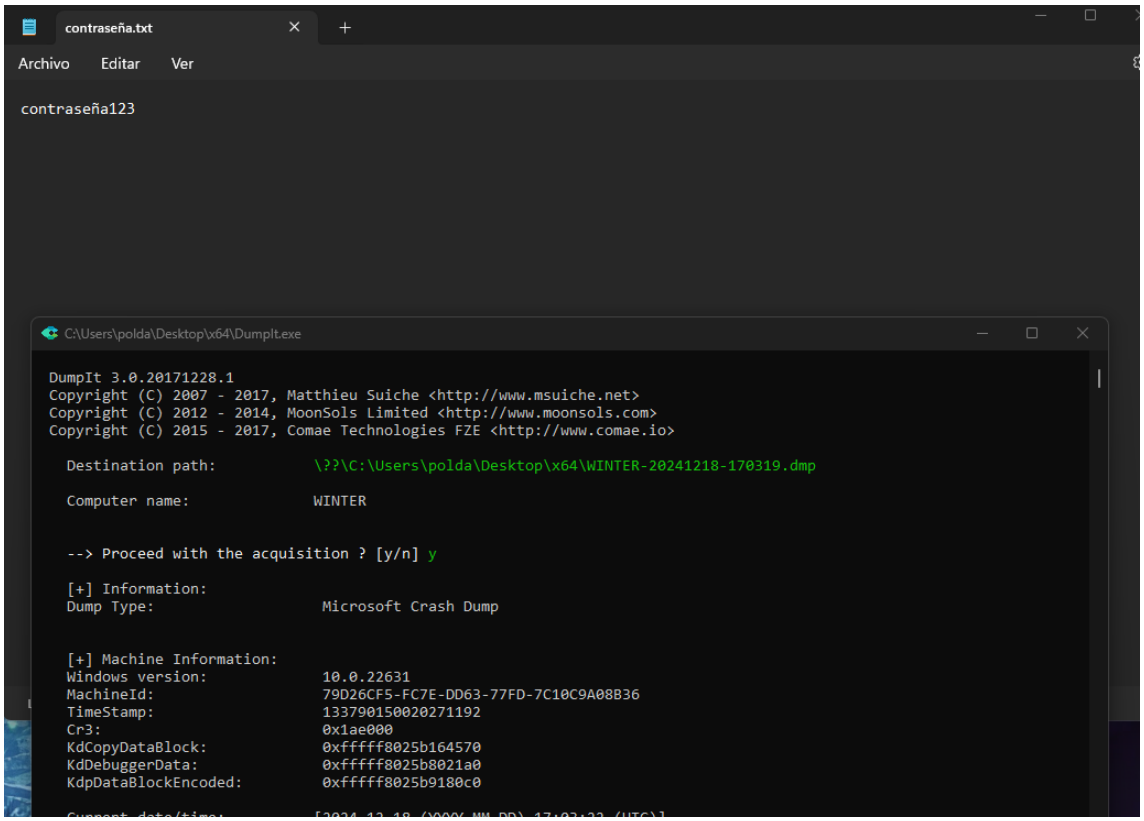
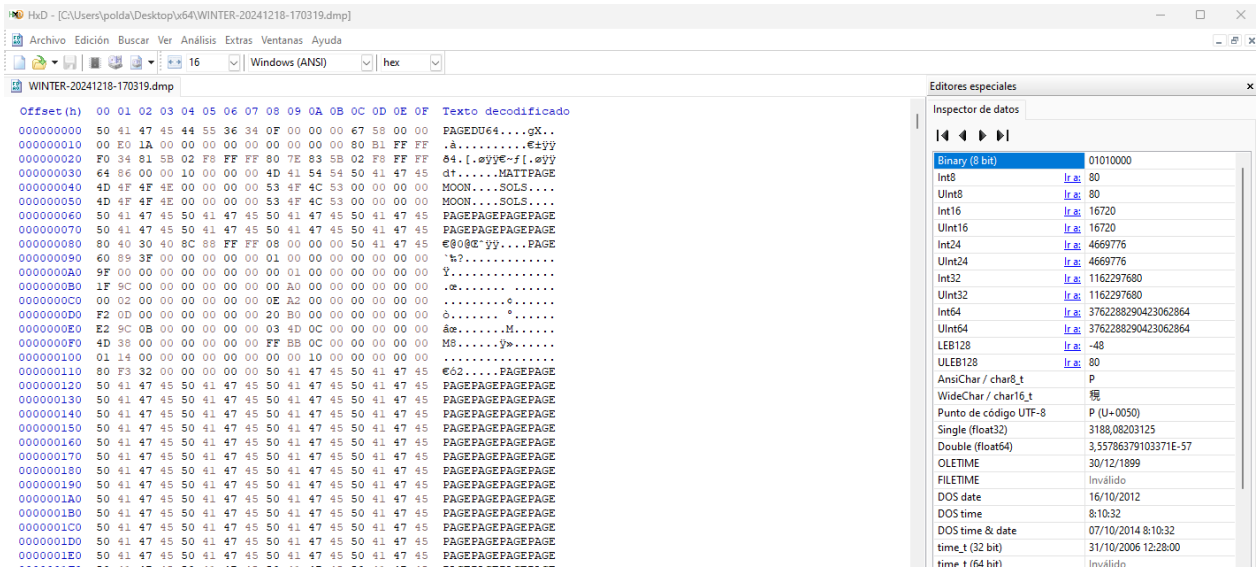
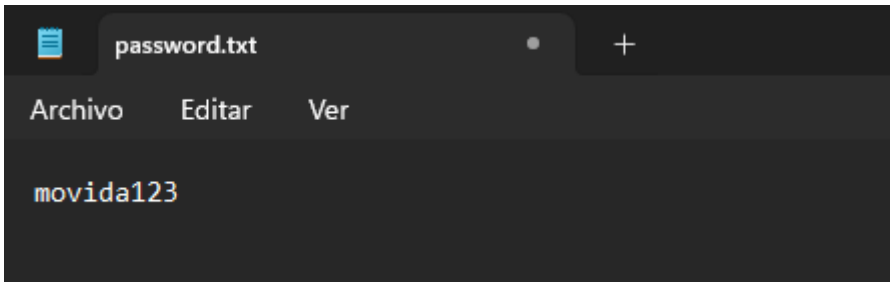
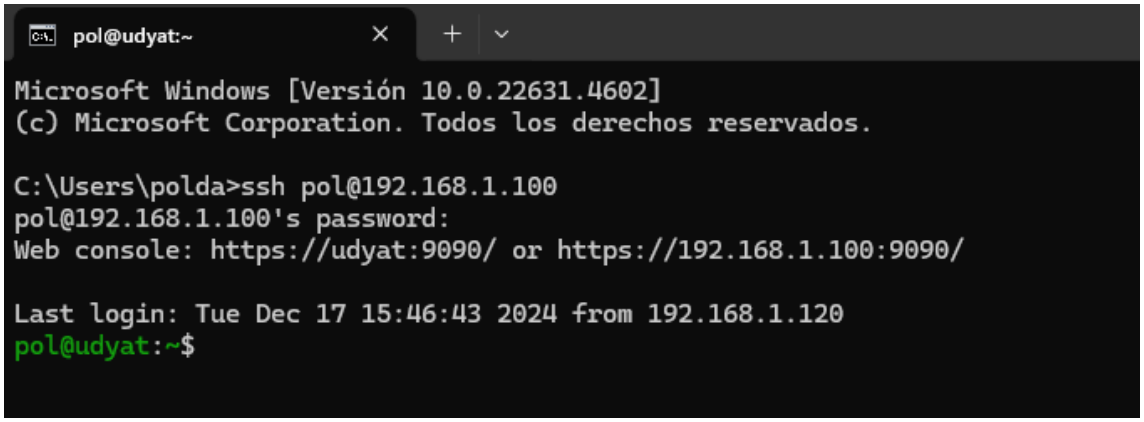

contraseña.txt
Archivo Editar Ver
contraseña123
C:\Users\polda\Desktop\x64\DumpIt.exe
DumpIt 3.0.20171228.1
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>
Destination path: \??\C:\Users\polda\Desktop\x64\WINTER-20241218-170319.dmp
Computer name: WINTER
--> Proceed with the acquisition ? [y/n] y
[+] Information:
Dump Type: Microsoft Crash Dump
[+] Machine Information:
Windows version: 10.0.22631
MachineId: 79D26CF5-FC7E-DD63-77FD-7C10C9A08B36
TimeStamp: 133790150020271192
Cr3: 0x1ae000
KdCopyDataBlock: 0xfffff8025b164570
KdDebuggerData: 0xfffff8025b8021a0
KdpDataBlockEncoded: 0xfffff8025b9180c0


HxD - [C:\Users\polda\Desktop\x64\WINTER-20241218-170319.dmp]
Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda
Windows (ANSI)
hex
WINTER-20241218-170319.dmp
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto decodificado
000000000 50 41 47 45 44 55 36 34 0F 00 00 00 67 58 00 00 PAGEDU64....gX..
000000010 00 E0 1A 00 00 00 00 00 00 00 00 00 80 B1 FF FF .à..........€±ÿÿ
000000020 F0 34 81 5B 02 F8 FF FF 80 7E 83 5B 02 F8 FF FF ð4.[.øÿÿ€~ƒ[.øÿÿ
000000030 64 86 00 00 10 00 00 00 4D 41 54 54 50 41 47 45 d†......MATTPAGE
000000040 4D 4F 4F 4E 00 00 00 00 53 4F 4C 53 00 00 00 00 MOON....SOLS....
000000050 4D 4F 4F 4E 00 00 00 00 53 4F 4C 53 00 00 00 00 MOON....SOLS....
000000060 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000070 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000080 80 40 30 40 8C 88 FF FF 08 00 00 00 50 41 47 45 €@0@Œˆÿÿ....PAGE
000000090 60 89 3F 00 00 00 00 00 01 00 00 00 00 00 00 00 `‰?.............
0000000A0 9F 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 Ÿ...............
0000000B0 1F 9C 00 00 00 00 00 00 00 A0 00 00 00 00 00 00 .œ..... ......
0000000C0 00 02 00 00 00 00 00 00 0E A2 00 00 00 00 00 00 ....¢......
0000000D0 F2 0D 00 00 00 00 00 00 20 B0 00 00 00 00 00 00 ò....... °......
0000000E0 E2 9C 0B 00 00 00 00 00 03 4D 0C 00 00 00 00 00 âœ.......M......
0000000F0 4D 38 00 00 00 00 00 00 FF BB 0C 00 00 00 00 00 M8......ÿ»......
000000100 01 14 00 00 00 00 00 00 00 00 10 00 00 00 00 00 ....
000000110 80 F3 32 00 00 00 00 00 50 41 47 45 50 41 47 45 €ó2.....PAGEPAGE
000000120 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000130 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000140 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000150 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000160 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000170 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000180 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
000000190 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
0000001A0 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
0000001B0 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
0000001C0 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
0000001D0 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
0000001E0 50 41 47 45 50 41 47 45 50 41 47 45 50 41 47 45 PAGEPAGEPAGEPAGE
Editores especiales
Inspector de datos
Binary (8 bit) 01010000
Int8 Ir a: 80
UInt8 Ir a: 80
Int16 Ir a: 16720
UInt16 Ir a: 16720
Int24 Ir a: 4669776
UInt24 Ir a: 4669776
Int32 Ir a: 1162297680
UInt32 Ir a: 1162297680
Int64 Ir a: 3762288290423062864
UInt64 Ir a: 3762288290423062864
LEB128 Ir a: -48
ULEB128 Ir a: 80
AnsiChar / char8_t P
WideChar / char16_t 稩
Punto de código UTF-8 P (U+0050)
Single (float32) 3188,08203125
Double (float64) 3,557863791033771E-57
OLETIME 30/12/1899
FILETIME Inválido
DOS date 16/10/2012
DOS time 8:10:32
DOS time & date 07/10/2014 8:10:32
time_t (32 bit) 31/10/2006 12:28:00
time_t (64 bit) Inválido

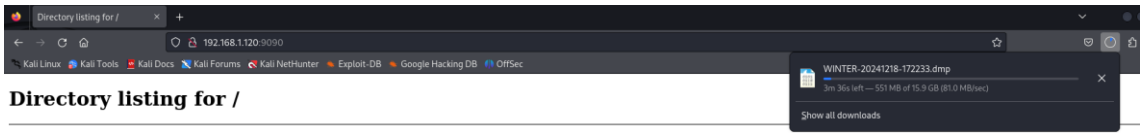



```
1E8F645A0  C0 1F 64 98 ED 01 00 00 C0 22 64 98 ED 01 00 00  À.d˜í...À"d˜í...
1E8F645B0  50 0D 64 98 ED 01 00 00 3C C6 D6 83 00 24 00 80  P.d˜í...<ÆÖƒ.$.€
1E8F645C0  6D 00 6F 00 76 00 69 00 64 00 61 00 31 00 32 00  m.o.v.i.d.a.1.2.
1E8F645D0  33 00 00 00 00 00 00 00 30 1E 68 98 ED 01 00 00  3.......0.h˜í...
1E8F645E0  00 00 00 00 ED 01 00 00 39 C6 D5 83 00 25 00 90  ....í...9ÆÕƒ.%..
1E8F645F0  D8 EE 60 51 FA 7F 00 00 15 00 00 00 00 00 00 00  Øî`Qú...........
1E8F64600  00 00 00 00 00 00 00 00 C0 1F 64 98 ED 01 00 00  ........À.d˜í...
```

Parte 2



```
DumpIt 3.0.20171228.1
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>

  Destination path:           \??\C:\Users\polda\Desktop\x64\WINTER-20241218-172233.dmp

  Computer name:              WINTER


  --> Proceed with the acquisition ? [y/n] y

  [+] Information:
  Dump Type:                   Microsoft Crash Dump


  [+] Machine Information:
  Windows version:             10.0.22631
  MachineId:                   79D26CF5-FC7E-DD63-77FD-7C10C9A08B36
  TimeStamp:                   133790161564868696
  Cr3:                         0x1ae000
  KdCopyDataBlock:             0xfffff8025b164570
  KdDebuggerData:              0xfffff8025b8021a0
  KdpDataBlockEncoded:         0xfffff8025b9180c0

  Current date/time:           [2024-12-18 (YYYY-MM-DD) 17:22:36 (UTC)]
  + Processing...
```




```
┌──(kali㉿kali)-[~]
└─$ pip install volatility3
Defaulting to user installation because normal site-packages is not writeable
Collecting volatility3
  Downloading volatility3-2.8.0-py3-none-any.whl.metadata (7.1 kB)
Requirement already satisfied: pefile ⩾ 2023.2.7 in /usr/lib/python3/dist-packages (from volatility3) (2023.2.7)
Downloading volatility3-2.8.0-py3-none-any.whl (740 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 740.1/740.1 kB 9.9 MB/s eta 0:00:00
Installing collected packages: volatility3
  WARNING: The scripts vol and volshell are installed in '/home/kali/.local/bin' which is not on PATH.
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-location.
Successfully installed volatility3-2.8.0

┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/volatilityfoundation/volatility3.git
Cloning into 'volatility3'...
remote: Enumerating objects: 38725, done.
remote: Counting objects: 100% (5475/5475), done.
remote: Compressing objects: 100% (868/868), done.
remote: Total 38725 (delta 5108), reused 4607 (delta 4607), pack-reused 33250 (from 3)
Receiving objects: 100% (38725/38725), 7.97 MiB | 10.00 MiB/s, done.
Resolving deltas: 100% (29596/29596), done.
```

Windows.info

```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f WINTER-20241218-172233.dmp windows.info
Volatility 3 Framework 2.13.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f8025ac00000
DTB     0×1ae000
Symbols file:///home/kali/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/C69901A080C51A3DC5B0956D4880730A-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 WindowsCrashDump64Layer
base_layer      2 FileLayer
KdVersionBlock  0×f8025b809998
Major/Minor     15.22621
MachineType     34404
KeNumberProcessors      16
SystemTime      2024-12-18 17:22:37+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Sat Mar 24 23:31:57 2001
```

Windows.pslist

```
┌──(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f WINTER-20241218-172233.dmp windows.pslist
Volatility 3 Framework 2.13.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0×888c10741040  395     -       N/A     False   2024-12-12 09:23:10.000000 UTC  N/A     Disabled
172     4       Secure System   0×888c107d8040  0       -       N/A     False   2024-12-12 09:23:04.000000 UTC  N/A     Disabled
212     4       Registry        0×888c108d0040  4       -       N/A     False   2024-12-12 09:23:04.000000 UTC  N/A     Disabled
768     4       smss.exe        0×888c17d56080  2       -       N/A     False   2024-12-12 09:23:10.000000 UTC  N/A     Disabled
648     1016    csrss.exe       0×888c1791c180  13      -       0       False   2024-12-12 09:23:12.000000 UTC  N/A     Disabled
1132    1016    wininit.exe     0×888c19ec90c0  2       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1156    1124    csrss.exe       0×888c21718180  0       -       1       False   2024-12-12 09:23:14.000000 UTC  2024-12-12 17:17:08.000000 UTC  Disabled
1208    1132    services.exe    0×888c20f86100  8       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1280    1132    LsaIso.exe      0×888c1d0b00c0  1       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1296    1132    lsass.exe       0×888c1d0950c0  12      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1444    1208    svchost.exe     0×888c20fdb0c0  26      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1472    1132    fontdrvhost.ex  0×888c210680c0  5       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1552    1208    WUDFHost.exe    0×888c212570c0  8       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1620    1208    svchost.exe     0×888c2138a0c0  31      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1664    1208    svchost.exe     0×888c214bd0c0  5       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1844    1208    svchost.exe     0×888c1d6760c0  3       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1896    1208    svchost.exe     0×888c1d7020c0  2       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1904    1208    svchost.exe     0×888c1d6db0c0  2       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1968    1208    svchost.exe     0×888c1d7880c0  9       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
1992    1208    svchost.exe     0×888c1d9340c0  1       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2044    1208    svchost.exe     0×888c1d9aa0c0  13      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2148    1208    svchost.exe     0×888c1df560c0  10      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2316    1208    svchost.exe     0×888c1e46f0c0  6       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2380    1208    svchost.exe     0×888c1e8130c0  13      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2432    1208    svchost.exe     0×888c1e6ec0c0  4       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2468    1208    svchost.exe     0×888c1e86e0c0  7       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2592    1208    vmms.exe        0×888c1f4ea0c0  12      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2600    1208    svchost.exe     0×888c1f6870c0  5       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2668    1208    svchost.exe     0×888c217230c0  7       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2676    1208    amdfendrsr.exe  0×888c217020c0  4       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2684    1208    AsusCertServic  0×888c217550c0  5       -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2692    1208    atiesrxx.exe    0×888c203e90c0  14      -       0       False   2024-12-12 09:23:14.000000 UTC  N/A     Disabled
2888    1208    svchost.exe     0×888c1e3c20c0  5       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
2924    1208    svchost.exe     0×888c1e5f20c0  7       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
2992    1208    svchost.exe     0×888c210c70c0  3       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3000    1208    svchost.exe     0×888c210c90c0  6       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3008    1208    svchost.exe     0×888c210d80c0  4       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
1220    4       MemCompression  0×888c21139080  26      -       N/A     False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3100    1208    svchost.exe     0×888c211520c0  2       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3144    1208    svchost.exe     0×888c2117b0c0  2       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3152    1208    svchost.exe     0×888c2117f0c0  9       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3240    1248    dwm.exe 0×888c211d80c0  0       -       1       False   2024-12-12 09:23:15.000000 UTC  2024-12-12 17:17:06.000000 UTC  Disabled
3332    1208    svchost.exe     0×888c212260c0  7       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3360    1208    svchost.exe     0×888c212540c0  12      -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3384    1208    atkexComSvc.ex  0×888c2128b0c0  3       -       0       True    2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3536    1444    WmiPrvSE.exe    0×888c2131b0c0  4       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
3712    1208    svchost.exe     0×888c213b40c0  2       -       0       False   2024-12-12 09:23:15.000000 UTC  N/A     Disabled
```

```
26992   31332   cmd.exe 0×888c2d3e7080  1       -       6       False   2024-12-18 17:21:26.000000 UTC  N/A     Disabled
9460    26992   conhost.exe     0×888c294e4080  4       -       6       False   2024-12-18 17:21:26.000000 UTC  N/A     Disabled
28280   1444    OpenConsole.ex  0×888c21f35080  10      -       6       False   2024-12-18 17:21:26.000000 UTC  N/A     Disabled
2480    1444    WindowsTermina  0×888c25af2080  49      -       6       False   2024-12-18 17:21:26.000000 UTC  N/A     Disabled
14100   1444    RuntimeBroker.  0×888c2a4e3080  4       -       6       False   2024-12-18 17:21:26.000000 UTC  N/A     Disabled
10276   1208    svchost.exe     0×888c2d2a50c0  6       -       0       False   2024-12-18 17:21:52.000000 UTC  N/A     Disabled
9712    11796   SearchProtocol  0×888c385900c0  6       -       0       False   2024-12-18 17:21:54.000000 UTC  N/A     Disabled
14504   11796   SearchFilterHo  0×888c26b660c0  3       -       0       False   2024-12-18 17:21:54.000000 UTC  N/A     Disabled
17704   26992   ssh.exe 0×888c232f7080  4       -       6       False   2024-12-18 17:21:57.000000 UTC  N/A     Disabled
```

Como me he conectado con la Shell supongo que o el cmd.exe o ssh.exe (más ssh.exe que el cmd) és el proceso que esta ejecutando la conexión

```
0×888c2b5c4a80  TCPv4   192.168.1.120   3299    192.168.1.1     46072   CLOSED  -       -       N/A
0×888c2b5ed010  TCPv4   192.168.1.120   3311    192.168.1.100   22      ESTABLISHED     -       -       N/A
0×888c2c17ba70  TCPv4   192.168.1.120   3138    95.100.109.84   443     CLOSED  -       -       N/A
0×888c2c1d8a50  TCPv4   192.168.1.120   2970    192.168.1.1     53      CLOSED  -       -       N/A
0×888c2c9a7ae0  TCPv4   127.0.0.1       2159    127.0.0.1       9012    ESTABLISHED     -       -       N/A
0×888c2d20fdc0  UDPv4   0.0.0.0 51596   *       0       -       -       2024-12-17 17:48:30.000000 UTC
0×888c2d20fdc0  UDPv6   ::      51596   *       0       -       -       2024-12-17 17:48:30.000000 UTC
0×888c2d2485e0  TCPv4   192.168.1.120   3246    185.199.111.154 443     ESTABLISHED     -       -       N/A
0×888c2d407010  TCPv4   192.168.1.120   2316    52.123.135.28   443     ESTABLISHED     -       -       N/A
0×888c2d408010  TCPv4   192.168.1.120   3282    84.53.132.121   443     CLOSED  -       -       N/A
0×888c2d408520  TCPv4   192.168.1.120   2310    52.112.100.74   443     CLOSED  -       -       N/A
0×888c2db1bab0  TCPv4   192.168.1.120   2936    52.111.243.12   443     CLOSED  -       -       N/A
0×888c2e0d55e0  TCPv4   192.168.1.120   3288    2.17.211.161    443     ESTABLISHED     -       -       N/A
```

Ahí vemos la conexión desde mi ordenador al servidor destino.

Preguntas:

1. **¿Cuál es la utilidad del análisis de memoria en un escenario forense?**

   En un escenario forense, permite identificar actividades sospechosas, como malware en ejecución, conexiones de red activas, o credenciales almacenadas temporalmente, ayudando a reconstruir eventos o detectar amenazas.

2. **¿Qué tipos de artefactos se pueden recuperar de un volcado de memoria?**
   Se pueden recuperar contraseñas en texto claro, información sobre procesos en ejecución, claves de cifrado, actividad en la red, documentos abiertos y datos temporales que no se almacenan en disco.

3. **¿Cómo podría un atacante aprovechar la información extraída de un volcado de memoria?**
   Un atacante podría usar información sensible, como contraseñas o claves de cifrado, para escalar privilegios, acceder a sistemas adicionales o descifrar datos protegidos.

4. **¿Qué medidas de seguridad se podrían implementar para mitigar los riesgos asociados con los datos que se encuentran en un volcado de memoria?**

    - Cifrar la memoria en reposo.
    - Limitar los permisos de acceso a la memoria.
    - Usar soluciones que limpien datos sensibles de la memoria regularmente.
    - Detectar y bloquear herramientas que intenten realizar volcados de memoria.