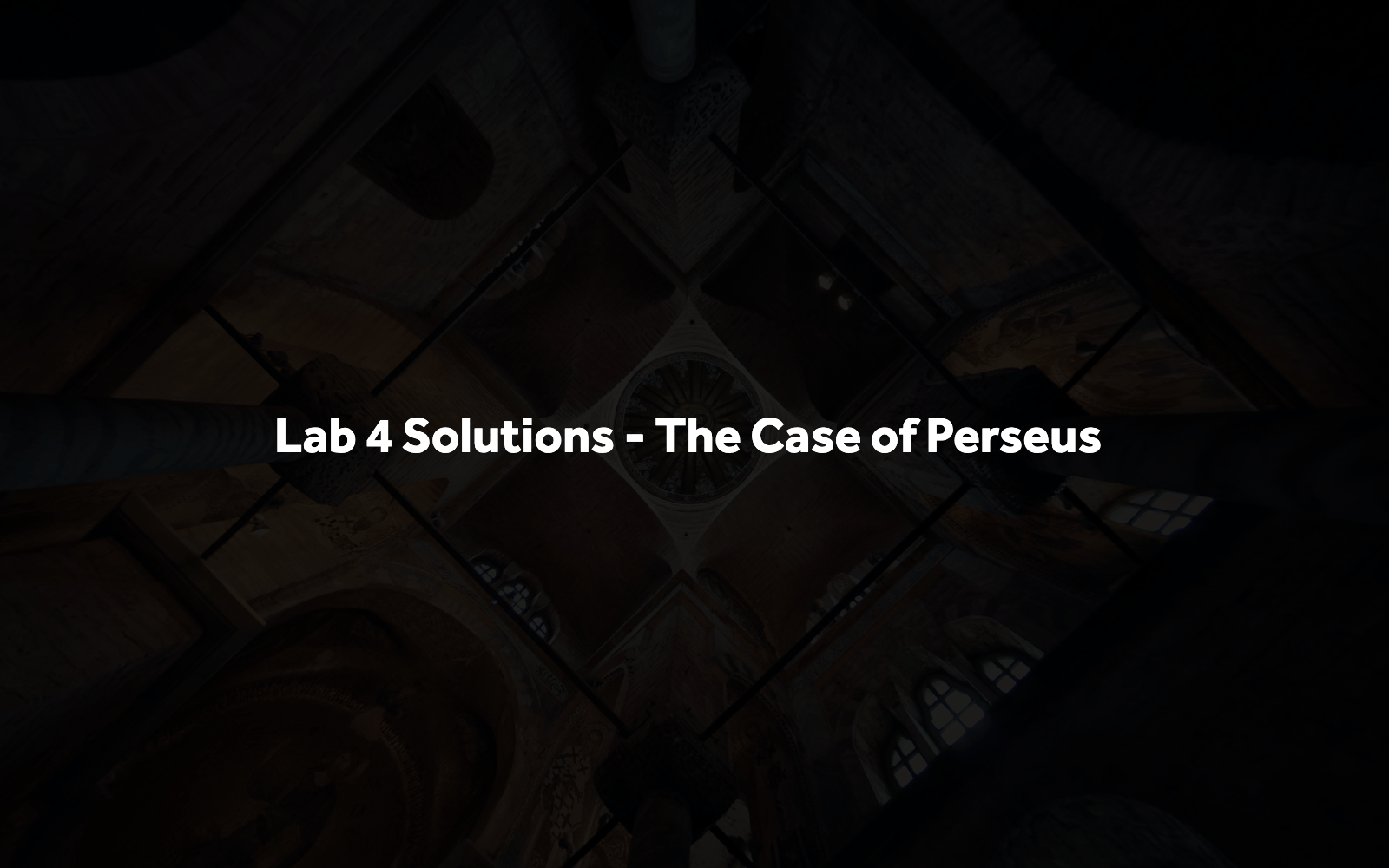
Lab 4 Solutions - The Case of Perseus



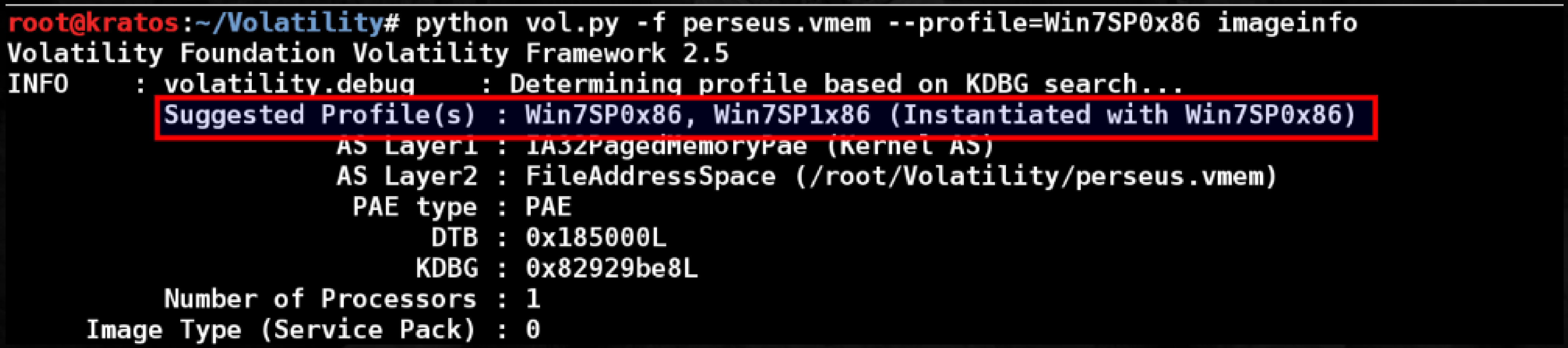
Lab 4: The Case of Perseus

A Top executive in your organization suspects that his system is infected after opening an attachment that came in via email. You are the incident responder handling this incident, you have collected the memory image (***perseus.vmem***). Investigate the memory image and answer the below questions:

- Do you see any process that looks suspicious?
- What is the name of the suspicious process?
- What is the process id of the suspicious process?
- Are there more than one suspicious process?
- How are these suspicious processes related?
- How is the attacker trying to blend in with legitimate processes?

Answers

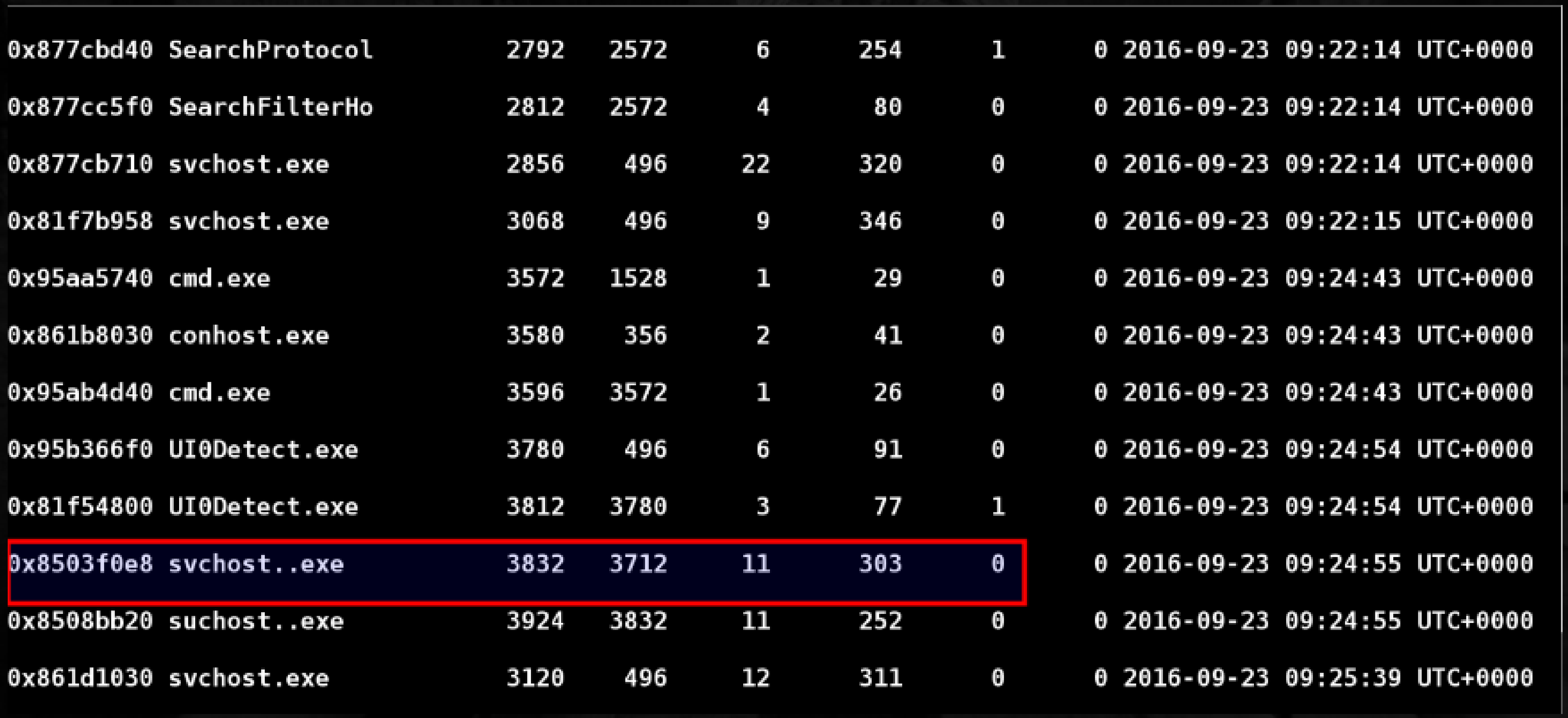
Before answering the questions, we need to determine the profile, this can be done by running the imageinfo plugin as shown in the screenshot



```
root@kratos:~/Volatility# python vol.py -f perseus.vmem --profile=Win7SP0x86 imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x86, Win7SP1x86 (Instantiated with Win7SP0x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Volatility/perseus.vmem)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82929be8L
          Number of Processors : 1
     Image Type (Service Pack) : 0
```

01. Do you see any process that looks suspicious?

Running the pslist command shows a suspicious process running on a system, the name of the file is not ***svchost.exe*** it is ***svchost..exe*** (there is an additional dot character before the ***.exe*** extension),



```
0x877cbd40 SearchProtocol         2792   2572      6      254      1      0 2016-09-23 09:22:14 UTC+0000
0x877cc5f0 SearchFilterHo         2812   2572      4       80      0      0 2016-09-23 09:22:14 UTC+0000
0x877cb710 svchost.exe            2856    496     22      320      0      0 2016-09-23 09:22:14 UTC+0000
0x81f7b958 svchost.exe            3068    496      9      346      0      0 2016-09-23 09:22:15 UTC+0000
0x95aa5740 cmd.exe                3572   1528      1       29      0      0 2016-09-23 09:24:43 UTC+0000
0x861b8030 conhost.exe            3580    356      2       41      0      0 2016-09-23 09:24:43 UTC+0000
0x95ab4d40 cmd.exe                3596   3572      1       26      0      0 2016-09-23 09:24:43 UTC+0000
0x95b366f0 UI0Detect.exe          3780    496      6       91      0      0 2016-09-23 09:24:54 UTC+0000
0x81f54800 UI0Detect.exe          3812   3780      3       77      1      0 2016-09-23 09:24:54 UTC+0000
0x8503f0e8 svchost..exe           3832   3712     11      303      0      0 2016-09-23 09:24:55 UTC+0000
0x8508bb20 suchost..exe           3924   3832     11      252      0      0 2016-09-23 09:24:55 UTC+0000
0x861d1030 svchost.exe            3120    496     12      311      0      0 2016-09-23 09:25:39 UTC+0000
```

02. What is the name of the suspicious process?

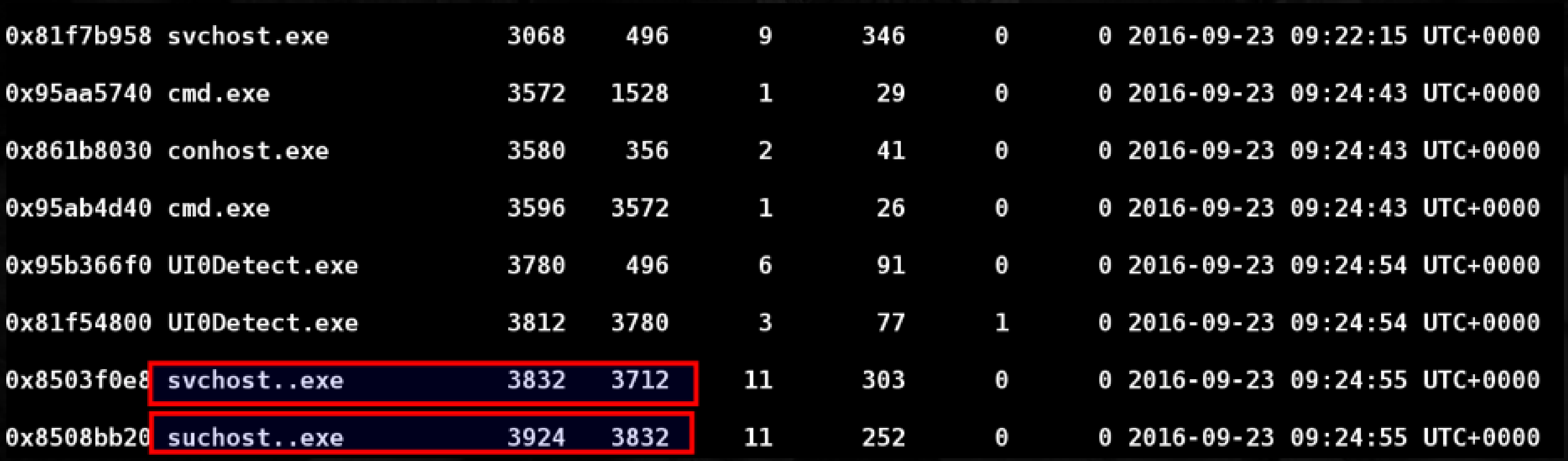
The name of the suspicious process is ***svchost..exe*** (with an additional dot character before **.exe**)

03. What is the process id?

The process id of the suspicious process (***svchost..exe***) is ***3832***

04. Are there more than one suspicious process?

Yes, there is one more process that is suspicious, that is the process ***suchost..exe*** (with ***pid 3924***). Both the suspicious processes are shown below.



```
0x81f7b958 svchost.exe            3068    496      9      346      0      0 2016-09-23 09:22:15 UTC+0000
0x95aa5740 cmd.exe                3572   1528      1       29      0      0 2016-09-23 09:24:43 UTC+0000
0x861b8030 conhost.exe            3580    356      2       41      0      0 2016-09-23 09:24:43 UTC+0000
0x95ab4d40 cmd.exe                3596   3572      1       26      0      0 2016-09-23 09:24:43 UTC+0000
0x95b366f0 UI0Detect.exe          3780    496      6       91      0      0 2016-09-23 09:24:54 UTC+0000
0x81f54800 UI0Detect.exe          3812   3780      3       77      1      0 2016-09-23 09:24:54 UTC+0000
0x8503f0e8 svchost..exe           3832   3712     11      303      0      0 2016-09-23 09:24:55 UTC+0000
0x8508bb20 suchost..exe           3924   3832     11      252      0      0 2016-09-23 09:24:55 UTC+0000
```

05. How are these suspicious processes related?

These two processes have a parent-child relationship, the parent id of ***suchost..exe*** is **3832** which is associated with ***svchost..exe***, this indicates that ***svchost..exe*** (***pid 3832***) created the process ***suchost..exe*** (***pid 3924***)

06. How is the attacker trying to blend in with legitimate processes?

The attacker is trying to blend in by creating a process whose name is similar to the legitimate process. On a clean system, there are multiple instances of ***svchost.exe*** processes running, in this case, both ***svchost..exe*** & ***suchost..exe*** have been made to look similar to the legitimate process ***svchost.exe***. This is an attempt to blend in with legitimate processes.