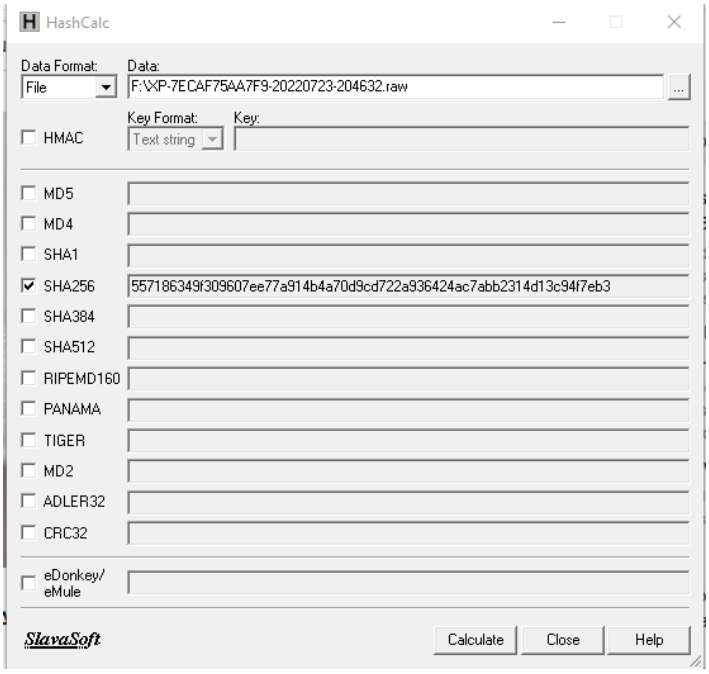


Y obtenemos el resultado



1. ¿Cuál es el Hash (SHA256) de la evidencia obtenida?

   557186349f309607ee77a914b4a70d9cd722a936424ac7abb2314d13c94f7eb3



2. ¿Cuál es el perfil de la evidencia?

   WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)

3. ¿Cuál sistema operativo instalado?

   Windows XP

4. ¿Cuáles son los procesos que se estaban ejecutando en el Dump de la memoria?

```
F:\volatility>volatility_2.6.exe -f "F:\XP-7ECAF75AA7F9-20220723-204632.raw" --profile=WinXPSP3x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----------
0x89a439c8 System                    4      0     51      164 ------      0

0x898b0da0 smss.exe                344      4      3       19 ------      0 2022-07-23 20:32:19 UTC+0000

0x8984d580 csrss.exe               400    344     11      348      0      0 2022-07-23 20:32:20 UTC+0000

0x8984dda0 winlogon.exe            424    344     20      543      0      0 2022-07-23 20:32:20 UTC+0000

0x89836368 services.exe            468    424     17      323      0      0 2022-07-23 20:32:23 UTC+0000

0x898318b0 lsass.exe               480    424     18      321      0      0 2022-07-23 20:32:23 UTC+0000

0x89810b88 svchost.exe             692    468      9      221      0      0 2022-07-23 20:32:26 UTC+0000

0x897fdda0 svchost.exe             732    468     73     1514      0      0 2022-07-23 20:32:26 UTC+0000

0x897f5500 svchost.exe             760    468     18      211      0      0 2022-07-23 20:32:26 UTC+0000

0x897db020 svchost.exe            1008    468      4       56      0      0 2022-07-23 20:35:32 UTC+0000

0x897d83e0 svchost.exe            1068    468     14      186      0      0 2022-07-23 20:35:32 UTC+0000

0x897c45a8 spoolsv.exe            1148    468     11      118      0      0 2022-07-23 20:35:32 UTC+0000

0x897497e0 alg.exe                1624    468      6       98      0      0 2022-07-23 20:35:36 UTC+0000

0x8972eda0 wmiprvse.exe           1920    760      6        0 ------      0 2022-07-23 20:35:36 UTC+0000

0x896df020 explorer.exe           1552   1524     17      532      0      0 2022-07-23 20:36:13 UTC+0000

0x896a62d0 wscntfy.exe            1892    732      1       35      0      0 2022-07-23 20:36:15 UTC+0000

0x89696428 ctfmon.exe              864   1552      1       74      0      0 2022-07-23 20:36:28 UTC+0000

0x89711020 wmplayer.exe           1760   1848     12      221      0      0 2022-07-23 20:45:51 UTC+0000

0x897b7020 mshearts.exe           1824   1552      2       67      0      0 2022-07-23 20:46:21 UTC+0000

0x89635918 DumpIt.exe             2004   1552      1       25      0      0 2022-07-23 20:46:32 UTC+0000
```

5. Muestra el listado de procesos en forma grafica (árbol)

```
F:\volatility>volatility_2.6.exe -f "F:\XP-7ECAF75AA7F9-20220723-204632.raw" --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x89a439c8:System                                      4      0     51    164 1970-01-01 00:00:00 UTC+0000
. 0x898b0da0:smss.exe                                 344      4      3     19 2022-07-23 20:32:19 UTC+0000
.. 0x8984dda0:winlogon.exe                            424    344     20    543 2022-07-23 20:32:20 UTC+0000
... 0x898318b0:lsass.exe                              480    424     18    321 2022-07-23 20:32:23 UTC+0000
... 0x89836368:services.exe                           468    424     17    323 2022-07-23 20:32:23 UTC+0000
.... 0x897db020:svchost.exe                          1008    468      4     56 2022-07-23 20:35:32 UTC+0000
.... 0x897c45a8:spoolsv.exe                          1148    468     11    118 2022-07-23 20:35:32 UTC+0000
.... 0x897497e0:alg.exe                              1624    468      6     98 2022-07-23 20:35:36 UTC+0000
.... 0x897d83e0:svchost.exe                          1068    468     14    186 2022-07-23 20:35:32 UTC+0000
.... 0x897f5500:svchost.exe                           760    468     18    211 2022-07-23 20:32:26 UTC+0000
..... 0x8972eda0:wmiprvse.exe                        1920    760      6      0 2022-07-23 20:35:36 UTC+0000
.... 0x89810b88:svchost.exe                           692    468      9    221 2022-07-23 20:32:26 UTC+0000
.... 0x897fdda0:svchost.exe                           732    468     73   1514 2022-07-23 20:32:26 UTC+0000
..... 0x896a62d0:wscntfy.exe                         1892    732      1     35 2022-07-23 20:36:15 UTC+0000
.. 0x8984d580:csrss.exe                               400    344     11    348 2022-07-23 20:32:20 UTC+0000
 0x896df020:explorer.exe                             1552   1524     17    532 2022-07-23 20:36:13 UTC+0000
. 0x89696428:ctfmon.exe                               864   1552      1     74 2022-07-23 20:36:28 UTC+0000
. 0x89635918:DumpIt.exe                              2004   1552      1     25 2022-07-23 20:46:32 UTC+0000
. 0x897b7020:mshearts.exe                            1824   1552      2     67 2022-07-23 20:46:21 UTC+0000
 0x89711020:wmplayer.exe                             1760   1848     12    221 2022-07-23 20:45:51 UTC+0000

F:\volatility>
```

6. ¿Cuáles son los puertos y conexiones abiertas?

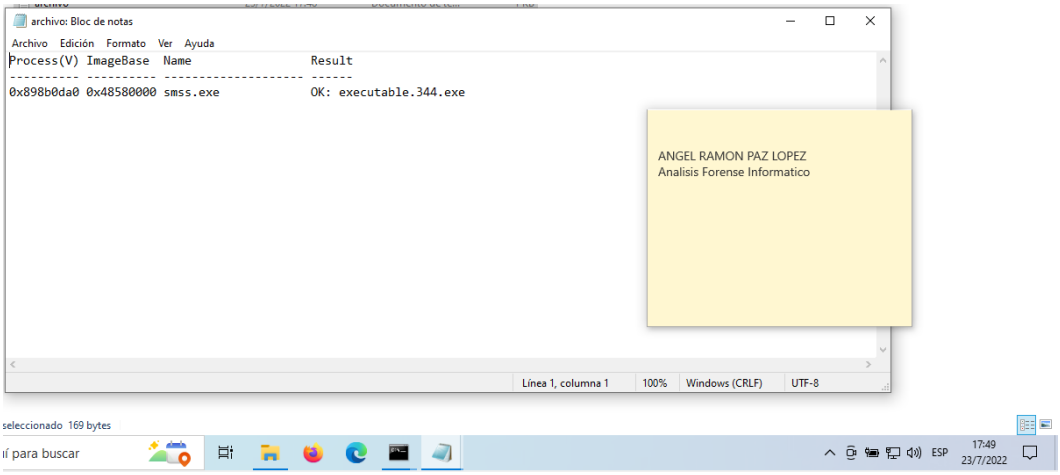
   No hubo ningún resultado

```
F:\volatility>volatility_2.6.exe -f "F:\XP-7ECAF75AA7F9-20220723-204632.raw" --profile=WinXPSP3x86 netscan
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : This command does not support the profile WinXPSP3x86

F:\volatility>volatility_2.6.exe -f "F:\XP-7ECAF75AA7F9-20220723-204632.raw" --profile=WinXPSP3x86 connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---

F:\volatility>
```

7. Extrae el proceso no. 15 que se estaba ejecutando en el Dump de memoria a un archivo de texto (agrega solo la imagen del archivo obtenido).

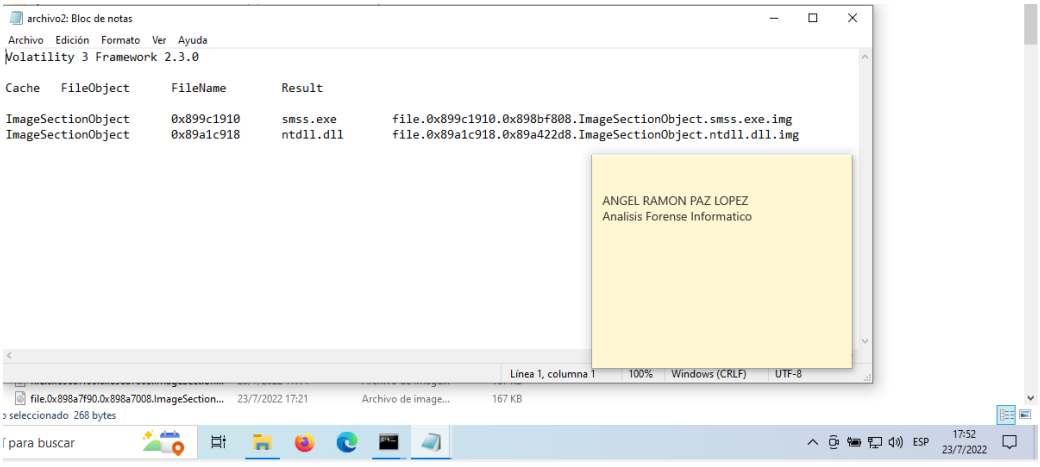
   No tenemos un proceso con numero 15 por lo cual probamos con el proceso 344

```
F:\volatility>volatility_2.6.exe -f "F:\XP-7ECAF75AA7F9-20220723-204632.raw" --profile=WinXPSP3x86 procdump -p 344 --dump-dir=F: >
archivo.txt
Volatility Foundation Volatility Framework 2.6
```



Probamos con volatility 3

```
F:\volatility3>vol.py -f "F:\XP-7ECAF75AA7F9-20220723-204632.raw" -o F: windows.dumpfiles --pid=344 > archivo2.txt
Progress:  100.00               PDB scanning finished
F:\volatility3>
```



8. Extrae los hashes de las contraseñas de los diferentes usuarios en un fichero llamado hashes.txt