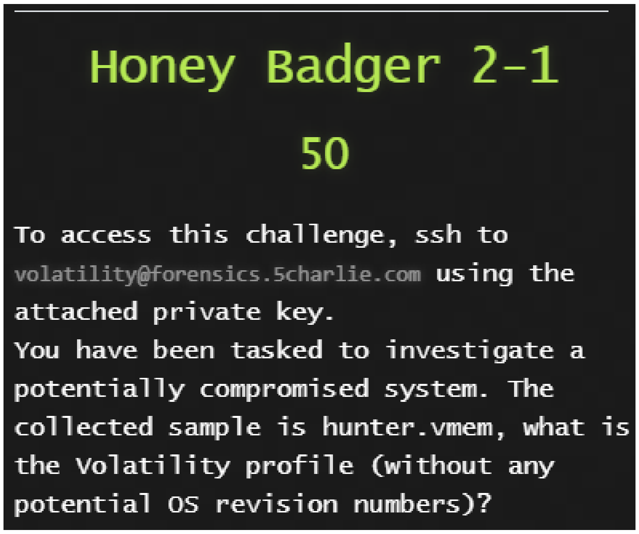


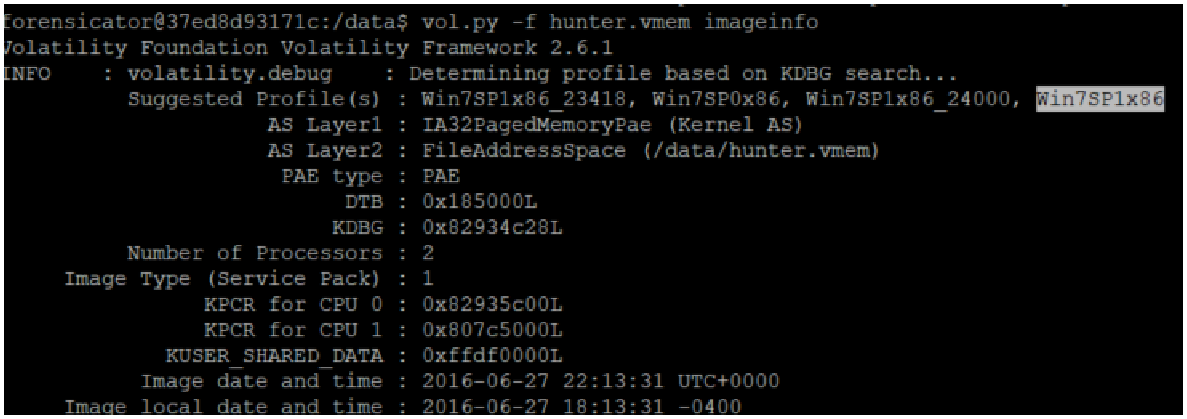
Honey Badger 2-1

50

To access this challenge, ssh to volatility@forensics.5charlie.com using the attached private key.
You have been tasked to investigate a potentially compromised system. The collected sample is hunter.vmem, what is the Volatility profile (without any potential OS revision numbers)?

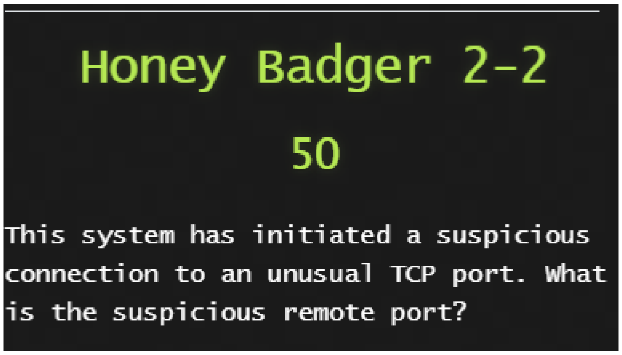
Pull the imageinfo off the file:

vol.py -f hunter.vmem imageinfo



```
forensicator@37ed8d93171c:/data$ vol.py -f hunter.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/data/hunter.vmem)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82934c28L
          Number of Processors : 2
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x82935c00L
                KPCR for CPU 1 : 0x807c5000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2016-06-27 22:13:31 UTC+0000
     Image local date and time : 2016-06-27 18:13:31 -0400
```

Flag: Win7SP1x86

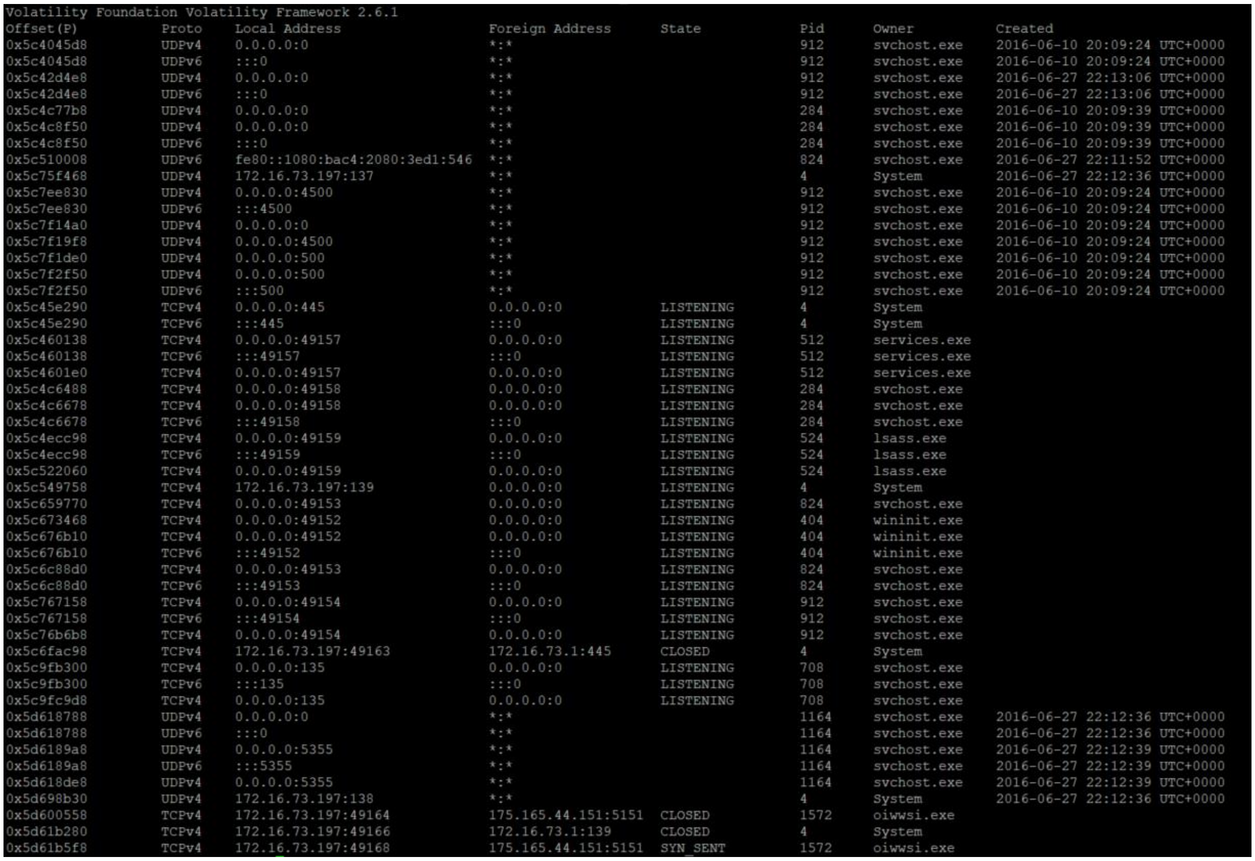


Honey Badger 2-2

50

This system has initiated a suspicious connection to an unusual TCP port. What is the suspicious remote port?

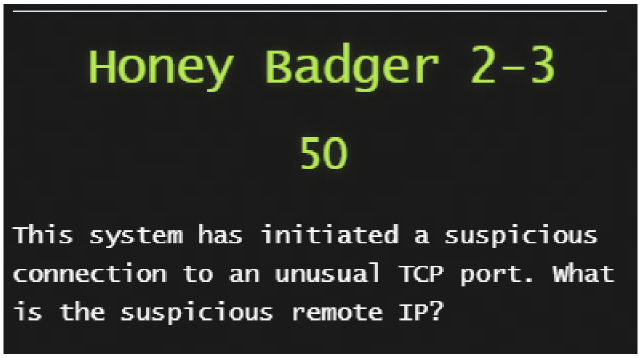
Run the following to get a list of connections: vol.py -f hunter.vmem --profile=Win7SP1x86_24000 netscan



```
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x5c4045d8         UDPv4    0.0.0.0:0                      *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c4045d8         UDPv6    :::0                           *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c42d4e8         UDPv4    0.0.0.0:0                      *:*                                   912      svchost.exe    2016-06-27 22:13:06 UTC+0000
0x5c42d4e8         UDPv6    :::0                           *:*                                   912      svchost.exe    2016-06-27 22:13:06 UTC+0000
0x5c4c77b8         UDPv4    0.0.0.0:0                      *:*                                   284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c4c8f50         UDPv4    0.0.0.0:0                      *:*                                   284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c4c8f50         UDPv6    :::0                           *:*                                   284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c510008         UDPv6    fe80::1080:bac4:2080:3ed1:546  *:*                                   824      svchost.exe    2016-06-27 22:11:52 UTC+0000
0x5c75f468         UDPv4    172.16.73.197:137              *:*                                   4        System         2016-06-27 22:12:36 UTC+0000
0x5c7ee830         UDPv4    0.0.0.0:4500                   *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7ee830         UDPv6    :::4500                        *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f14a0         UDPv4    0.0.0.0:0                      *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f19f8         UDPv4    0.0.0.0:4500                   *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f1de0         UDPv4    0.0.0.0:500                    *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f2f50         UDPv4    0.0.0.0:500                    *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f2f50         UDPv6    :::500                         *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c45e290         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING        4        System
0x5c45e290         TCPv6    :::445                         :::0                 LISTENING        4        System
0x5c460138         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING        512      services.exe
0x5c460138         TCPv6    :::49157                       :::0                 LISTENING        512      services.exe
0x5c4601e0         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING        512      services.exe
0x5c4c6488         TCPv4    0.0.0.0:49158                  0.0.0.0:0            LISTENING        284      svchost.exe
0x5c4c6678         TCPv4    0.0.0.0:49158                  0.0.0.0:0            LISTENING        284      svchost.exe
0x5c4c6678         TCPv6    :::49158                       :::0                 LISTENING        284      svchost.exe
0x5c4ecc98         TCPv4    0.0.0.0:49159                  0.0.0.0:0            LISTENING        524      lsass.exe
0x5c4ecc98         TCPv6    :::49159                       :::0                 LISTENING        524      lsass.exe
0x5c522060         TCPv4    0.0.0.0:49159                  0.0.0.0:0            LISTENING        524      lsass.exe
0x5c549758         TCPv4    172.16.73.197:139              0.0.0.0:0            LISTENING        4        System
0x5c659770         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        824      svchost.exe
0x5c673468         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        404      wininit.exe
0x5c676b10         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        404      wininit.exe
0x5c676b10         TCPv6    :::49152                       :::0                 LISTENING        404      wininit.exe
0x5c6c88d0         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING        824      svchost.exe
0x5c6c88d0         TCPv6    :::49153                       :::0                 LISTENING        824      svchost.exe
0x5c767158         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        912      svchost.exe
0x5c767158         TCPv6    :::49154                       :::0                 LISTENING        912      svchost.exe
0x5c76b6b8         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        912      svchost.exe
0x5c6fac98         TCPv4    172.16.73.197:49163            172.16.73.1:445      CLOSED           4        System
0x5c9fb300         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        708      svchost.exe
0x5c9fb300         TCPv6    :::135                         :::0                 LISTENING        708      svchost.exe
0x5c9fc9d8         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING        708      svchost.exe
0x5d618788         UDPv4    0.0.0.0:0                      *:*                                   1164     svchost.exe    2016-06-27 22:12:36 UTC+0000
0x5d618788         UDPv6    :::0                           *:*                                   1164     svchost.exe    2016-06-27 22:12:36 UTC+0000
0x5d6189a8         UDPv4    0.0.0.0:5355                   *:*                                   1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d6189a8         UDPv6    :::5355                        *:*                                   1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d618de8         UDPv4    0.0.0.0:5355                   *:*                                   1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d698b30         UDPv4    172.16.73.197:138              *:*                                   4        System         2016-06-27 22:12:36 UTC+0000
0x5d600558         TCPv4    172.16.73.197:49164            175.165.44.151:5151  CLOSED           1572     oiwwsi.exe
0x5d61b280         TCPv4    172.16.73.197:49166            172.16.73.1:139      CLOSED           4        System
0x5d61b5f8         TCPv4    172.16.73.197:49168            175.165.44.151:5151  SYN_SENT         1572     oiwwsi.exe
```

We see the .exe at the bottom connected to a nonstandard ip and port.

Flag: 5151

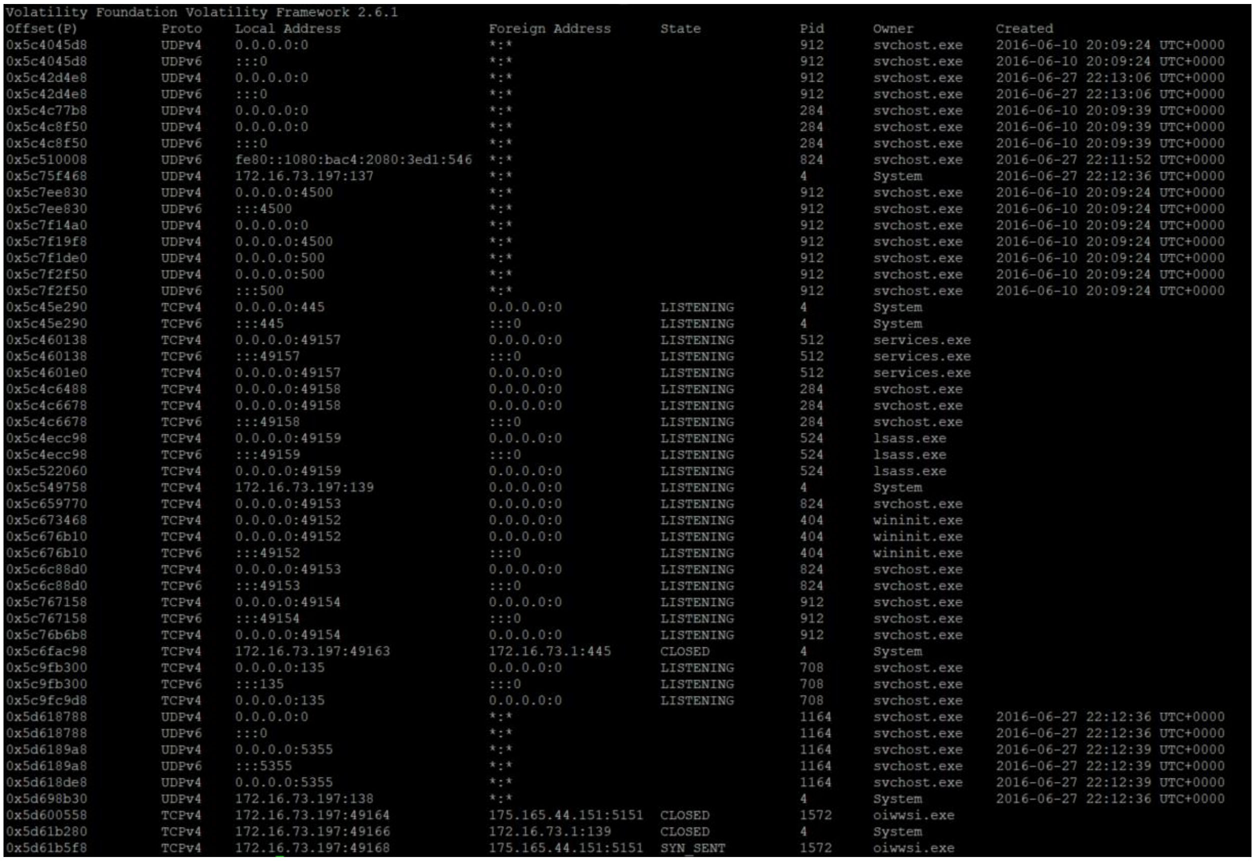


Honey Badger 2-3

50

This system has initiated a suspicious connection to an unusual TCP port. What is the suspicious remote IP?

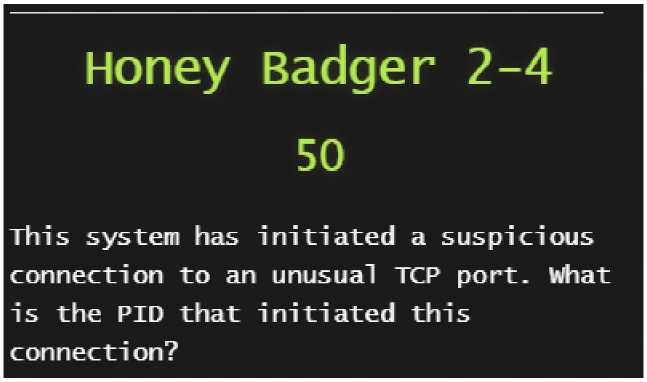
vol.py -f hunter.vmem --profile=Win7SP1x86_24000 netscan



```
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                      Foreign Address      State            Pid      Owner          Created
0x5c4045d8         UDPv4    0.0.0.0:0                          *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c4045d8         UDPv6    :::0                               *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c42d4e8         UDPv4    0.0.0.0:0                          *:*                                   912      svchost.exe    2016-06-27 22:13:06 UTC+0000
0x5c42d4e8         UDPv6    :::0                               *:*                                   912      svchost.exe    2016-06-27 22:13:06 UTC+0000
0x5c4c77b8         UDPv4    0.0.0.0:0                          *:*                                   284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c4c8f50         UDPv4    0.0.0.0:0                          *:*                                   284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c4c8f50         UDPv6    :::0                               *:*                                   284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c510008         UDPv6    fe80::1080:bac4:2080:3ed1:546      *:*                                   824      svchost.exe    2016-06-27 22:11:52 UTC+0000
0x5c75f468         UDPv4    172.16.73.197:137                  *:*                                   4        System         2016-06-27 22:12:36 UTC+0000
0x5c7ee830         UDPv4    0.0.0.0:4500                       *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7ee830         UDPv6    :::4500                            *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f14a0         UDPv4    0.0.0.0:0                          *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f19f8         UDPv4    0.0.0.0:4500                       *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f1de0         UDPv4    0.0.0.0:500                        *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f2f50         UDPv4    0.0.0.0:500                        *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f2f50         UDPv6    :::500                             *:*                                   912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c45e290         TCPv4    0.0.0.0:445                        0.0.0.0:0            LISTENING        4        System
0x5c45e290         TCPv6    :::445                             :::0                 LISTENING        4        System
0x5c460138         TCPv4    0.0.0.0:49157                      0.0.0.0:0            LISTENING        512      services.exe
0x5c460138         TCPv6    :::49157                           :::0                 LISTENING        512      services.exe
0x5c4601e0         TCPv4    0.0.0.0:49157                      0.0.0.0:0            LISTENING        512      services.exe
0x5c4c6488         TCPv4    0.0.0.0:49158                      0.0.0.0:0            LISTENING        284      svchost.exe
0x5c4c6678         TCPv4    0.0.0.0:49158                      0.0.0.0:0            LISTENING        284      svchost.exe
0x5c4c6678         TCPv6    :::49158                           :::0                 LISTENING        284      svchost.exe
0x5c4ecc98         TCPv4    0.0.0.0:49159                      0.0.0.0:0            LISTENING        524      lsass.exe
0x5c4ecc98         TCPv6    :::49159                           :::0                 LISTENING        524      lsass.exe
0x5c522060         TCPv4    0.0.0.0:49159                      0.0.0.0:0            LISTENING        524      lsass.exe
0x5c549758         TCPv4    172.16.73.197:139                  0.0.0.0:0            LISTENING        4        System
0x5c659770         TCPv4    0.0.0.0:49153                      0.0.0.0:0            LISTENING        824      svchost.exe
0x5c673468         TCPv4    0.0.0.0:49152                      0.0.0.0:0            LISTENING        404      wininit.exe
0x5c676b10         TCPv4    0.0.0.0:49152                      0.0.0.0:0            LISTENING        404      wininit.exe
0x5c676b10         TCPv6    :::49152                           :::0                 LISTENING        404      wininit.exe
0x5c6c88d0         TCPv4    0.0.0.0:49153                      0.0.0.0:0            LISTENING        824      svchost.exe
0x5c6c88d0         TCPv6    :::49153                           :::0                 LISTENING        824      svchost.exe
0x5c767158         TCPv4    0.0.0.0:49154                      0.0.0.0:0            LISTENING        912      svchost.exe
0x5c767158         TCPv6    :::49154                           :::0                 LISTENING        912      svchost.exe
0x5c76b6b8         TCPv4    0.0.0.0:49154                      0.0.0.0:0            LISTENING        912      svchost.exe
0x5c6fac98         TCPv4    172.16.73.197:49163                172.16.73.1:445      CLOSED           4        System
0x5c9fb300         TCPv4    0.0.0.0:135                        0.0.0.0:0            LISTENING        708      svchost.exe
0x5c9fb300         TCPv6    :::135                             :::0                 LISTENING        708      svchost.exe
0x5c9fc9d8         TCPv4    0.0.0.0:135                        0.0.0.0:0            LISTENING        708      svchost.exe
0x5d618788         UDPv4    0.0.0.0:0                          *:*                                   1164     svchost.exe    2016-06-27 22:12:36 UTC+0000
0x5d618788         UDPv6    :::0                               *:*                                   1164     svchost.exe    2016-06-27 22:12:36 UTC+0000
0x5d6189a8         UDPv4    0.0.0.0:5355                       *:*                                   1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d6189a8         UDPv6    :::5355                            *:*                                   1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d618de8         UDPv4    0.0.0.0:5355                       *:*                                   1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d698b30         UDPv4    172.16.73.197:138                  *:*                                   4        System         2016-06-27 22:12:36 UTC+0000
0x5d600558         TCPv4    172.16.73.197:49164                175.165.44.151:5151  CLOSED           1572     oiwwsi.exe
0x5d61b280         TCPv4    172.16.73.197:49166                172.16.73.1:139      CLOSED           4        System
0x5d61b5f8         TCPv4    172.16.73.197:49168                175.165.44.151:5151  SYN_SENT         1572     oiwwsi.exe
```

IP of the previous question.

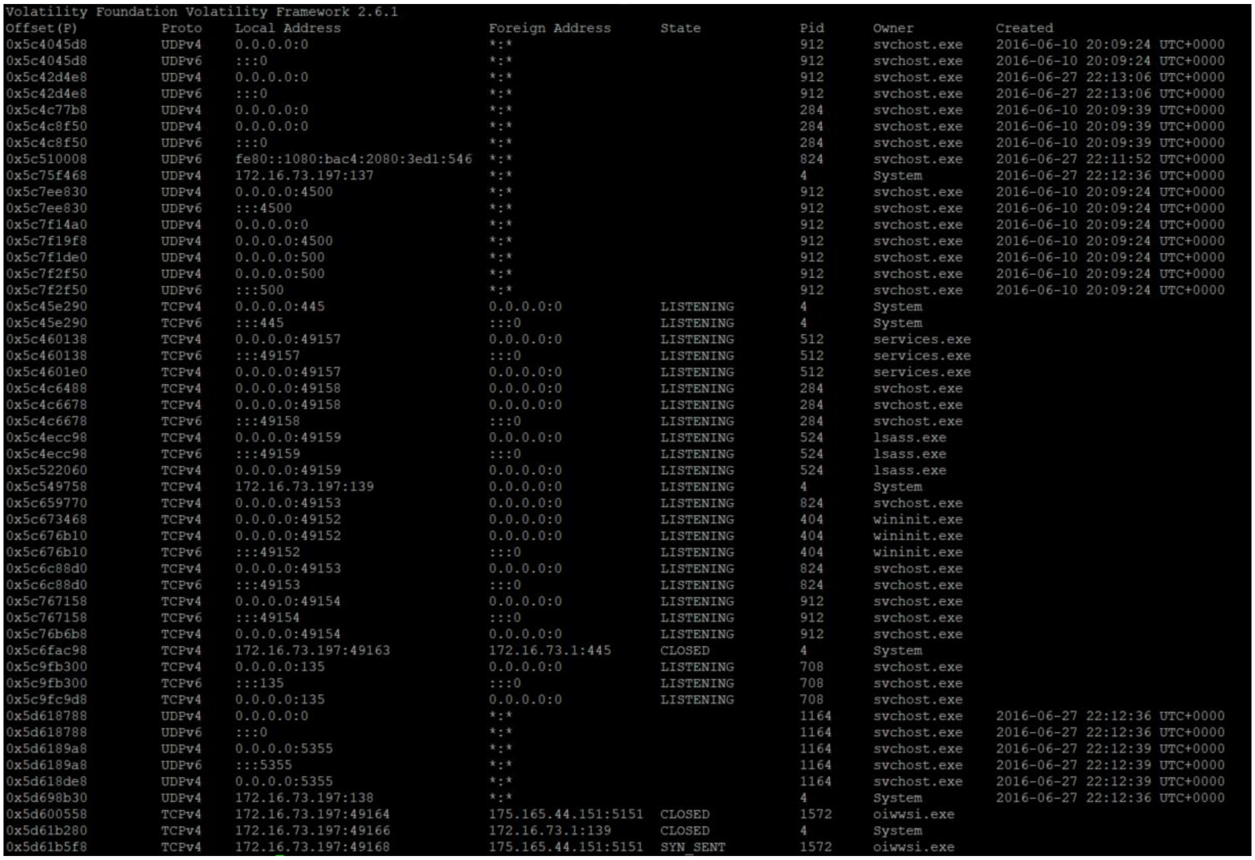
Flag: 175.165.44.151



Honey Badger 2-4

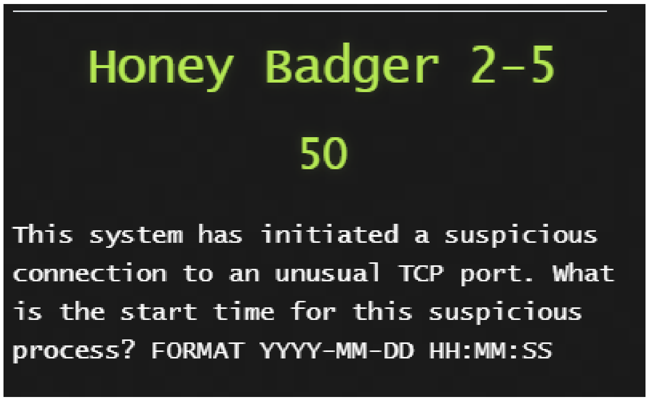
50

This system has initiated a suspicious connection to an unusual TCP port. What is the PID that initiated this connection?



```
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Proto    Local Address                  Foreign Address      State           Pid      Owner          Created
0x5c4045d8         UDPv4    0.0.0.0:0                      *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c4045d8         UDPv6    :::0                           *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c42d4e8         UDPv4    0.0.0.0:0                      *:*                                  912      svchost.exe    2016-06-27 22:13:06 UTC+0000
0x5c42d4e8         UDPv6    :::0                           *:*                                  912      svchost.exe    2016-06-27 22:13:06 UTC+0000
0x5c4c77b8         UDPv4    0.0.0.0:0                      *:*                                  284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c4c8f50         UDPv4    0.0.0.0:0                      *:*                                  284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c4c8f50         UDPv6    :::0                           *:*                                  284      svchost.exe    2016-06-10 20:09:39 UTC+0000
0x5c510008         UDPv6    fe80::1080:bac4:2080:3ed1:546  *:*                                  824      svchost.exe    2016-06-27 22:11:52 UTC+0000
0x5c75f468         UDPv4    172.16.73.197:137              *:*                                  4        System         2016-06-27 22:12:36 UTC+0000
0x5c7ee830         UDPv4    0.0.0.0:4500                   *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7ee830         UDPv6    :::4500                        *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f14a0         UDPv4    0.0.0.0:0                      *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f19f8         UDPv4    0.0.0.0:4500                   *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f1de0         UDPv4    0.0.0.0:500                    *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f2f50         UDPv4    0.0.0.0:500                    *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c7f2f50         UDPv6    :::500                         *:*                                  912      svchost.exe    2016-06-10 20:09:24 UTC+0000
0x5c45e290         TCPv4    0.0.0.0:445                    0.0.0.0:0            LISTENING       4        System
0x5c45e290         TCPv6    :::445                         :::0                 LISTENING       4        System
0x5c460138         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING       512      services.exe
0x5c460138         TCPv6    :::49157                       :::0                 LISTENING       512      services.exe
0x5c4601e0         TCPv4    0.0.0.0:49157                  0.0.0.0:0            LISTENING       512      services.exe
0x5c4c6488         TCPv4    0.0.0.0:49158                  0.0.0.0:0            LISTENING       284      svchost.exe
0x5c4c6678         TCPv4    0.0.0.0:49158                  0.0.0.0:0            LISTENING       284      svchost.exe
0x5c4c6678         TCPv6    :::49158                       :::0                 LISTENING       284      svchost.exe
0x5c4ecc98         TCPv4    0.0.0.0:49159                  0.0.0.0:0            LISTENING       524      lsass.exe
0x5c4ecc98         TCPv6    :::49159                       :::0                 LISTENING       524      lsass.exe
0x5c522060         TCPv4    0.0.0.0:49159                  0.0.0.0:0            LISTENING       524      lsass.exe
0x5c549758         TCPv4    172.16.73.197:139              0.0.0.0:0            LISTENING       4        System
0x5c659770         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING       824      svchost.exe
0x5c673468         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING       404      wininit.exe
0x5c676b10         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING       404      wininit.exe
0x5c676b10         TCPv6    :::49152                       :::0                 LISTENING       404      wininit.exe
0x5c6c88d0         TCPv4    0.0.0.0:49153                  0.0.0.0:0            LISTENING       824      svchost.exe
0x5c6c88d0         TCPv6    :::49153                       :::0                 LISTENING       824      svchost.exe
0x5c767158         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING       912      svchost.exe
0x5c767158         TCPv6    :::49154                       :::0                 LISTENING       912      svchost.exe
0x5c76b6b8         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING       912      svchost.exe
0x5c6fac98         TCPv4    172.16.73.197:49163            172.16.73.1:445      CLOSED          4        System
0x5c9fb300         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING       708      svchost.exe
0x5c9fb300         TCPv6    :::135                         :::0                 LISTENING       708      svchost.exe
0x5c9fc9d8         TCPv4    0.0.0.0:135                    0.0.0.0:0            LISTENING       708      svchost.exe
0x5d618788         UDPv4    0.0.0.0:0                      *:*                                  1164     svchost.exe    2016-06-27 22:12:36 UTC+0000
0x5d618788         UDPv6    :::0                           *:*                                  1164     svchost.exe    2016-06-27 22:12:36 UTC+0000
0x5d6189a8         UDPv4    0.0.0.0:5355                   *:*                                  1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d6189a8         UDPv6    :::5355                        *:*                                  1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d618de8         UDPv4    0.0.0.0:5355                   *:*                                  1164     svchost.exe    2016-06-27 22:12:39 UTC+0000
0x5d698b30         UDPv4    172.16.73.197:138              *:*                                  4        System         2016-06-27 22:12:36 UTC+0000
0x5d600558         TCPv4    172.16.73.197:49164            175.165.44.151:5151  CLOSED          1572     oiwwsi.exe
0x5d61b280         TCPv4    172.16.73.197:49166            172.16.73.1:139      CLOSED          4        System
0x5d61b5f8         TCPv4    172.16.73.197:49168            175.165.44.151:5151  SYN_SENT        1572     oiwwsi.exe
```

Flag: 1572



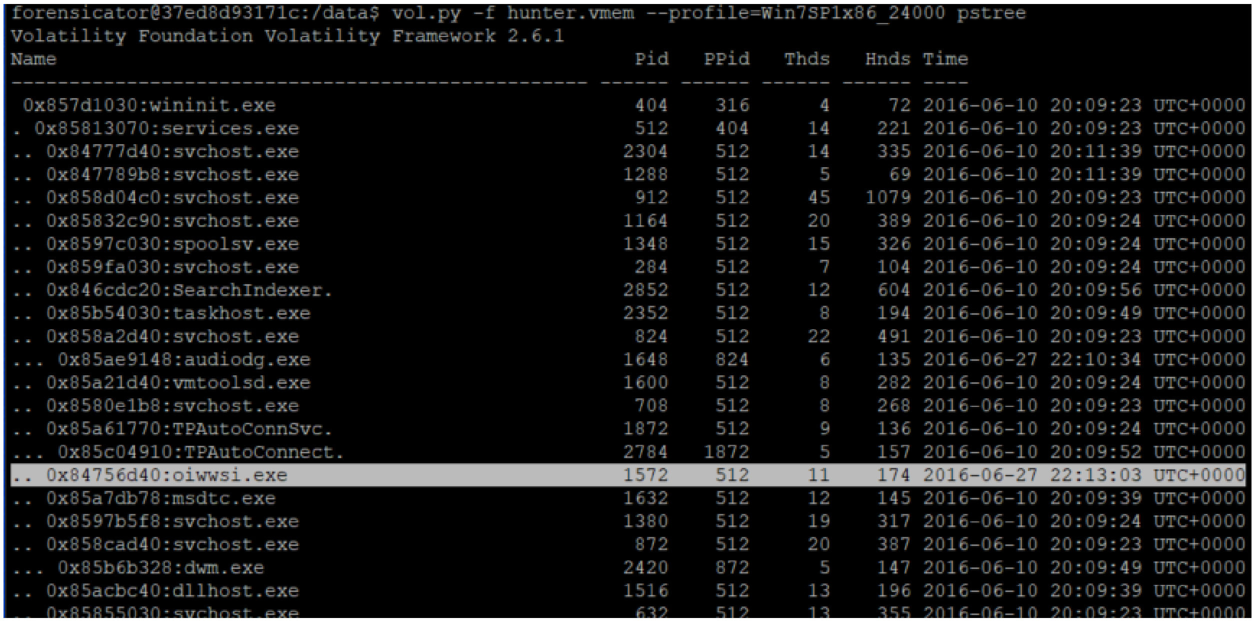
Honey Badger 2-5

50

This system has initiated a suspicious connection to an unusual TCP port. What is the start time for this suspicious process? FORMAT YYYY-MM-DD HH:MM:SS

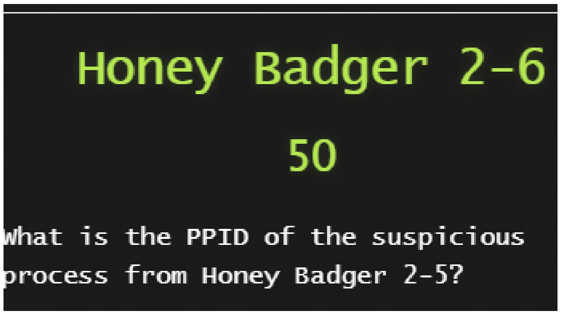
We need to look at the pstree for pid 1572

vol.py -f hunter.vmem --profile=Win7SP1x86_24000 pstree



```
forensicator@37ed8d93171c:/data$ vol.py -f hunter.vmem --profile=Win7SP1x86_24000 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x857d1030:wininit.exe                               404    316      4     72 2016-06-10 20:09:23 UTC+0000
. 0x85813070:services.exe                             512    404     14    221 2016-06-10 20:09:23 UTC+0000
.. 0x84777d40:svchost.exe                            2304    512     14    335 2016-06-10 20:11:39 UTC+0000
.. 0x847789b8:svchost.exe                            1288    512      5     69 2016-06-10 20:11:39 UTC+0000
.. 0x858d04c0:svchost.exe                             912    512     45   1079 2016-06-10 20:09:23 UTC+0000
.. 0x85832c90:svchost.exe                            1164    512     20    389 2016-06-10 20:09:24 UTC+0000
.. 0x8597c030:spoolsv.exe                            1348    512     15    326 2016-06-10 20:09:24 UTC+0000
.. 0x859fa030:svchost.exe                             284    512      7    104 2016-06-10 20:09:24 UTC+0000
.. 0x846cdc20:SearchIndexer.                         2852    512     12    604 2016-06-10 20:09:56 UTC+0000
.. 0x85b54030:taskhost.exe                           2352    512      8    194 2016-06-10 20:09:49 UTC+0000
.. 0x858a2d40:svchost.exe                             824    512     22    491 2016-06-10 20:09:23 UTC+0000
... 0x85ae9148:audiodg.exe                           1648    824      6    135 2016-06-27 22:10:34 UTC+0000
.. 0x85a21d40:vmtoolsd.exe                           1600    512      8    282 2016-06-10 20:09:24 UTC+0000
.. 0x8580e1b8:svchost.exe                             708    512      8    268 2016-06-10 20:09:23 UTC+0000
.. 0x85a61770:TPAutoConnSvc.                         1872    512      9    136 2016-06-10 20:09:24 UTC+0000
... 0x85c04910:TPAutoConnect.                        2784   1872      5    157 2016-06-10 20:09:52 UTC+0000
.. 0x84756d40:oiwwsi.exe                             1572    512     11    174 2016-06-27 22:13:03 UTC+0000
.. 0x85a7db78:msdtc.exe                              1632    512     12    145 2016-06-10 20:09:39 UTC+0000
.. 0x8597b5f8:svchost.exe                            1380    512     19    317 2016-06-10 20:09:24 UTC+0000
.. 0x858cad40:svchost.exe                             872    512     20    387 2016-06-10 20:09:23 UTC+0000
... 0x85b6b328:dwm.exe                               2420    872      5    147 2016-06-10 20:09:49 UTC+0000
.. 0x85acbc40:dllhost.exe                            1516    512     13    196 2016-06-10 20:09:39 UTC+0000
.. 0x85855030:svchost.exe                             632    512     13    355 2016-06-10 20:09:23 UTC+0000
```

Flag: 2016-06-27 22:13:03

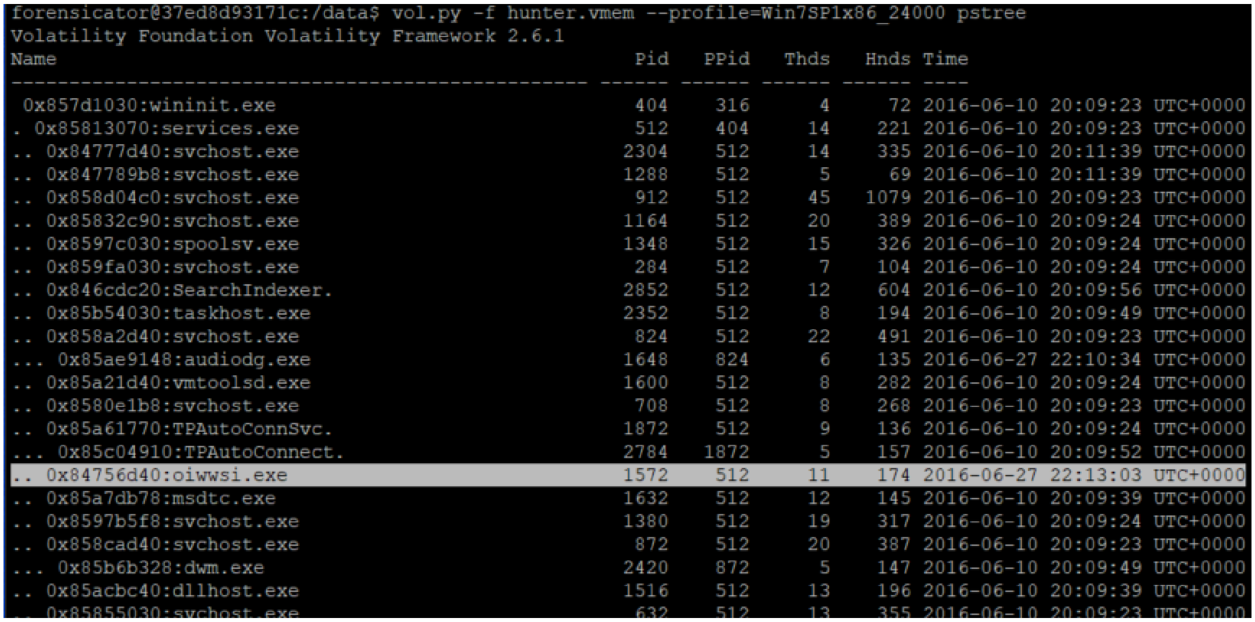


Honey Badger 2-6

50

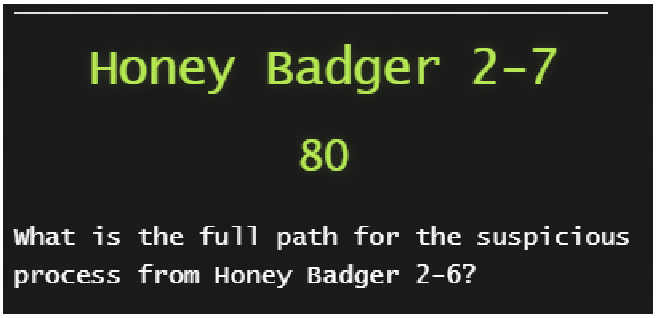
What is the PPID of the suspicious process from Honey Badger 2-5?

vol.py -f hunter.vmem --profile=Win7SP1x86_24000 pstree



```
forensicator@37ed8d93171c:/data$ vol.py -f hunter.vmem --profile=Win7SP1x86_24000 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x857d1030:wininit.exe                                404    316      4     72 2016-06-10 20:09:23 UTC+0000
. 0x85813070:services.exe                              512    404     14    221 2016-06-10 20:09:23 UTC+0000
.. 0x84777d40:svchost.exe                             2304    512     14    335 2016-06-10 20:11:39 UTC+0000
.. 0x847789b8:svchost.exe                             1288    512      5     69 2016-06-10 20:11:39 UTC+0000
.. 0x858d04c0:svchost.exe                              912    512     45   1079 2016-06-10 20:09:23 UTC+0000
.. 0x85832c90:svchost.exe                             1164    512     20    389 2016-06-10 20:09:24 UTC+0000
.. 0x8597c030:spoolsv.exe                             1348    512     15    326 2016-06-10 20:09:24 UTC+0000
.. 0x859fa030:svchost.exe                              284    512      7    104 2016-06-10 20:09:24 UTC+0000
.. 0x846cdc20:SearchIndexer.                          2852    512     12    604 2016-06-10 20:09:56 UTC+0000
.. 0x85b54030:taskhost.exe                            2352    512      8    194 2016-06-10 20:09:49 UTC+0000
.. 0x858a2d40:svchost.exe                              824    512     22    491 2016-06-10 20:09:23 UTC+0000
... 0x85ae9148:audiodg.exe                            1648    824      6    135 2016-06-27 22:10:34 UTC+0000
.. 0x85a21d40:vmtoolsd.exe                            1600    512      8    282 2016-06-10 20:09:24 UTC+0000
.. 0x8580e1b8:svchost.exe                              708    512      8    268 2016-06-10 20:09:23 UTC+0000
.. 0x85a61770:TPAutoConnSvc.                          1872    512      9    136 2016-06-10 20:09:24 UTC+0000
... 0x85c04910:TPAutoConnect.                         2784   1872      5    157 2016-06-10 20:09:52 UTC+0000
.. 0x84756d40:oiwwsi.exe                              1572    512     11    174 2016-06-27 22:13:03 UTC+0000
.. 0x85a7db78:msdtc.exe                               1632    512     12    145 2016-06-10 20:09:39 UTC+0000
.. 0x8597b5f8:svchost.exe                             1380    512     19    317 2016-06-10 20:09:24 UTC+0000
.. 0x858cad40:svchost.exe                              872    512     20    387 2016-06-10 20:09:23 UTC+0000
... 0x85b6b328:dwm.exe                                2420    872      5    147 2016-06-10 20:09:49 UTC+0000
.. 0x85acbc40:dllhost.exe                             1516    512     13    196 2016-06-10 20:09:39 UTC+0000
.. 0x85855030:svchost.exe                              632    512     13    355 2016-06-10 20:09:23 UTC+0000
```

Flag: 512



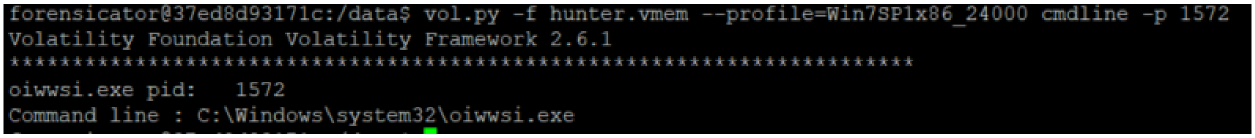
Honey Badger 2-7

80

What is the full path for the suspicious process from Honey Badger 2-6?

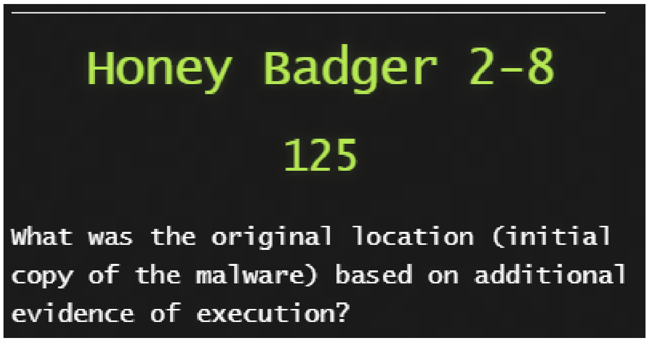
vol.py -f hunter.vmem --profile=Win7SP1x86_24000 cmdline -p 1572

this will tell us the command that was used to launch the process.



```
forensicator@37ed8d93171c:/data$ vol.py -f hunter.vmem --profile=Win7SP1x86_24000 cmdline -p 1572
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
oiwwsi.exe pid:   1572
Command line : C:\Windows\system32\oiwwsi.exe
```

Flag: C:\Windows\system32\oiwwsi.exe



Honey Badger 2-8

125

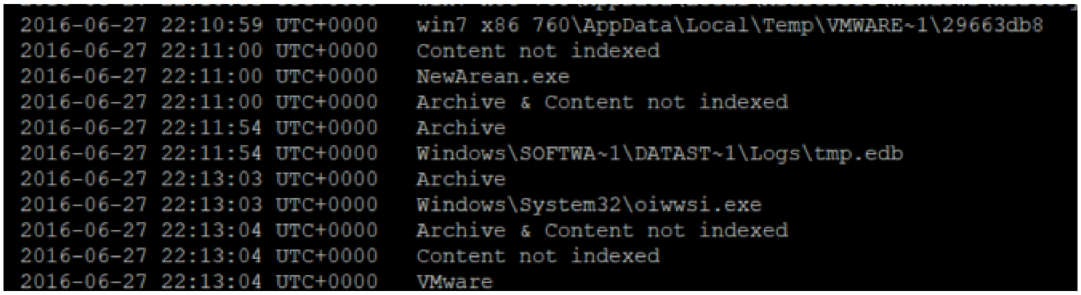
What was the original location (initial copy of the malware) based on additional evidence of execution?

For this question we want to follow a timeline of events on this, and this answer is not jumping out (Time Spent hunting this one down too long). But the hint said to follow GCFA processes, so we should look at file creation times. To get the file creation times lets create a file with all the mft data in this image.

vol.py -f hunter.vmem --profile=Win7SP1x86_24000 mftparser > /tmp/mft

Now that we have that created search for the oiwwsi.exe file, and we get a creation date of 2016-06-27 22:13:03

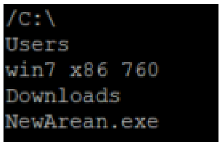
So now lets look for anything that happened on that day: cat /tmp/mft | grep "2016-06-27 22:" | sort -u



```
2016-06-27 22:10:59 UTC+0000   win7 x86 760\AppData\Local\Temp\VMWARE~1\29663db8
2016-06-27 22:11:00 UTC+0000   Content not indexed
2016-06-27 22:11:00 UTC+0000   NewArean.exe
2016-06-27 22:11:00 UTC+0000   Archive & Content not indexed
2016-06-27 22:11:54 UTC+0000   Archive
2016-06-27 22:11:54 UTC+0000   Windows\SOFTWA~1\DATAST~1\Logs\tmp.edb
2016-06-27 22:13:03 UTC+0000   Archive
2016-06-27 22:13:03 UTC+0000   Windows\System32\oiwwsi.exe
2016-06-27 22:13:04 UTC+0000   Archive & Content not indexed
2016-06-27 22:13:04 UTC+0000   Content not indexed
2016-06-27 22:13:04 UTC+0000   VMware
```

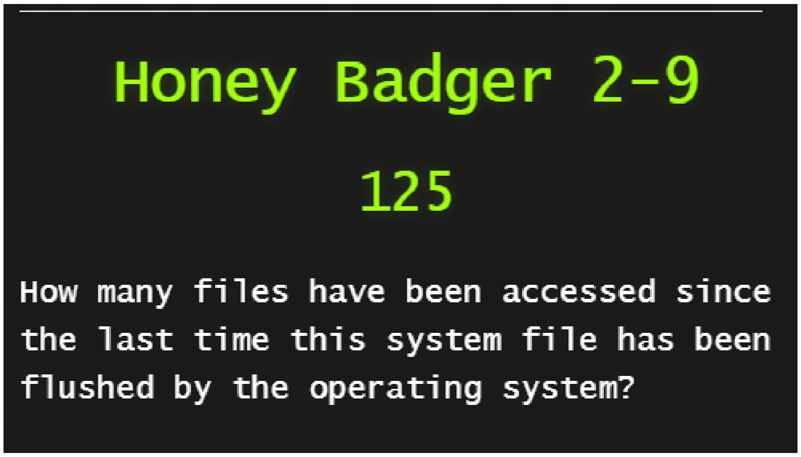
Now we have a file there @ 22:11:00 NewArean.exe we need to find the location of that file.

There is no easy way to find this other than to strings the image. strings hunter.vmem | grep -i NewArean -B 5



```
/C:\
Users
win7 x86 760
Downloads
NewArean.exe
```

Flag: C:\Users\win7 x86 760\Downloads\NewArean.exe

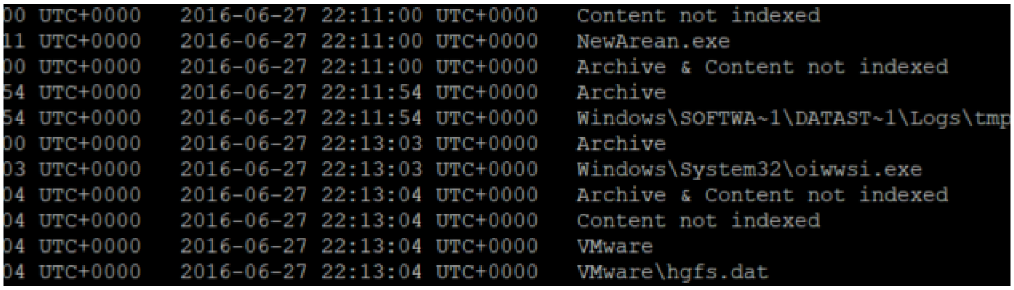


Honey Badger 2-9

125

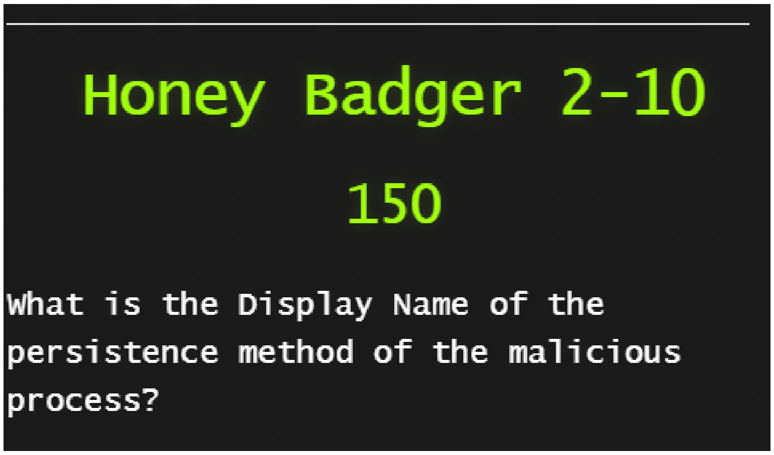
How many files have been accessed since the last time this system file has been flushed by the operating system?

cat /tmp/mft | grep "2016-06-27 22:" | sort -u



```
00 UTC+0000   2016-06-27 22:11:00 UTC+0000   Content not indexed
11 UTC+0000   2016-06-27 22:11:00 UTC+0000   NewArean.exe
00 UTC+0000   2016-06-27 22:11:00 UTC+0000   Archive & Content not indexed
54 UTC+0000   2016-06-27 22:11:54 UTC+0000   Archive
54 UTC+0000   2016-06-27 22:11:54 UTC+0000   Windows\SOFTWA~1\DATAST~1\Logs\tmp
00 UTC+0000   2016-06-27 22:13:03 UTC+0000   Archive
03 UTC+0000   2016-06-27 22:13:03 UTC+0000   Windows\System32\oiwwsi.exe
04 UTC+0000   2016-06-27 22:13:04 UTC+0000   Archive & Content not indexed
04 UTC+0000   2016-06-27 22:13:04 UTC+0000   Content not indexed
04 UTC+0000   2016-06-27 22:13:04 UTC+0000   VMware
04 UTC+0000   2016-06-27 22:13:04 UTC+0000   VMware\hgfs.dat
```

Flag: 12



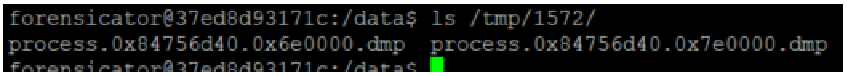
Honey Badger 2-10

150

What is the Display Name of the persistence method of the malicious process?

We are going to use malfind to dump the process files, but we need to make the dir to dump to first: mkdir /tmp/1572

vol.py -f hunter.vmem --profile=Win7SP1x86_24000 malfind -p 1572 --dump-dir=/tmp/1572/



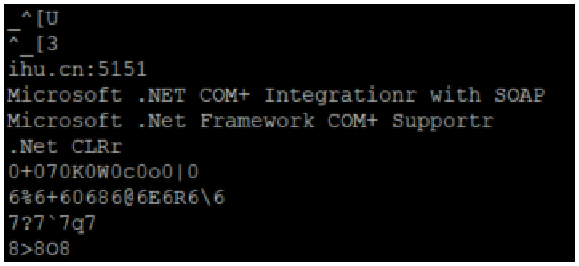
```
forensicator@37ed8d93171c:/data$ ls /tmp/1572/
process.0x84756d40.0x6e0000.dmp  process.0x84756d40.0x7e0000.dmp
forensicator@37ed8d93171c:/data$ 
```

Then run strings on the 2 files:

First file returns no strings

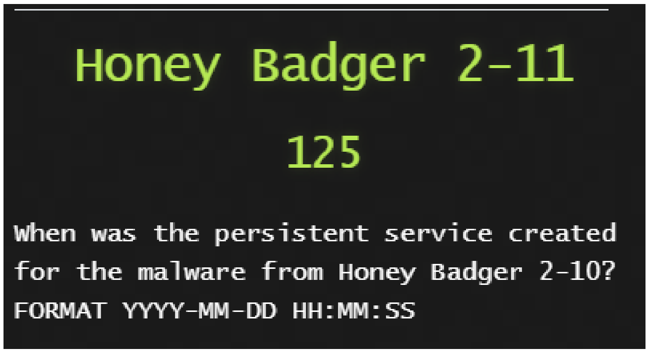
Second file strings

strings /tmp/1572/process.0x84756d40.0x7e0000.dmp



```
_^[U
^_[3
ihu.cn:5151
Microsoft .NET COM+ Integrationr with SOAP
Microsoft .Net Framework COM+ Supportr
.Net CLRr
0+070K0W0c0o0|0
6%6+60686@6E6R6\6
7?7`7q7
8>808
```

Flag: Microsoft .Net Framework COM+ Supportr



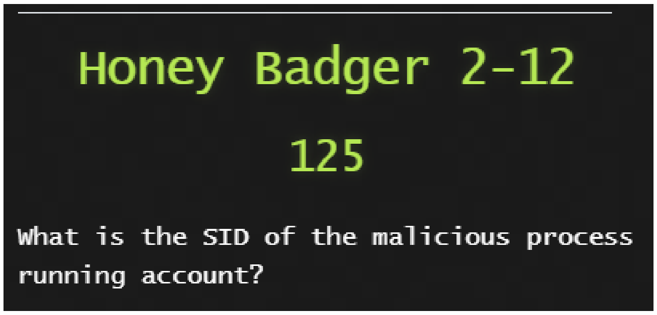
Honey Badger 2-11

125

When was the persistent service created for the malware from Honey Badger 2-10? FORMAT YYYY-MM-DD HH:MM:SS

Run pstree and look at pid 1572, oiwwsi.exe

Flag: 2016-06-27 22:13:03

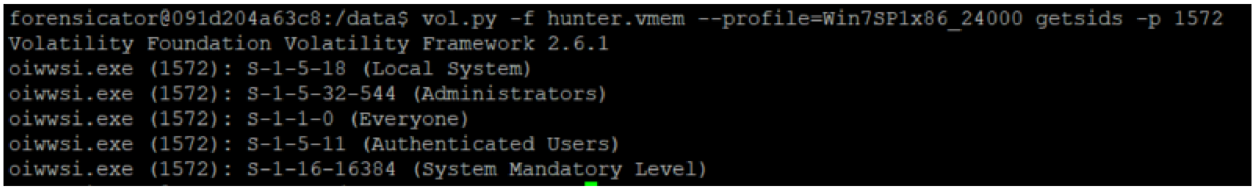


Honey Badger 2-12

125

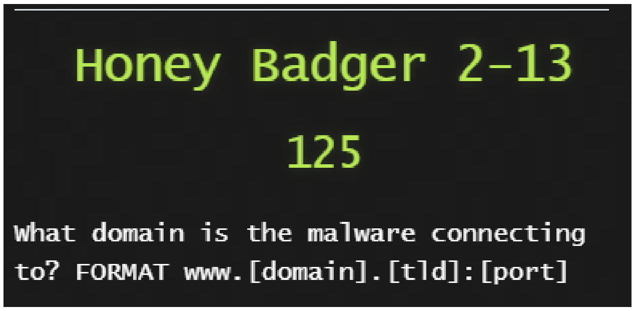
What is the SID of the malicious process running account?

vol.py -f hunter.vmem --profile=Win7SP1x86_24000 getsids -p 1572



```
forensicator@091d204a63c8:/data$ vol.py -f hunter.vmem --profile=Win7SP1x86_24000 getsids -p 1572
Volatility Foundation Volatility Framework 2.6.1
oiwwsi.exe (1572): S-1-5-18 (Local System)
oiwwsi.exe (1572): S-1-5-32-544 (Administrators)
oiwwsi.exe (1572): S-1-1-0 (Everyone)
oiwwsi.exe (1572): S-1-5-11 (Authenticated Users)
oiwwsi.exe (1572): S-1-16-16384 (System Mandatory Level)
```

Flag: S-1-5-18



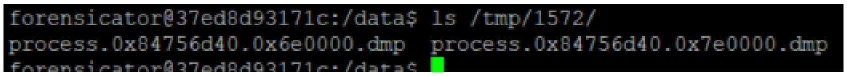
Honey Badger 2-13

125

What domain is the malware connecting to? FORMAT www.[domain].[tld]:[port]

We are going to use malfind to dump the process files, but we need to make the dir to dump to first: mkdir /tmp/1572

vol.py -f hunter.vmem --profile=Win7SP1x86_24000 malfind -p 1572 --dump-dir=/tmp/1572/



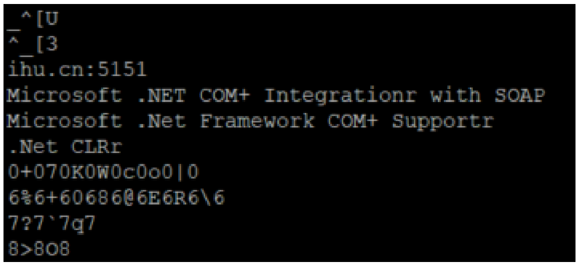
```
forensicator@37ed8d93171c:/data$ ls /tmp/1572/
process.0x84756d40.0x6e0000.dmp  process.0x84756d40.0x7e0000.dmp
forensicator@37ed8d93171c:/data$
```

Then run strings on the 2 files:

First file returns no strings

Second file strings

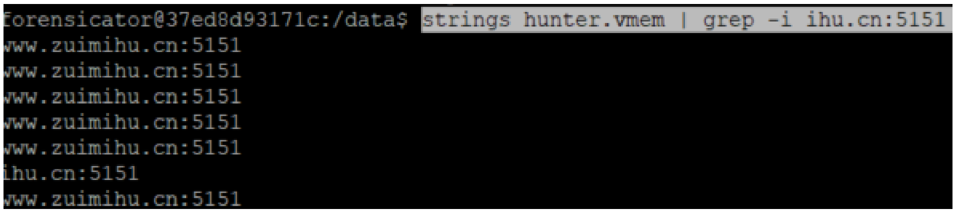
strings /tmp/1572/process.0x84756d40.0x7e0000.dmp



```
_^[U
^_[3
ihu.cn:5151
Microsoft .NET COM+ Integrationr with SOAP
Microsoft .Net Framework COM+ Supportr
.Net CLRr
0+070K0W0c0o0|0
6%6+60686@6E6R6\6
7?7`7q7
8>8O8
```

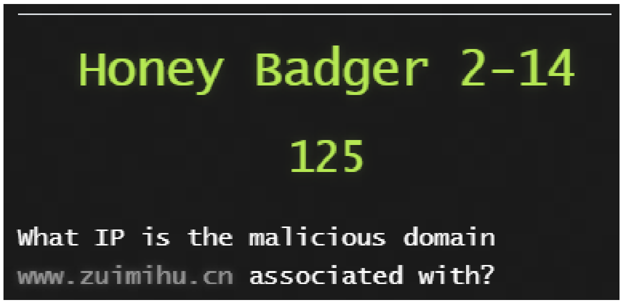
Next we need to find the full web address as that only seems to be a partial.

strings hunter.vmem | grep -i ihu.cn:5151



```
forensicator@37ed8d93171c:/data$ strings hunter.vmem | grep -i ihu.cn:5151
www.zuimihu.cn:5151
www.zuimihu.cn:5151
www.zuimihu.cn:5151
www.zuimihu.cn:5151
www.zuimihu.cn:5151
ihu.cn:5151
www.zuimihu.cn:5151
```

Flag: www.zuimihu.cn:5151



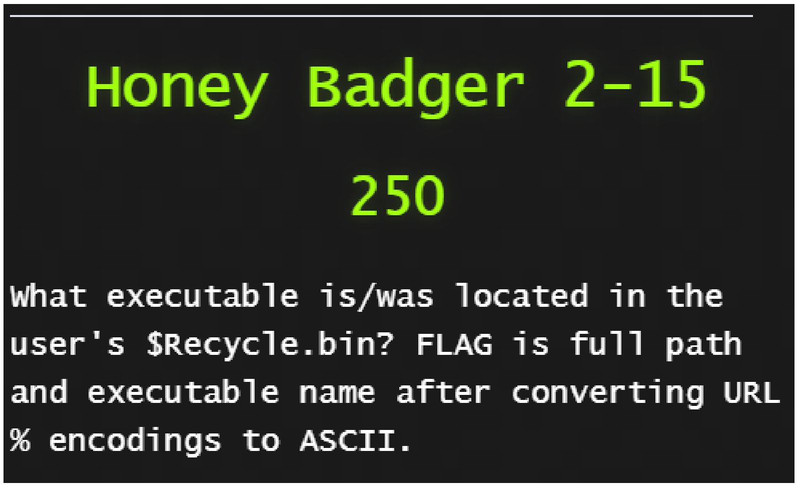
Honey Badger 2-14

125

What IP is the malicious domain www.zuimihu.cn associated with?

This goes back to 2-3 as we see the port 5151 again.

Flag: 175.165.44.151



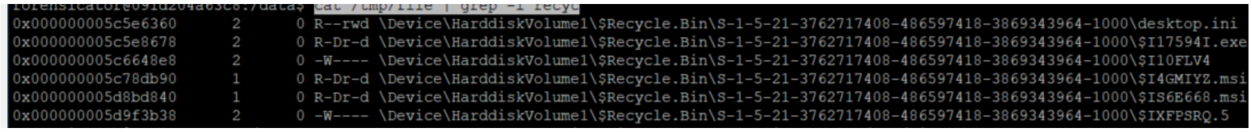
Honey Badger 2-15

250

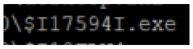
What executable is/was located in the user's $Recycle.bin? FLAG is full path and executable name after converting URL % encodings to ASCII.

First, we need to get a list of stuff in the recycle bin: vol.py -f hunter.vmem --profile=Win7SP1x86_24000 filescan > /tmp/file

cat /tmp/file | grep -i recyc

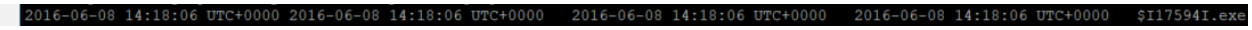


```
forensicator@091d204a63c8:/data$ cat /tmp/file | grep -i recyc
0x000000005c5e6360      2      0 R--rwd \Device\HarddiskVolume1\$Recycle.Bin\S-1-5-21-3762717408-486597418-3869343964-1000\desktop.ini
0x000000005c5e8678      2      0 R-Dr-d \Device\HarddiskVolume1\$Recycle.Bin\S-1-5-21-3762717408-486597418-3869343964-1000\$I17594I.exe
0x000000005c6648e8      2      0 -W---- \Device\HarddiskVolume1\$Recycle.Bin\S-1-5-21-3762717408-486597418-3869343964-1000\$I10FLV4
0x000000005c78db90      1      0 R-Dr-d \Device\HarddiskVolume1\$Recycle.Bin\S-1-5-21-3762717408-486597418-3869343964-1000\$I4GMIYZ.msi
0x000000005d8bd840      1      0 R-Dr-d \Device\HarddiskVolume1\$Recycle.Bin\S-1-5-21-3762717408-486597418-3869343964-1000\$IS6E668.msi
0x000000005d9f3b38      2      0 -W---- \Device\HarddiskVolume1\$Recycle.Bin\S-1-5-21-3762717408-486597418-3869343964-1000\$IXFPSRQ.5
```



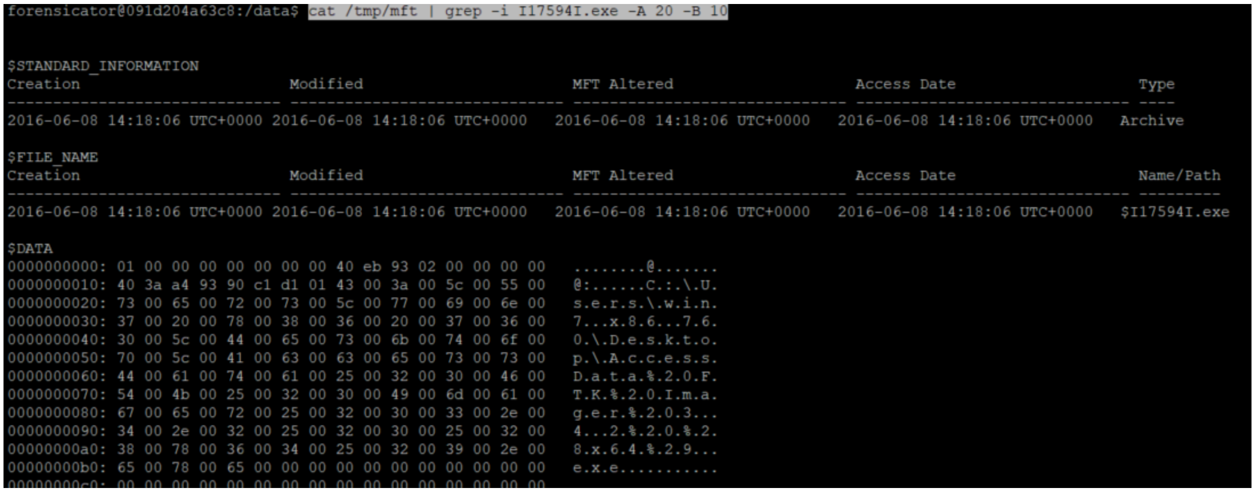
```
0\$I17594I.exe
```

Turn this over to the mft file: cat /tmp/mft | grep -i I17594I.exe



```
2016-06-08 14:18:06 UTC+0000 2016-06-08 14:18:06 UTC+0000   2016-06-08 14:18:06 UTC+0000   2016-06-08 14:18:06 UTC+0000   $I17594I.exe
```

Now let's look at the data around this: cat /tmp/mft | grep -i I17594I.exe -A 20 -B 10



```
forensicator@091d204a63c8:/data$ cat /tmp/mft | grep -i I17594I.exe -A 20 -B 10


$STANDARD_INFORMATION
Creation                       Modified                       MFT Altered                    Access Date                    Type
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----
2016-06-08 14:18:06 UTC+0000 2016-06-08 14:18:06 UTC+0000   2016-06-08 14:18:06 UTC+0000   2016-06-08 14:18:06 UTC+0000   Archive

$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ---------
2016-06-08 14:18:06 UTC+0000 2016-06-08 14:18:06 UTC+0000   2016-06-08 14:18:06 UTC+0000   2016-06-08 14:18:06 UTC+0000   $I17594I.exe

$DATA
0000000000: 01 00 00 00 00 00 00 00 40 eb 93 02 00 00 00 00   ........@.......
0000000010: 40 3a a4 93 90 c1 d1 01 43 00 3a 00 5c 00 55 00   @:......C.:.\.U.
0000000020: 73 00 65 00 72 00 73 00 5c 00 77 00 69 00 6e 00   s.e.r.s.\.w.i.n.
0000000030: 37 00 20 00 78 00 38 00 36 00 20 00 37 00 36 00   7...x.8.6...7.6.
0000000040: 30 00 5c 00 44 00 65 00 73 00 6b 00 74 00 6f 00   0.\.D.e.s.k.t.o.
0000000050: 70 00 5c 00 41 00 63 00 63 00 65 00 73 00 73 00   p.\.A.c.c.e.s.s.
0000000060: 44 00 61 00 74 00 61 00 25 00 32 00 30 00 46 00   D.a.t.a.%.2.0.F.
0000000070: 54 00 4b 00 25 00 32 00 30 00 49 00 6d 00 61 00   T.K.%.2.0.I.m.a.
0000000080: 67 00 65 00 72 00 25 00 32 00 30 00 33 00 2e 00   g.e.r.%.2.0.3...
0000000090: 34 00 2e 00 32 00 25 00 32 00 30 00 25 00 32 00   4...2.%.2.0.%.2.
00000000a0: 38 00 78 00 36 00 34 00 25 00 32 00 39 00 2e 00   8.x.6.4.%.2.9...
00000000b0: 65 00 78 00 65 00 00 00 00 00 00 00 00 00 00 00   e.x.e...........
00000000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

&20 is space %28 is (and %29 is)

Flag C:\Users\win7 x86 760\Desktop\AccessData FTK Imager 3.4.2 (x64).exe