

What volatility profile is the most appropriate for this machine? | Weight: +25

```
└── vol.py -f memory.dmp imageinfo
  Volatility Foundation Volatility Framework 2.6.1
  INFO : volatility.debug : Determining profile based on KDBG search...
  Suggested Profile(s): WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
    AS Layer1 : IA32PagedMemoryPae (Kernel AS)
    AS Layer2 : WindowsCrashDumpSpace32 (Unnamed AS)
    AS Layer3 : FileAddressSpace (/mnt/c/Users/Mohamed Rafrraf/Desktop/The Pilot/memory.dmp)
    PAE type : PAE
      DTB : 0x2a60020L
      KDBG : 0x8054d2e0L
    Number of Processors : 4
  Image Type (Service Pack) : 3
    KPCR for CPU 0 : 0xffdff000L
    KPCR for CPU 1 : 0xf8922000L
    KPCR for CPU 2 : 0xf892a000L
    KPCR for CPU 3 : 0xf8932000L
    KUSER_SHARED_DATA : 0xffdf0000L
  Image date and time : 2022-08-31 15:14:53 UTC+0000
  Image local date and time : 2022-08-31 10:14:53 -0500
at 22:33:1
```

What is the MD5 hash of the memory dump? | Weight: +25

```
└── md5sum memory.dmp
  9200b1d9e8804ca472695e1b66a7925f  memory.dmp
```

What is the hostname? | Weight: +25

```
└── vol.py -f memory.dmp envars | grep -i computer
  Volatility Foundation Volatility Framework 2.6.1
    640 winlogon.exe      0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
    684 services.exe      0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
    696 lsass.exe         0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
    868 vmacthlp.exe      0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
    884 svchost.exe       0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
    956 svchost.exe       0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
   1084 svchost.exe       0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
   1272 svchost.exe       0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
   1376 svchost.exe       0x00010000 COMPUTERNAME      UNKNOWN-F549DD2
```

What is the PID of the Notepad process? | Weight: +25

vol.py -f memory.dmp pstrace

Volatility Foundation Volatility Framework 2.6.1

Name	Pid	PPid	Thds	Hnds	Time	
0x823c6830:System	4	0	69	259	1970-01-01 00:00:00	UTC+0000
0x81e16550:smss.exe	552	4	3	19	2022-08-31 15:03:46	UTC+0000
0x8202e2c0:winlogon.exe	640	552	16	292	2022-08-31 15:03:49	UTC+0000
0x81fdb458:services.exe	684	640	15	301	2022-08-31 15:03:50	UTC+0000
0x81e9d948:alg.exe	1680	684	7	113	2022-08-31 15:04:38	UTC+0000
0x81e11a78:svchost.exe	1292	684	4	112	2022-08-31 15:04:15	UTC+0000
0x822507e8:svchost.exe	816	684	21	432	2022-08-31 15:04:16	UTC+0000
0x81e16808:svchost.exe	1084	684	73	1199	2022-08-31 15:03:54	UTC+0000
0x81ea1550:wsctnfy.exe	1344	1084	1	43	2022-08-31 15:04:35	UTC+0000
0x81f31020:wuauclt.exe	2924	1084	7	141	2022-08-31 15:09:55	UTC+0000
0x821f3228:svchost.exe	1376	684	13	190	2022-08-31 15:03:56	UTC+0000
0x82041da0:vmacthlp.exe	868	684	1	26	2022-08-31 15:03:52	UTC+0000
0x81ef3b20:VGAuthService.e	1768	684	2	60	2022-08-31 15:04:19	UTC+0000
0x81e09020:svchost.exe	956	684	11	310	2022-08-31 15:03:53	UTC+0000
0x81a75770:spoolsv.exe	1520	684	10	142	2022-08-31 15:03:59	UTC+0000
0x8225c8a0:vmtoolsd.exe	168	684	8	279	2022-08-31 15:04:27	UTC+0000
0x820ae020:cmd.exe	2732	168	0	-----	2022-08-31 15:14:52	UTC+0000
0x81e263e8:svchost.exe	884	684	22	235	2022-08-31 15:03:52	UTC+0000
0x81ebc8c8:wmiprvse.exe	496	884	13	283	2022-08-31 15:04:33	UTC+0000
0x820f6da0:svchost.exe	1272	684	4	81	2022-08-31 15:03:55	UTC+0000
0x81e1da70:lsass.exe	696	640	27	394	2022-08-31 15:03:50	UTC+0000
0x821fb020:csrss.exe	616	552	12	475	2022-08-31 15:03:47	UTC+0000
0x81f10158:explorer.exe	1308	1216	17	493	2022-08-31 15:04:15	UTC+0000
0x81a50020:cmd.exe	3904	1308	1	30	2022-08-31 15:07:25	UTC+0000
0x81fbe3c0:ctfmon.exe	1164	1308	1	94	2022-08-31 15:04:23	UTC+0000
0x81e82508:clipbrd.exe	3048	1308	1	64	2022-08-31 15:05:51	UTC+0000
0x82023228:vmtoolsd.exe	1972	1308	5	151	2022-08-31 15:04:23	UTC+0000
0x81e27da0:notepad.exe	584	1308	1	61	2022-08-31 15:05:02	UTC+0000
0x820b9da0:iexplore.exe	312	1308	14	593	2022-08-31 15:05:15	UTC+0000

What is the PID of the Explorer process? | Weight: +25 : 1308

What is the parent process start time of notepad.exe? | Weight: +50 : 2022-08-31 15:04:15

0x81f10158:explorer.exe	1308	1216	17	493	2022-08-31 15:04:15	UTC+0000
0x81a50020:cmd.exe	3904	1308	1	30	2022-08-31 15:07:25	UTC+0000
0x81fbe3c0:ctfmon.exe	1164	1308	1	94	2022-08-31 15:04:23	UTC+0000
0x81e82508:clipbrd.exe	3048	1308	1	64	2022-08-31 15:05:51	UTC+0000
0x82023228:vmtoolsd.exe	1972	1308	5	151	2022-08-31 15:04:23	UTC+0000
0x81e27da0:notepad.exe	584	1308	1	61	2022-08-31 15:05:02	UTC+0000

What is the IP Address used by the machine? | Weight: +50

```
└──╼ └── /mnt/c/Users/Mohamed Rafrraf/Desktop/The Pilot
    └── vol.py -f memory.dmp connscan
```

Volatility Foundation Volatility Framework 2.6.1

Offset(P)	Local Address	Remote Address	Pid
0x01c2d6e0	192.168.1.130:1121	52.97.201.226:443	312
0x01c30638	192.168.1.130:1090	104.20.67.143:443	564
0x01c69e68	192.168.1.130:1113	41.231.245.24:443	564
0x01c77008	192.168.1.130:1098	92.123.112.145:443	564
0x01c9d008	192.168.1.130:1124	20.190.159.5:443	564
0x02039420	37.0.0.0:0	42.0.0.0:8192	23

What is the executable path for process ID 1164? | Weight: +75

```
└──╼ └── /mnt/c/Users/Mohamed Rafrraf/Desktop/The Pilot
    └── vol.py -f memory.dmp cmdline | grep 1164 -C 1
```

Volatility Foundation Volatility Framework 2.6.1

```
*****  
ctfmon.exe pid:  1164  
Command line : "C:\WINDOWS\system32\ctfmon.exe"
```

My Grandfather calls CMD, the Black Language, can you find the flag there? | Weight: +50

```
└─$ vol.py -f memory.dmp cmdscan
Volatility Foundation Volatility Framework 2.6.1
*****
CommandProcess: csrss.exe Pid: 616
CommandHistory: 0x504ef0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 8 LastAdded: 7 LastDisplayed: 7
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x650
Cmd #0 @ 0x501eb8: echo "Hi Dude"
Cmd #1 @ 0xaa3898: echo "This Plugin allow you"
Cmd #2 @ 0xaa3400: >echo "To inspect the history"
Cmd #3 @ 0xaa34c8: echo "of Command Prompt (CMD)"
Cmd #4 @ 0xaa3398: echo "I used to called it as Language Ak7el"
Cmd #5 @ 0xaa3598: echo eWVzIHRha2UgaXQg0lNlY3VyaW5ldHN7VEgzX0JMNENLX0xWZ3V
Cmd #6 @ 0xaa3740: BZ2VfMTVfQVczNTBtZX0=
Cmd #7 @ 0x509078: echo eWVzIHRha2UgaXQg0lNlY3VyaW5ldHN7VEgzX0JMNENLX0xWZ3VBZ2VfMTVfQVczNTBtZX0=
^C
```

```
└─$ echo eWVzIHRha2UgaXQg0lNlY3VyaW5ldHN7VEgzX0JMNENLX0xWZ3VBZ2VfMTVfQVczNTBtZX0= | base64 -d
yes take it :Securinets{TH3_BL4CK_LVguAge_15_AW350me}%
```

My Grandfather is environmental, can you find the flag? | Weight: +75 (it's hint about variable env)

```
└─$ vol.py -f memory.dmp envars | grep -i flag
Volatility Foundation Volatility Framework 2.6.1
1308 explorer.exe          0x00990000 flag is here yes
V4r1Able_ENV_1S_Helpful
```

My Grandfather left something in the Desktop, can you find it? | Weight: +100

```
└─ vol.py -f memory.dmp filescan | grep Desktop
Volatility Foundation Volatility Framework 2.6.1
0x00000000001c4f600 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\Documents\My
0x00000000001c4f698 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Admin\Recent\Desktop.in
0x0000000000200a5b8 3 1 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\Desktop
0x00000000002024580 3 1 R--rwd \Device\HarddiskVolume1\Documents and Settings\Admin\Desktop
0x0000000000207df50 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\Documents\My
0x0000000000208a1b8 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\All Users\Documents\My
0x0000000000209eb20 1 1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Admin\Desktop
0x000000000020a1b00 1 0 R--r-- \Device\HarddiskVolume1\Documents and Settings\Admin\Desktop\flag.png
0x000000000020bc2d0 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Admin\Favorites\Desktop
0x0000000000212c028 1 0 R--r-d \Device\HarddiskVolume1\Documents and Settings\All Users\Start Menu\Pr
Connection.lnk
0x000000000023167f8 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Admin\My Documents\My P
0x000000000023ffb00 1 0 R--rwd \Device\HarddiskVolume1\Documents and Settings\Admin\My Documents\My M
0x000000000024190c0 1 1 R--rw- \Device\HarddiskVolume1\Documents and Settings\Admin\Desktop

└─ vol.py -f memory.dmp dumpfiles -Q 0x000000000020a1b00 -D .
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x020a1b00 None \Device\HarddiskVolume1\Documents and Settings\Admin\Desktop\flag.png
```

Securinets{Dump_F1L3S_1S_My_Be5t_PLuG1N}

My Grandfather copied his password, can you find it? | Weight: +100

```
vol.py -f memory.dmp clipboard -v
Volatility Foundation Volatility Framework 2.6.1
Session WindowStation Format Handle Object Data
-----
0 WinSta0 0xc009L 0x1f0101 0xe1c72570
0xe1c7257c f2 01 01 00
0 WinSta0 CF_TEXT 0xd -----
0 WinSta0 CF_TEXT 0x0 -----
0 WinSta0 0x300085L 0x1 -----
0 WinSta0 CF_LOCALE 0x780055 0xe1805580
0xe180558c 09 04 00 00
0 WinSta0 0x0L 0x1 -----
0 ----- 0x1a0237 0xe1d202c0
0xe1d202cc 43 00 4f 00 70 00 59 00 5f 00 50 00 34 00 73 00 C.0.p.Y._.P.4.s.
0xe1d202dc 54 00 33 00 5f 00 53 00 34 00 76 00 33 00 5f 00 T.3._.S.4.v.3._.
0xe1d202ec 4d 00 79 00 5f 00 4c 00 31 00 66 00 33 00 00 00 M.y._.L.1.f.3...
0 ----- 0x300085 0xe2377d20
```

Just one more mysterious flag, can you find it? | Weight: +200:

Mmm just i wrote the flag in notepad , strings -e l (little endian) will be helpful to get the flag

```
strings -e l memory.dmp | grep -i securinets
Securinets{StR1Ngs_h3lpFUL_But_FuCK_1t}
```

My grandfather had saved some sensitive information in a specific website. Can you find what's been hidden in the history of his default browser

Run Vol.py -f memory.dmp iehistory

```
*****
Process: 564 iexplore.exe
Cache type "URL" at 0x5ad5000
Record length: 0x100
Location: :2022083120220901: Admin@https://pastebin.com/aNBAWAP8
Last modified: 2022-08-31 10:05:38 UTC+0000
Last accessed: 2022-08-31 15:05:38 UTC+0000
File Offset: 0x100, Data Offset: 0x0, Data Length: 0x0
*****
```

 Not a member of Pastebin yet? [Sign Up](#), it unlocks many cool features!

text 0.09 KB | None |  0  0

1. You'll find the flag here honestly
2. U2VjdXJpbmV0c3sxX0wwdjNfQ3VyTF9GdWNLX0JyMHc1ZVJzfQ==

```
└─➤ /mnt/c/Users/Mohamed Rafrraf/Desktop/The Pilot
└─➤ echo "U2VjdXJpbmV0c3sxX0wwdjNfQ3VyTF9GdWNLX0JyMHc1ZVJzfQ==" | base64 -d
Securinets{1_L0v3_CurL_FucK_Br0w5eRs}%
```