TryHackMe: Dead End?

The following writeup covers the room Dead End?, which is an hard difficulty room that involves analysing a memory dump using volatility and a disk image using FTK Imager. I was able to complete most of the questions, excluding the last 2 in the disk image section, so I highly recommend checking out this writeup.

Scenario: An in-depth analysis of specific endpoints is reserved for those you're certain to have been compromised. It is usually done to understand how specific adversary tools or malwares work on the endpoint level; the lessons learned here are applied to the rest of the incident.

You're presented with two main artefacts: a memory dump and a disk image. Can you follow the artefact trail and find the flag?

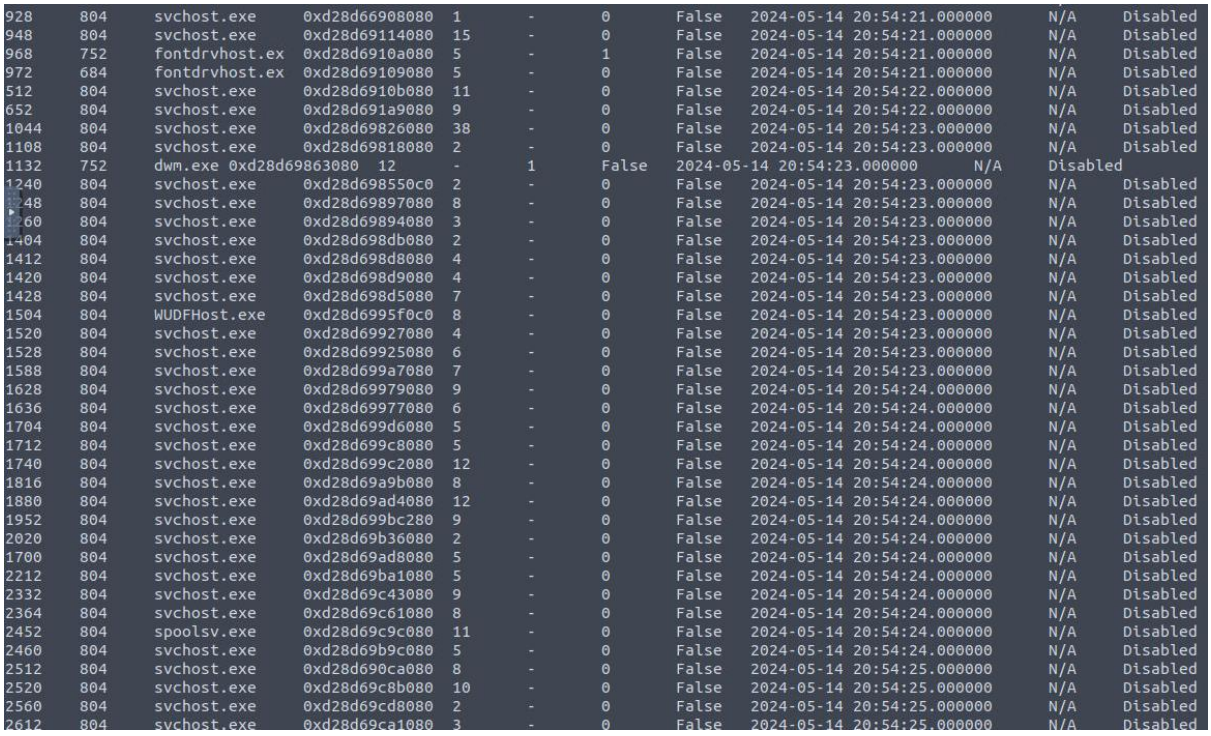
What binary gives the most apparent sign of suspicious activity in the given memory image?

Use the full path of the artefact.

When investigating a memory image, I like to start by listing all the running processes by using the pslist plugin:

```
python3 vol.py -f ../RobertMemdump/memdump.mem windows.pslist
```

This took a relatively long time (maybe 1-2 minutes), however, once it finished, we can see a large number of svchost.exe processes:



```
928     804     svchost.exe     0xd28d66908080  1       -       0       False   2024-05-14 20:54:21.000000      N/A     Disabled
948     804     svchost.exe     0xd28d69114080  15      -       0       False   2024-05-14 20:54:21.000000      N/A     Disabled
968     752     fontdrvhost.ex  0xd28d6910a080  5       -       1       False   2024-05-14 20:54:21.000000      N/A     Disabled
972     684     fontdrvhost.ex  0xd28d69109080  5       -       0       False   2024-05-14 20:54:21.000000      N/A     Disabled
512     804     svchost.exe     0xd28d6910b080  11      -       0       False   2024-05-14 20:54:22.000000      N/A     Disabled
652     804     svchost.exe     0xd28d691a9080  9       -       0       False   2024-05-14 20:54:22.000000      N/A     Disabled
1044    804     svchost.exe     0xd28d69826080  38      -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1108    804     svchost.exe     0xd28d69818080  2       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1132    752     dwm.exe 0xd28d69863080  12      -       1       False   2024-05-14 20:54:23.000000      N/A     Disabled
1240    804     svchost.exe     0xd28d698550c0  2       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1248    804     svchost.exe     0xd28d69897080  8       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1260    804     svchost.exe     0xd28d69894080  3       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1404    804     svchost.exe     0xd28d698db080  2       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1412    804     svchost.exe     0xd28d698d8080  4       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1420    804     svchost.exe     0xd28d698d9080  4       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1428    804     svchost.exe     0xd28d698d5080  7       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1504    804     WUDFHost.exe    0xd28d6995f0c0  8       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1520    804     svchost.exe     0xd28d69927080  4       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1528    804     svchost.exe     0xd28d69925080  6       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1588    804     svchost.exe     0xd28d699a7080  7       -       0       False   2024-05-14 20:54:23.000000      N/A     Disabled
1628    804     svchost.exe     0xd28d69979080  9       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1636    804     svchost.exe     0xd28d69977080  6       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1704    804     svchost.exe     0xd28d699d6080  5       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1712    804     svchost.exe     0xd28d699c8080  5       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1740    804     svchost.exe     0xd28d699c2080  12      -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1816    804     svchost.exe     0xd28d69a9b080  8       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1880    804     svchost.exe     0xd28d69ad4080  12      -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1952    804     svchost.exe     0xd28d699bc280  9       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
2020    804     svchost.exe     0xd28d69b36080  2       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
1700    804     svchost.exe     0xd28d69ad8080  5       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
2212    804     svchost.exe     0xd28d69ba1080  5       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
2332    804     svchost.exe     0xd28d69c43080  9       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
2364    804     svchost.exe     0xd28d69c61080  8       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
2452    804     spoolsv.exe     0xd28d69c9c080  11      -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
2460    804     svchost.exe     0xd28d69b9c080  5       -       0       False   2024-05-14 20:54:24.000000      N/A     Disabled
2512    804     svchost.exe     0xd28d690ca080  8       -       0       False   2024-05-14 20:54:25.000000      N/A     Disabled
2520    804     svchost.exe     0xd28d69c8b080  10      -       0       False   2024-05-14 20:54:25.000000      N/A     Disabled
2560    804     svchost.exe     0xd28d69cd8080  2       -       0       False   2024-05-14 20:54:25.000000      N/A     Disabled
2612    804     svchost.exe     0xd28d69ca1080  3       -       0       False   2024-05-14 20:54:25.000000      N/A     Disabled
```

Whilst this in and of itself is not an indicator of malicious activity, let's use the pstree plugin to see the file path:

```
python3 vol.py -f ../RobertMemdump/memdump.mem windows.pstree | grep svchost.exe
```

And boom, we have svchost being launched in the C:\Tools\ directory which is not the typical path of C:\Windows\system32:

```
N/A     \Device\HarddiskVolume1\Tools\svchost.exe       "C:\Tools\svchost.exe" -e cmd.exe
```

Answer: C:\Tools\svchost.exe

The answer above shares the same parent process with another binary that references a .txt file - what is the full path of this .txt file?

Based on the output of the pstree plugin, we know that the PPID of this svchost.exe instance is 1036, so we can search for this using the pstree plugin:

```
python3 vol.py -f ../RobertMemdump/memdump.mem windows.pstree --pid 1036
```

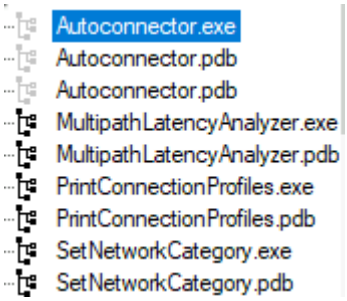
```
C:\Users\Bobby\Documents\tmp\part2.txt
```

Answer: C:\Users\Bobby\Documents\tmp\part2.txt

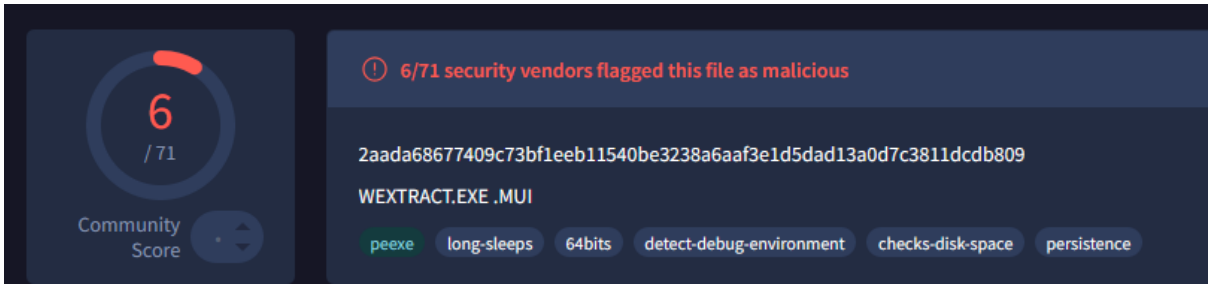
What binary gives the most apparent sign of suspicious activity in the given disk image?

Use the full path of the artefact.

After importing the disk image into FTK Imager, and looking through the file system, I came across an interesting binary located at C:\Tools\windows-networking-tools-master\windows-networking-tools-master\LatestBuilds\x64\Autoconnector.exe



I right-clicked the binary and exported the file hash so we can check it against VirusTotal:

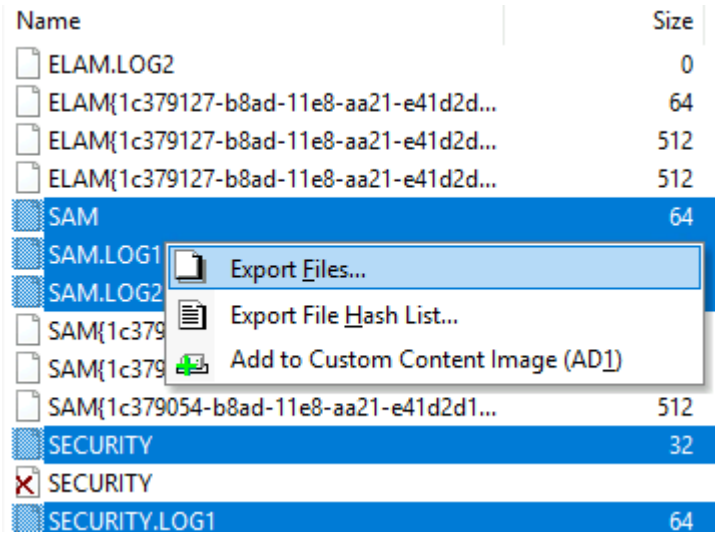


Whilst 6 results isn't anything crazy, it does indicate that this file is likely malicious.

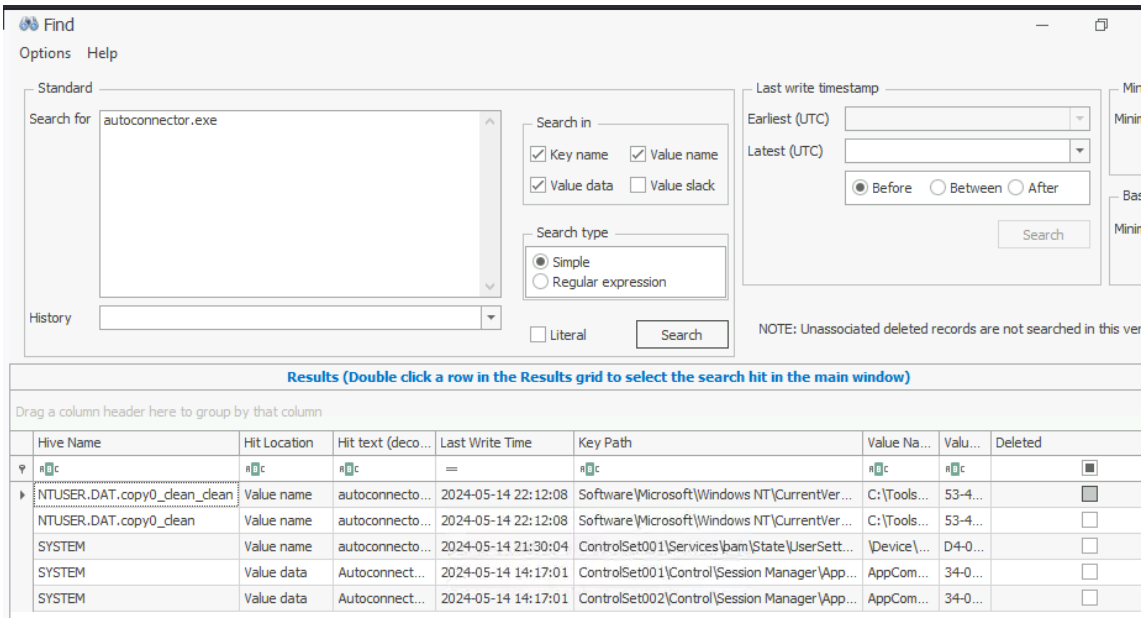
Answer: C:\Tools\windows-networking-tools-master\windows-networking-tools-master\LatestBuilds\x64\Autoconnector.exe

What is the full registry path where the existence of the binary above is confirmed?

Start by dumping all the registry hives found in C:\Windows\system32\config:



You can now import all the needed hives into RegistryExplorer, including their transaction logs. We can now use the keyboard search option to look for Autoconnector.exe:



ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1966530601-3185510712-10604624-1008

Answer: Key Path

ControlSet001\Services\bam\State\UserSettings\S-1-5-21-1966530601-3185510712-10604624-1008

What is the content of "Part2"?

faDB3XzJfcDF2T1R9

What is the flag?

THM{6l4D_y0u_kNOw_h0w_2_p1vOT}