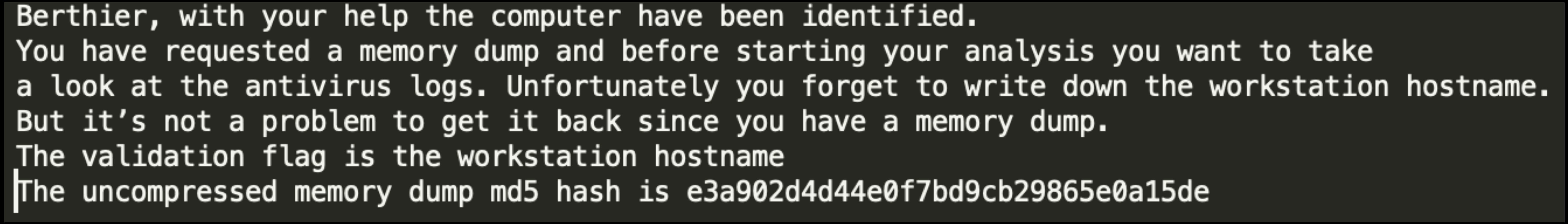
Root-me Command & Control level2

2019.01.08@plit00

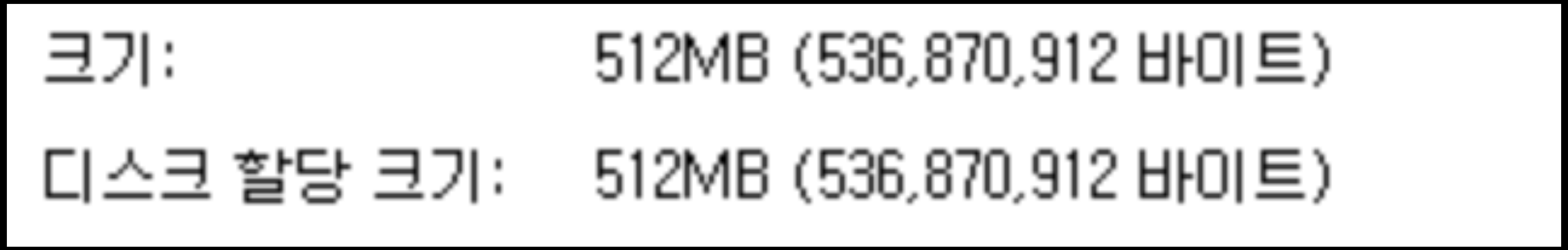
Prl



```
Berthier, with your help the computer have been identified.
You have requested a memory dump and before starting your analysis you want to take
a look at the antivirus logs. Unfortunately you forget to write down the workstation hostname.
But it’s not a problem to get it back since you have a memory dump.
The validation flag is the workstation hostname
The uncompressed memory dump md5 hash is e3a902d4d44e0f7bd9cb29865e0a15de
```

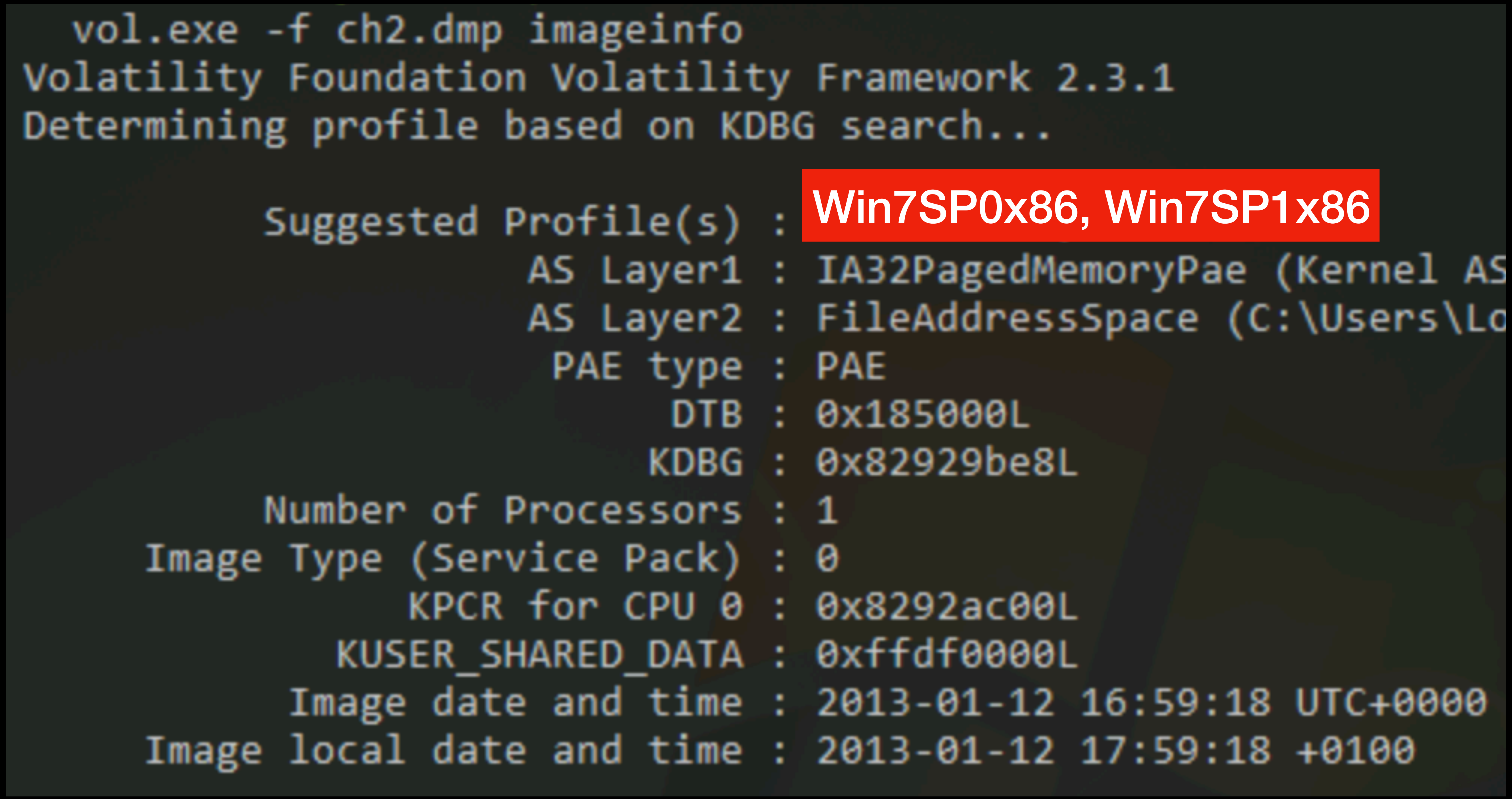
Cmder

Byte



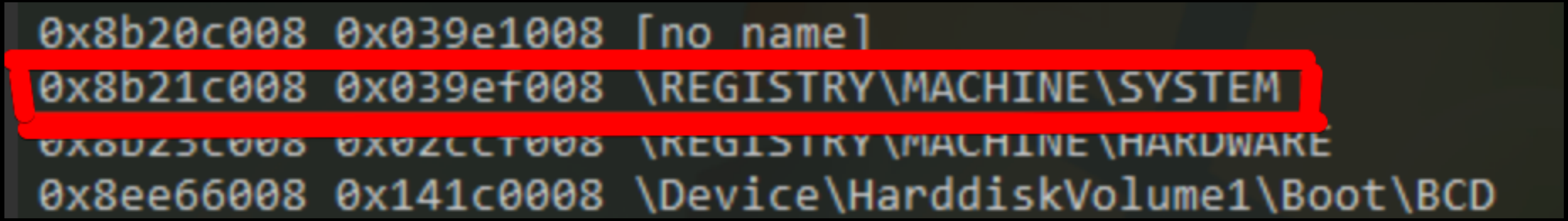
크기:	512MB (536,870,912 바이트)
디스크 할당 크기:	512MB (536,870,912 바이트)

Cmder



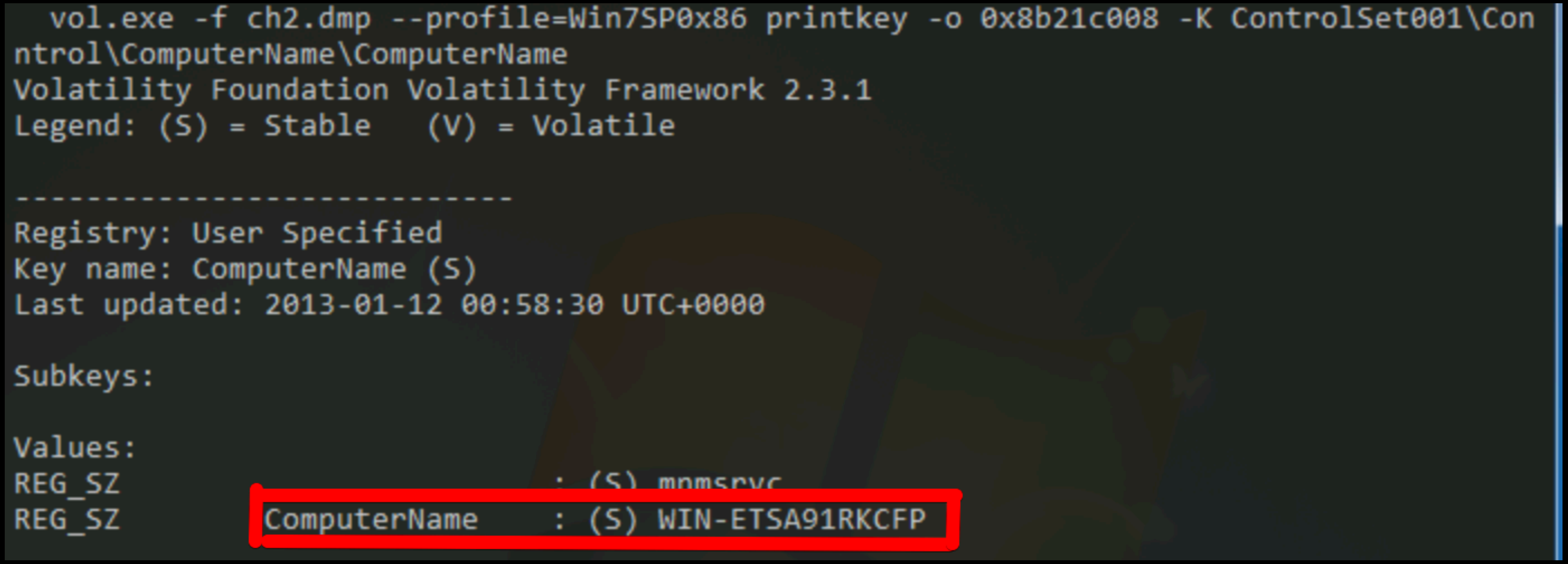
```
  vol.exe -f ch2.dmp imageinfo
Volatility Foundation Volatility Framework 2.3.1
Determining profile based on KDBG search...

          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS
                     AS Layer2 : FileAddressSpace (C:\Users\Lo
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82929be8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x8292ac00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2013-01-12 16:59:18 UTC+0000
     Image local date and time : 2013-01-12 17:59:18 +0100
```

Check the registry hive system address in memory



```
0x8b20c008 0x039e1008 [no name]
0x8b21c008 0x039ef008 \REGISTRY\MACHINE\SYSTEM
0x8b23c008 0x02ccf008 \REGISTRY\MACHINE\HARDWARE
0x8ee66008 0x141c0008 \Device\HarddiskVolume1\Boot\BCD
```

Hostname with registry analysis



```
  vol.exe -f ch2.dmp --profile=Win7SP0x86 printkey -o 0x8b21c008 -K ControlSet001\Con
ntrol\ComputerName\ComputerName
Volatility Foundation Volatility Framework 2.3.1
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: User Specified
Key name: ComputerName (S)
Last updated: 2013-01-12 00:58:30 UTC+0000

Subkeys:

Values:
REG_SZ                          : (S) mnmsrvc
REG_SZ       ComputerName       : (S) WIN-ETSA91RKCFP
```