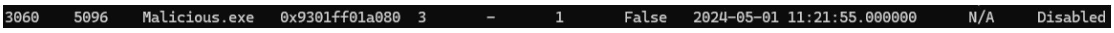
Task 1:

3.

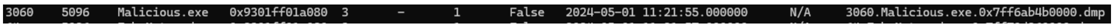
3060   5096   Malicious.exe   0x9301ff01a080   3   -   1   False



```
3060    5096    Malicious.exe   0x9301ff01a080  3       -       1       False   2024-05-01 11:21:55.000000      N/A     Disabled
```

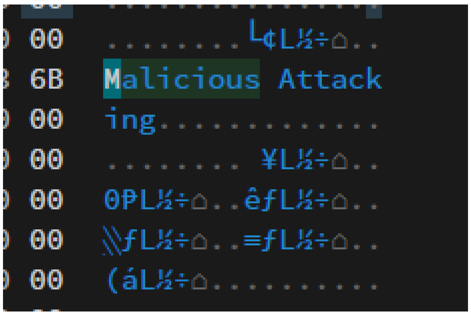
4.

Use python3 vol.py -f ~/path/to/your/dump/file windows.psscan --dump to get 3060.Malicious.exe.0x7ff6ab4b0000.dmp



```
3060    5096    Malicious.exe   0x9301ff01a080  3       -       1       False   2024-05-01 11:21:55.000000      N/A     3060.Malicious.exe.0x7ff6ab4b0000.dmp
```

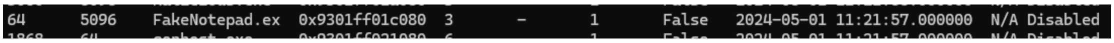
5.



```
 00  ........└¢L½÷⌂..
 6B  Malicious Attack
 00  ing.............
 00  ........ ¥L½÷⌂..
 00  0₧L½÷⌂..êƒL½÷⌂..
 00  ╲ƒL½÷⌂..≡ƒL½÷⌂..
 00  (áL½÷⌂..........
```

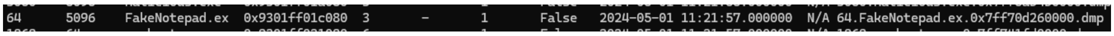
Task 2:

Use python3 vol.py -f ~/path/to/your/dump/file windows.psscan to show process



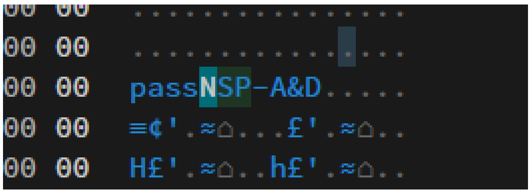
```
64      5096    FakeNotepad.ex  0x9301ff01c080  3       -       1       False   2024-05-01 11:21:57.000000  N/A Disabled
```

Use python3 vol.py -f ~/path/to/your/dump/file windows.psscan --dump to get



```
64      5096    FakeNotepad.ex  0x9301ff01c080  3       -       1       False   2024-05-01 11:21:57.000000  N/A 64.FakeNotepad.ex.0x7ff70d260000.dmp
```

Open the dmp file on HexEd.it to see the contents.



```
00 00  ................
00 00  passNSP-A&D.....
00 00  ≡¢'.≈⌂...£'.≈⌂..
00 00  H£'.≈⌂..h£'.≈⌂..
```