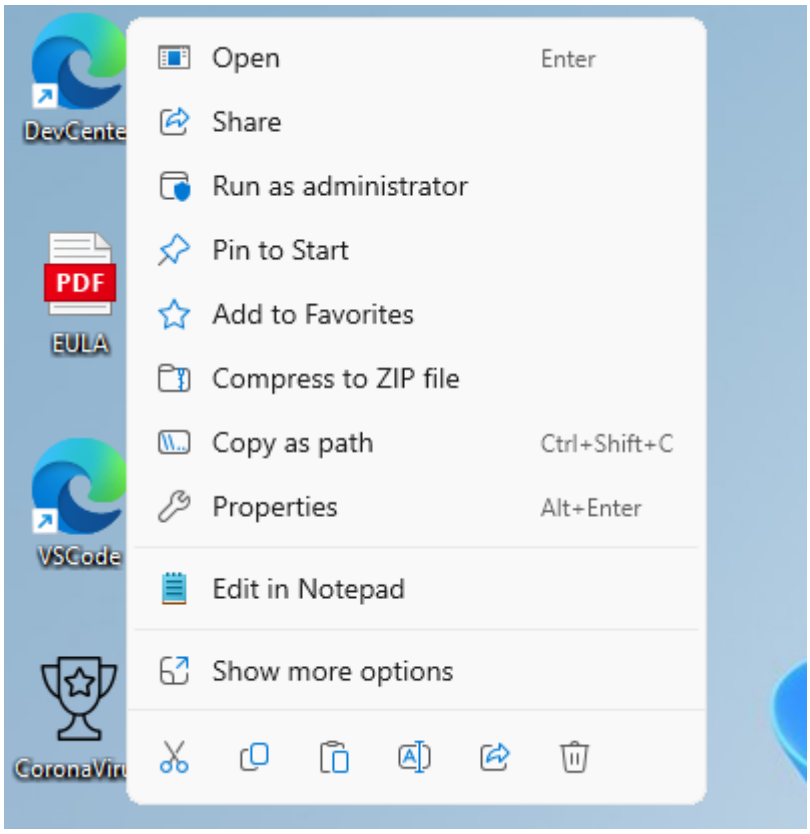
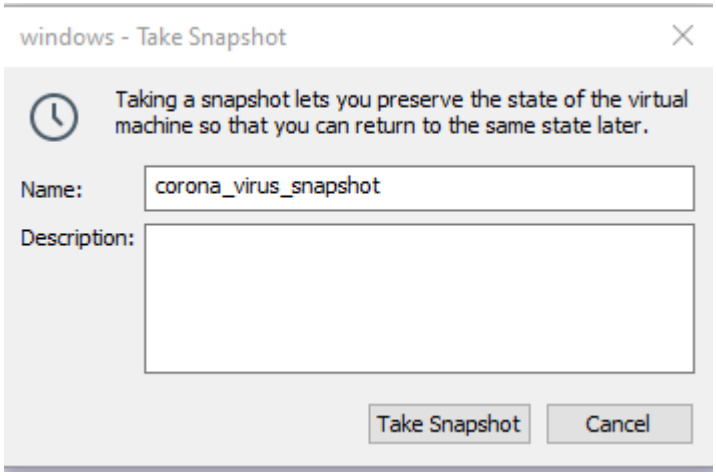
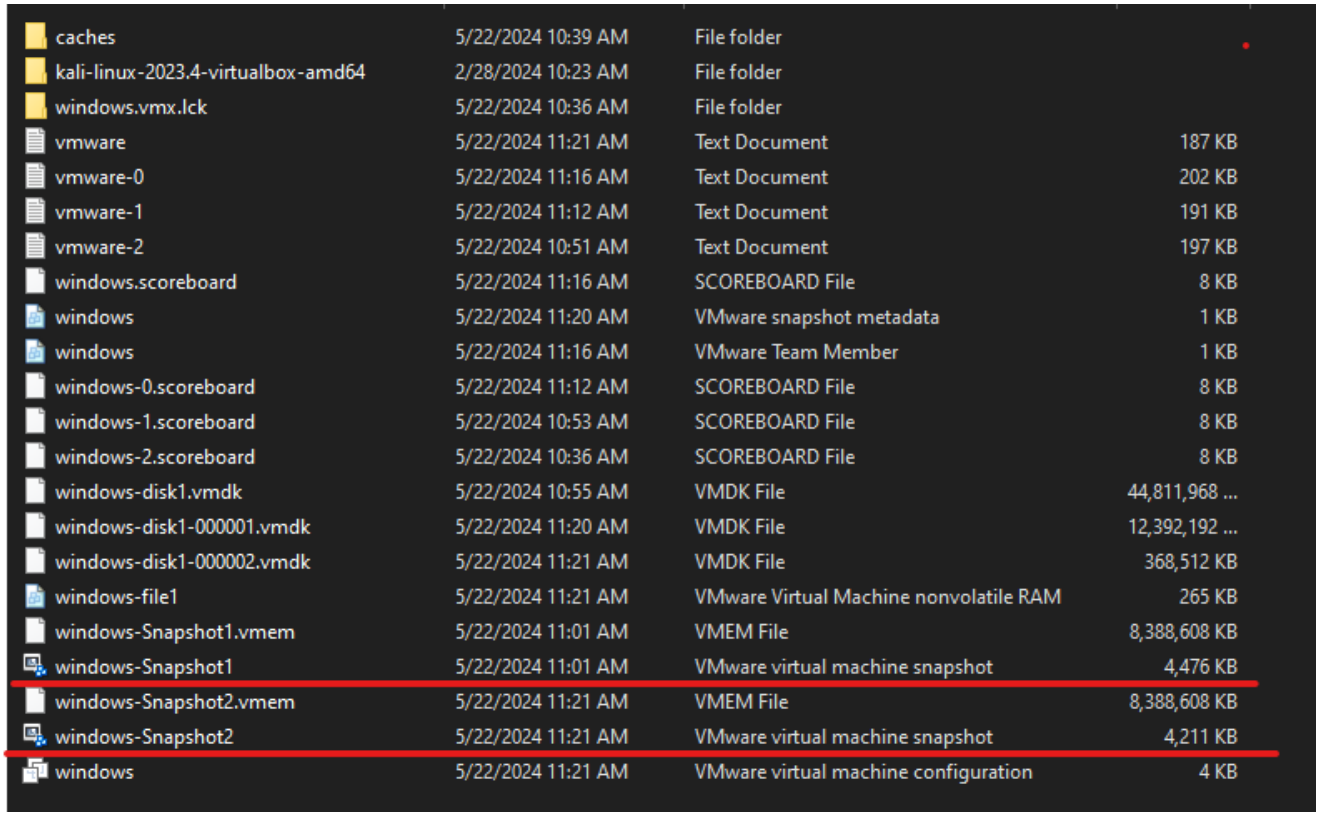
lab 3


DevCente
PDF
EULA
VSCode
CoronaViru
Open Enter
Share
Run as administrator
Pin to Start
Add to Favorites
Compress to ZIP file
Copy as path Ctrl+Shift+C
Properties Alt+Enter
Edit in Notepad
Show more options


All your files have been encrypted!
All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail coronavirus@qq.com
Write this ID in the title of your message 20C7F853
In case of no answer in 24 hours write us to theese e-mails: coronavirus@qq.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.
Free decryption as guarantee
Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)
How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/
Attention!
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.
Ubuntu on Windows





caches	5/22/2024 10:39 AM	File folder	
kali-linux-2023.4-virtualbox-amd64	2/28/2024 10:23 AM	File folder	
windows.vmx.lck	5/22/2024 10:36 AM	File folder	
vmware	5/22/2024 11:21 AM	Text Document	187 KB
vmware-0	5/22/2024 11:16 AM	Text Document	202 KB
vmware-1	5/22/2024 11:12 AM	Text Document	191 KB
vmware-2	5/22/2024 10:51 AM	Text Document	197 KB
windows.scoreboard	5/22/2024 11:16 AM	SCOREBOARD File	8 KB
windows	5/22/2024 11:20 AM	VMware snapshot metadata	1 KB
windows	5/22/2024 11:16 AM	VMware Team Member	1 KB
windows-0.scoreboard	5/22/2024 11:12 AM	SCOREBOARD File	8 KB
windows-1.scoreboard	5/22/2024 10:53 AM	SCOREBOARD File	8 KB
windows-2.scoreboard	5/22/2024 10:36 AM	SCOREBOARD File	8 KB
windows-disk1.vmdk	5/22/2024 10:55 AM	VMDK File	44,811,968 ...
windows-disk1-000001.vmdk	5/22/2024 11:20 AM	VMDK File	12,392,192 ...
windows-disk1-000002.vmdk	5/22/2024 11:21 AM	VMDK File	368,512 KB
windows-file1	5/22/2024 11:21 AM	VMware Virtual Machine nonvolatile RAM	265 KB
windows-Snapshot1.vmem	5/22/2024 11:01 AM	VMEM File	8,388,608 KB
windows-Snapshot1	5/22/2024 11:01 AM	VMware virtual machine snapshot	4,476 KB
windows-Snapshot2.vmem	5/22/2024 11:21 AM	VMEM File	8,388,608 KB
windows-Snapshot2	5/22/2024 11:21 AM	VMware virtual machine snapshot	4,211 KB
windows	5/22/2024 11:21 AM	VMware virtual machine configuration	4 KB

- .vmem - dump
- .vmsn - config pentru vmware
  python .\vol.py -f ..\vm\windows-Snapshot2.vmem windows.pslist

```
>> python .\vol.py -f ..\vm\windows-Snapshot2.vmem windows.pslist
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xc28f1d4a9040  190     -       N/A     False   2024-05-22 17:37:45.000000      N/A     Disabled
76      4       Secure System   0xc28f1d602080  0       -       N/A     False   2024-05-22 17:37:43.000000      N/A     Disabled
112     4       Registry        0xc28f1d520080  4       -       N/A     False   2024-05-22 17:37:43.000000      N/A     Disabled
420     4       smss.exe        0xc28f20260040  2       -       N/A     False   2024-05-22 17:37:45.000000      N/A     Disabled
556     548     csrss.exe       0xc28f20e2d2c0  10      -       0       False   2024-05-22 17:37:46.000000      N/A     Disabled
656     548     wininit.exe     0xc28f21103080  2       -       0       False   2024-05-22 17:37:46.000000      N/A     Disabled
664     648     csrss.exe       0xc28f2110a140  14      -       1       False   2024-05-22 17:37:46.000000      N/A     Disabled
748     648     winlogon.exe    0xc28f21141080  4       -       1       False   2024-05-22 17:37:46.000000      N/A     Disabled
796     656     services.exe    0xc28f211491c0  8       -       0       False   2024-05-22 17:37:46.000000      N/A     Disabled
816     656     LsaIso.exe      0xc28f21170180  4       -       0       False   2024-05-22 17:37:46.000000      N/A     Disabled
832     656     lsass.exe       0xc28f21172180  11      -       0       False   2024-05-22 17:37:46.000000      N/A     Disabled
964     796     svchost.exe     0xc28f2122c380  21      -       0       False   2024-05-22 17:37:47.000000      N/A     Disabled
992     748     fontdrvhost.ex  0xc28f2122f280  5       -       1       False   2024-05-22 17:37:47.000000      N/A     Disabled
1000    656     fontdrvhost.ex  0xc28f2122d080  5       -       0       False   2024-05-22 17:37:47.000000      N/A     Disabled
648     796     svchost.exe     0xc28f21260240  12      -       0       False   2024-05-22 17:37:47.000000      N/A     Disabled
920     796     svchost.exe     0xc28f212ca380  6       -       0       False   2024-05-22 17:37:47.000000      N/A     Disabled
1056    796     sppsvc.exe      0xc28f21309080  0       -       0       False   2024-05-22 17:37:47.000000      2024-05-22 07:42:45.000000      Disabled
1084    748     dwm.exe 0xc28f21311140  25      -       1       False   2024-05-22 17:37:47.000000      N/A     Disabled
1124    796     svchost.exe     0xc28f21375380  1       -       0       False   2024-05-22 17:37:47.000000      N/A     Disabled
1188    796     svchost.exe     0xc28f2139e240  2       -       0       False   2024-05-22 17:37:47.000000      N/A     Disabled
1280    796     svchost.exe     0xc28f213ef0c0  1       -       0       False   2024-05-22 17:37:47.000000      N/A     Disabled
1496    796     svchost.exe     0xc28f214823c0  2       -       0       False   2024-05-22 17:37:51.000000      N/A     Disabled
1544    796     svchost.exe     0xc28f1d5a9080  7       -       0       False   2024-05-22 17:37:51.000000      N/A     Disabled
1644    796     svchost.exe     0xc28f1d570080  3       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1652    796     svchost.exe     0xc28f1d56a080  4       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1704    796     svchost.exe     0xc28f1d550080  9       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1868    796     svchost.exe     0xc28f2147d080  2       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1892    796     svchost.exe     0xc28f215b9380  11      -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1900    796     svchost.exe     0xc28f215b1280  9       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1908    796     svchost.exe     0xc28f216020c0  1       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1940    796     svchost.exe     0xc28f216240c0  7       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1948    796     svchost.exe     0xc28f21626380  1       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
8       796     svchost.exe     0xc28f216723c0  2       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
1468    796     svchost.exe     0xc28f21671080  5       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
2104    796     svchost.exe     0xc28f216f3080  3       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
2320    796     svchost.exe     0xc28f2178d380  7       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
2396    796     svchost.exe     0xc28f217ea380  5       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
2476    796     svchost.exe     0xc28f21830380  4       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
2492    796     svchost.exe     0xc28f21858380  5       -       0       False   2024-05-22 17:37:52.000000      N/A     Disabled
2572    796     svchost.exe     0xc28f21865080  7       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2644    796     svchost.exe     0xc28f218e6080  6       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2668    796     svchost.exe     0xc28f2190f080  4       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2676    796     svchost.exe     0xc28f2190e3c0  6       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2704    796     svchost.exe     0xc28f21915380  4       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2852    4       MemCompression  0xc28f219a5040  34      -       N/A     False   2024-05-22 17:37:53.000000      N/A     Disabled
2868    796     svchost.exe     0xc28f219a7380  5       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2952    796     svchost.exe     0xc28f21a2e0c0  9       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
3008    796     svchost.exe     0xc28f21c873c0  3       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2652    796     svchost.exe     0xc28f21ae50c0  1       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
2788    796     svchost.exe     0xc28f21d11140  2       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
3136    796     svchost.exe     0xc28f21b480c0  2       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
3168    796     svchost.exe     0xc28f21b4e0c0  1       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
3276    796     spoolsv.exe     0xc28f21ddc0c0  7       -       0       False   2024-05-22 17:37:53.000000      N/A     Disabled
3320    796     svchost.exe     0xc28f21bfb0c0  9       -       0       False   2024-05-22 17:37:54.000000      N/A     Disabled
3368    796     svchost.exe     0xc28f21c130c0  13      -       0       False   2024-05-22 17:37:54.000000      N/A     Disabled
3440    796     svchost.exe     0xc28f21c650c0  5       -       0       False   2024-05-22 17:37:54.000000      N/A     Disabled
3596    796     svchost.exe     0xc28f21fac0c0  1       -       0       False   2024-05-22 17:37:54.000000      N/A     Disabled
3708    796     MsMpEng.exe     0xc28f2219a0c0  21      -       0       False   2024-05-22 17:37:55.000000      N/A     Disabled
3940    796     svchost.exe     0xc28f21c44300  23      -       0       False   2024-05-22 17:37:55.000000      N/A     Disabled
3892    796     SearchIndexer.  0xc28f21ac4340  12      -       0       False   2024-05-22 17:37:56.000000      N/A     Disabled
4968    796     svchost.exe     0xc28f21b2d080  5       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
4976    796     svchost.exe     0xc28f22043380  9       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
4984    796     svchost.exe     0xc28f220ba340  11      -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
```

```
5012    796     svchost.exe     0xc28f21f223c0  3       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
5060    796     VGAuthService.  0xc28f21f55080  2       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
5072    796     vm3dservice.ex  0xc28f21fdd080  3       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
5080    796     vmtoolsd.exe    0xc28f21f77080  13      -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
5100    796     wlms.exe        0xc28f21f21080  2       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
5116    796     svchost.exe     0xc28f22042080  6       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
3836    796     svchost.exe     0xc28f21edc080  8       -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
4172    5072    vm3dservice.ex  0xc28f21f32340  4       -       1       False   2024-05-22 17:38:02.000000      N/A     Disabled
4392    796     svchost.exe     0xc28f21e213c0  12      -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
4588    796     svchost.exe     0xc28f227040c0  17      -       0       False   2024-05-22 17:38:02.000000      N/A     Disabled
4896    4976    AggregatorHost  0xc28f22796080  1       -       0       False   2024-05-22 17:38:03.000000      N/A     Disabled
948     796     svchost.exe     0xc28f2296b080  5       -       0       False   2024-05-22 17:38:05.000000      N/A     Disabled
4468    796     svchost.exe     0xc28f21f33080  8       -       0       False   2024-05-22 17:38:05.000000      N/A     Disabled
5140    964     WmiPrvSE.exe    0xc28f22aa83c0  4       -       0       False   2024-05-22 17:38:06.000000      N/A     Disabled
5240    796     svchost.exe     0xc28f21b66080  1       -       0       False   2024-05-22 17:38:06.000000      N/A     Disabled
5248    796     svchost.exe     0xc28f22ad13c0  20      -       0       False   2024-05-22 17:38:06.000000      N/A     Disabled
5340    3320    sihost.exe      0xc28f22b30080  15      -       1       False   2024-05-22 17:38:06.000000      N/A     Disabled
5360    796     svchost.exe     0xc28f22b323c0  4       -       1       False   2024-05-22 17:38:06.000000      N/A     Disabled
5396    796     svchost.exe     0xc28f22b750c0  2       -       1       False   2024-05-22 17:38:06.000000      N/A     Disabled
5440    796     svchost.exe     0xc28f22b773c0  8       -       1       False   2024-05-22 17:38:06.000000      N/A     Disabled
5592    796     svchost.exe     0xc28f22c25380  7       -       0       False   2024-05-22 17:38:06.000000      N/A     Disabled
5716    796     svchost.exe     0xc28f22c6d0c0  5       -       0       False   2024-05-22 17:38:06.000000      N/A     Disabled
5808    748     userinit.exe    0xc28f22ba32c0  0       -       1       False   2024-05-22 17:38:06.000000      2024-05-22 07:38:33.000000      Disabled
5832    5808    explorer.exe    0xc28f219e7080  80      -       1       False   2024-05-22 17:38:06.000000      N/A     Disabled
5860    964     WmiPrvSE.exe    0xc28f22c943c0  12      -       0       False   2024-05-22 17:38:06.000000      N/A     Disabled
6068    1892    taskhostw.exe   0xc28f22c9b3c0  9       -       1       False   2024-05-22 17:38:07.000000      N/A     Disabled
6092    1892    taskhostw.exe   0xc28f22cea080  3       -       1       False   2024-05-22 17:38:07.000000      N/A     Disabled
6484    796     dllhost.exe     0xc28f22eb53c0  10      -       0       False   2024-05-22 07:38:07.000000      N/A     Disabled
6544    5080    VMwareResoluti  0xc28f22eec080  0       -       1       False   2024-05-22 07:38:08.000000      2024-05-22 07:38:08.000000      Disabled
6604    796     msdtc.exe       0xc28f22ef03c0  9       -       0       False   2024-05-22 07:38:08.000000      N/A     Disabled
6696    796     svchost.exe     0xc28f22f6c380  2       -       0       False   2024-05-22 07:38:08.000000      N/A     Disabled
6800    796     svchost.exe     0xc28f22f7d080  6       -       0       False   2024-05-22 07:38:08.000000      N/A     Disabled
7072    796     svchost.exe     0xc28f23072380  3       -       0       False   2024-05-22 07:38:08.000000      N/A     Disabled
6320    3008    ctfmon.exe      0xc28f231b0340  12      -       1       False   2024-05-22 07:38:08.000000      N/A     Disabled
6992    796     svchost.exe     0xc28f23207380  4       -       0       False   2024-05-22 07:38:08.000000      N/A     Disabled
7484    7416    msedge.exe      0xc28f232cd080  0       -       1       False   2024-05-22 07:38:09.000000      2024-05-22 07:38:11.000000      Disabled
7312    796     svchost.exe     0xc28f234223c0  13      -       1       False   2024-05-22 07:38:12.000000      N/A     Disabled
7912    964     SearchHost.exe  0xc28f23069080  54      -       1       False   2024-05-22 07:38:12.000000      N/A     Disabled
7492    964     StartMenuExper  0xc28f2339d080  14      -       1       False   2024-05-22 07:38:12.000000      N/A     Disabled
8024    964     Widgets.exe     0xc28f235e2080  18      -       1       False   2024-05-22 07:38:12.000000      N/A     Disabled
6148    964     RuntimeBroker.  0xc28f236153c0  6       -       1       False   2024-05-22 07:38:12.000000      N/A     Disabled
8056    964     RuntimeBroker.  0xc28f236193c0  6       -       1       False   2024-05-22 07:38:12.000000      N/A     Disabled
7268    796     svchost.exe     0xc28f237103c0  3       -       1       False   2024-05-22 07:38:13.000000      N/A     Disabled
8408    796     svchost.exe     0xc28f238b9380  10      -       0       False   2024-05-22 07:38:13.000000      N/A     Disabled
8924    964     dllhost.exe     0xc28f23c0d080  7       -       1       False   2024-05-22 07:38:15.000000      N/A     Disabled
8760    796     svchost.exe     0xc28f234e8080  6       -       0       False   2024-05-22 07:38:28.000000      N/A     Disabled
3780    796     svchost.exe     0xc28f231e53c0  3       -       0       False   2024-05-22 07:38:39.000000      N/A     Disabled
4184    5832    SecurityHealth  0xc28f238bd080  4       -       1       False   2024-05-22 07:39:31.000000      N/A     Disabled
7552    796     SecurityHealth  0xc28f23af4380  14      -       0       False   2024-05-22 07:39:31.000000      N/A     Disabled
8240    5832    vmtoolsd.exe    0xc28f238d3080  7       -       1       False   2024-05-22 07:39:31.000000      N/A     Disabled
7992    6356    OneDrive.exe    0xc28f236240c0  21      -       1       False   2024-05-22 07:39:56.000000      N/A     Disabled
3376    7992    Microsoft.Shar  0xc28f24fc60c0  0       -       1       False   2024-05-22 07:39:58.000000      2024-05-22 07:49:59.000000      Disabled
2512    796     uhssvc.exe      0xc28f244e1080  3       -       0       False   2024-05-22 07:40:02.000000      N/A     Disabled
9012    796     svchost.exe     0xc28f24fc2080  13      -       0       False   2024-05-22 07:40:02.000000      N/A     Disabled
5232    796     svchost.exe     0xc28f231bc080  1       -       1       False   2024-05-22 07:40:02.000000      N/A     Disabled
2540    964     WidgetService.  0xc28f231ed080  7       -       1       False   2024-05-22 07:40:05.000000      N/A     Disabled
6640    796     svchost.exe     0xc28f23055080  11      -       0       False   2024-05-22 07:44:18.000000      N/A     Disabled
7512    964     ShellExperienc  0xc28f22d4d080  26      -       1       False   2024-05-22 07:44:26.000000      N/A     Disabled
1172    796     svchost.exe     0xc28f2344c080  3       -       1       False   2024-05-22 07:44:27.000000      N/A     Disabled
6744    964     RuntimeBroker.  0xc28f235c1080  15      -       1       False   2024-05-22 07:44:27.000000      N/A     Disabled
5096    964     SystemSettings  0xc28f23453080  6       -       1       False   2024-05-22 07:44:27.000000      N/A     Disabled
7128    796     svchost.exe     0xc28f2178e080  1       -       0       False   2024-05-22 07:44:28.000000      N/A     Disabled
5980    796     svchost.exe     0xc28f23351080  12      -       0       False   2024-05-22 07:44:29.000000      N/A     Disabled
2516    796     svchost.exe     0xc28f24f4d080  6       -       0       False   2024-05-22 07:45:24.000000      N/A     Disabled
4036    796     svchost.exe     0xc28f232f7080  29      -       0       False   2024-05-22 07:45:24.000000      N/A     Disabled
5676    796     svchost.exe     0xc28f23632080  5       -       0       False   2024-05-22 07:45:24.000000      N/A     Disabled
7700    8408    MoUsoCoreWorke  0xc28f23ce5080  9       -       0       False   2024-05-22 07:45:24.000000      N/A     Disabled
1824    3892    SearchProtocol  0xc28f23fe0080  7       -       0       False   2024-05-22 07:47:06.000000      N/A     Disabled
6404    796     TrustedInstall  0xc28f24455080  5       -       0       False   2024-05-22 07:48:20.000000      N/A     Disabled
2080    964     TiWorker.exe    0xc28f23bf4080  5       -       0       False   2024-05-22 07:48:20.000000      N/A     Disabled
808     7700    MoNotification  0xc28f23af7080  0       -       1       False   2024-05-22 07:48:47.000000      2024-05-22 07:48:47.000000      Disabled
6624    796     svchost.exe     0xc28f258cb080  5       -       0       False   2024-05-22 07:49:28.000000      N/A     Disabled
```

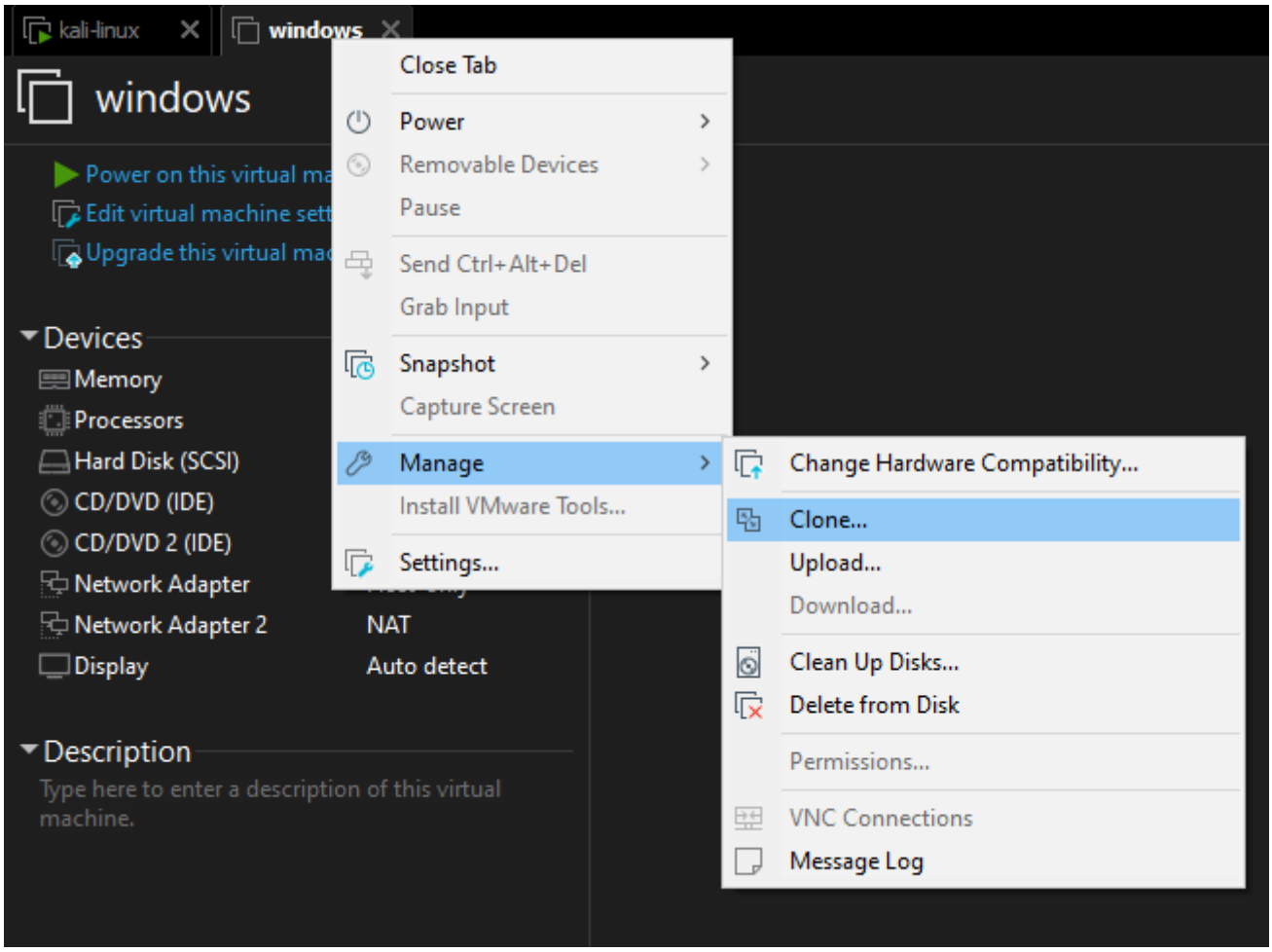
```
1596    964     smartscreen.ex  0xc28f25bd4300  9       -       1       False   2024-05-22 07:49:32.000000      N/A     Disabled
7924    7700    MoNotification  0xc28f24a88080  0       -       1       False   2024-05-22 07:51:11.000000      2024-05-22 07:51:11.000000      Disabled
8568    7700    MoNotification  0xc28f238ed080  0       -       1       False   2024-05-22 07:51:13.000000      2024-05-22 07:51:13.000000      Disabled
6452    796     svchost.exe     0xc28f2689d080  11      -       0       False   2024-05-22 07:54:16.000000      N/A     Disabled
8164    796     svchost.exe     0xc28f26830380  6       -       0       False   2024-05-22 07:54:17.000000      N/A     Disabled
4828    5176    setup.exe       0xc28f27480080  4       -       0       False   2024-05-22 07:54:32.000000      N/A     Disabled
8632    4828    setup.exe       0xc28f2749d080  6       -       0       False   2024-05-22 07:54:32.000000      N/A     Disabled
1928    8024    msedgewebview2  0xc28f22978080  45      -       1       False   2024-05-22 07:54:34.000000      N/A     Disabled
7940    1928    msedgewebview2  0xc28f24f0f080  7       -       1       False   2024-05-22 07:54:34.000000      N/A     Disabled
516     1928    msedgewebview2  0xc28f23ad0080  20      -       1       False   2024-05-22 07:54:35.000000      N/A     Disabled
3896    1928    msedgewebview2  0xc28f235bc080  13      -       1       False   2024-05-22 07:54:35.000000      N/A     Disabled
1772    1928    msedgewebview2  0xc28f21b20080  7       -       1       False   2024-05-22 07:54:35.000000      N/A     Disabled
6948    1928    msedgewebview2  0xc28f233a2080  16      -       1       False   2024-05-22 07:54:35.000000      N/A     Disabled
9200    796     svchost.exe     0xc28f25eeb080  16      -       0       False   2024-05-22 07:55:06.000000      N/A     Disabled
5172    3340    msedge.exe      0xc28f323a0080  0       -       1       False   2024-05-22 07:55:10.000000      2024-05-22 08:17:44.000000      Disabled
11252   7700    MoNotification  0xc28f26936080  0       -       1       False   2024-05-22 07:55:21.000000      2024-05-22 07:55:21.000000      Disabled
10716   964     ApplicationFra  0xc28f2680a380  4       -       1       False   2024-05-22 08:16:56.000000      N/A     Disabled
11432   7700    MoNotification  0xc28f2429a080  0       -       1       False   2024-05-22 08:16:59.000000      2024-05-22 08:17:00.000000      Disabled
12216   796     svchost.exe     0xc28f26ac2080  5       -       1       False   2024-05-22 08:17:10.000000      N/A     Disabled
7880    964     FileCoAuth.exe  0xc28f2687b080  5       -       1       False   2024-05-22 08:17:37.000000      N/A     Disabled
1780    3340    msedge.exe      0xc28f24289080  50      -       1       False   2024-05-22 08:17:44.000000      N/A     Disabled
10524   1780    msedge.exe      0xc28f26e12080  8       -       1       False   2024-05-22 08:17:44.000000      N/A     Disabled
7884    1780    msedge.exe      0xc28f24b2c080  17      -       1       False   2024-05-22 08:17:44.000000      N/A     Disabled
11744   1780    msedge.exe      0xc28f231c5080  14      -       1       False   2024-05-22 08:17:44.000000      N/A     Disabled
9544    1780    msedge.exe      0xc28f26812080  9       -       1       False   2024-05-22 08:17:44.000000      N/A     Disabled
7188    1780    msedge.exe      0xc28f24911080  16      -       1       False   2024-05-22 08:17:58.000000      N/A     Disabled
4768    1780    msedge.exe      0xc28f27ad6240  14      -       1       False   2024-05-22 08:17:58.000000      N/A     Disabled
11628   964     Microsoft.Phot  0xc28f23570080  15      -       1       False   2024-05-22 08:18:05.000000      N/A     Disabled
11492   964     RuntimeBroker.  0xc28f242a2080  6       -       1       False   2024-05-22 08:18:07.000000      N/A     Disabled
5912    964     CHXSmartScreen  0xc28f21c5a080  36      -       1       False   2024-05-22 08:18:09.000000      N/A     Disabled
11904   796     VSSVC.exe       0xc28f26828080  6       -       0       False   2024-05-22 08:18:39.000000      N/A     Disabled
11588   9844    mshta.exe       0xc28f24458080  17      -       1       False   2024-05-22 08:19:55.000000      N/A     Disabled
2848    9844    mshta.exe       0xc28f23397080  17      -       1       False   2024-05-22 08:19:55.000000      N/A     Disabled
10816   796     svchost.exe     0xc28f24c4f080  7       -       0       False   2024-05-22 08:20:01.000000      N/A     Disabled
9240    964     RuntimeBroker.  0xc28f24457080  12      -       1       False   2024-05-22 08:20:32.000000      N/A     Disabled
11040   1780    msedge.exe      0xc28f2485c080  9       -       1       False   2024-05-22 08:20:44.000000      N/A     Disabled
```

- **python .\vol.py -f ..\vm\windows-Snapshot2.vmem windows.cmdline**

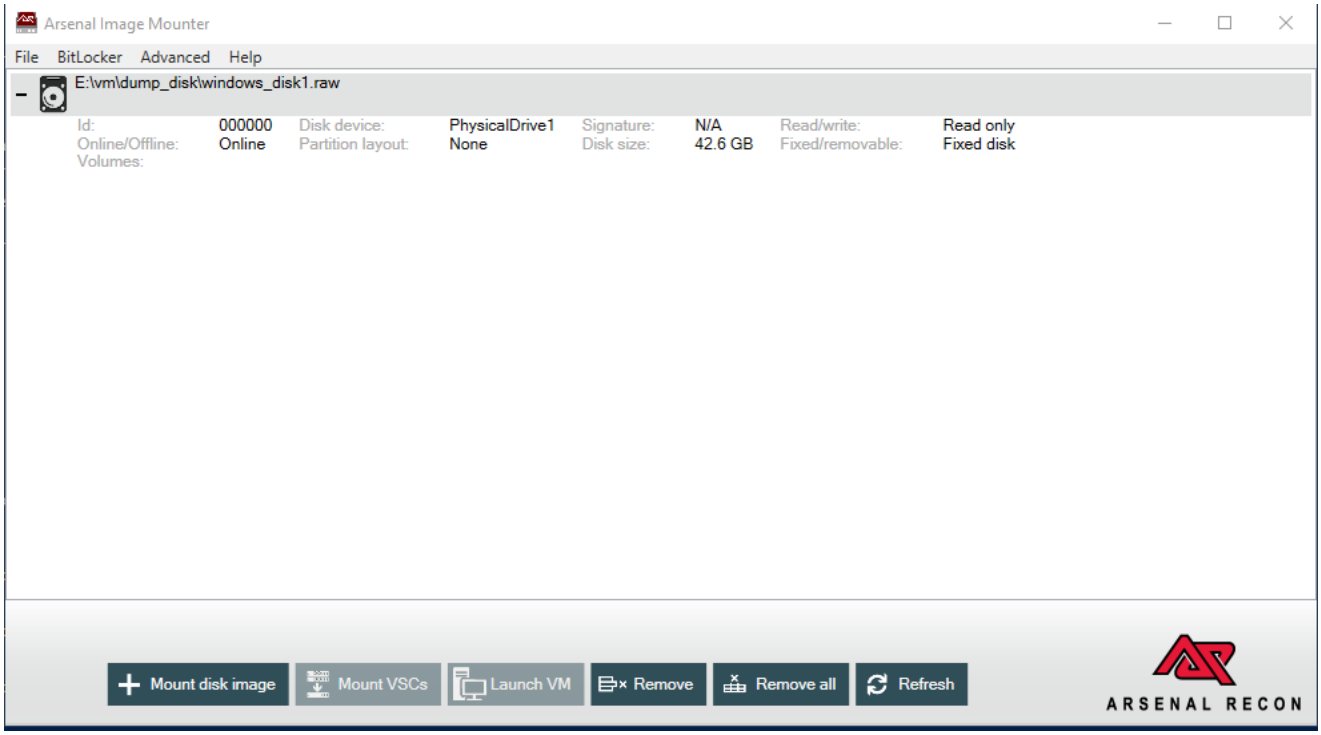
```
PS E:\volatility3> python .\vol.py -f ..\vm\windows-Snapshot2.vmem windows.cmdline
Volatility 3 Framework 2.7.0
Progress:  100.00               PDB scanning finished
PID     Process Args

4       System  Required memory at 0x20 is not valid (process exited?)
76      Secure System   Required memory at 0x20 is not valid (process exited?)
112     Registry        Required memory at 0x20 is not valid (process exited?)
420     smss.exe        \SystemRoot\System32\smss.exe
556     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
656     wininit.exe     wininit.exe
664     csrss.exe       %SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDll=basesrv,1 ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=sxssrv,4 ProfileControl=Off MaxRequestThreads=16
748     winlogon.exe    winlogon.exe
796     services.exe    C:\Windows\system32\services.exe
816     LsaIso.exe      \??\C:\Windows\system32\lsaiso.exe -CredGuard -KeyGuard
832     lsass.exe       C:\Windows\system32\lsass.exe
964     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p
992     fontdrvhost.ex  "fontdrvhost.exe"
1000    fontdrvhost.ex  "fontdrvhost.exe"
648     svchost.exe     C:\Windows\system32\svchost.exe -k RPCSS -p
920     svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
1056    sppsvc.exe      Required memory at 0xa8d522b020 is not valid (process exited?)
1084    dwm.exe "dwm.exe"
1124    svchost.exe     C:\Windows\system32\svchost.exe -k DcomLaunch -p -s DeviceInstall
1188    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork -p
1280    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s DispBrokerDesktopSvc
1496    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
1544    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
1644    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
1652    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -s W32Time
1704    svchost.exe     C:\Windows\System32\svchost.exe -k netprofm -p -s netprofm
1868    svchost.exe     C:\Windows\system32\svchost.exe -k UserProfileService -p -s ProfSvc
1892    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
1900    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService -p
1908    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s HvHost
1940    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService -p
1948    svchost.exe     C:\Windows\System32\svchost.exe -k wsappx -p -s ClipSVC
8       svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
1468    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
2104    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s AppIDSvc
2320    svchost.exe     C:\Windows\system32\svchost.exe -k appmodel -p -s StateRepository
2396    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
2476    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc
2492    svchost.exe     C:\Windows\system32\svchost.exe -k NetSvcs -p -s hns
2572    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
2644    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
2668    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s WinHttpAutoProxySvc
2676    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s SysMain
2704    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
2852    MemCompression  Required memory at 0x20 is not valid (process exited?)
2868    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
2952    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
3008    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TextInputManagementService
2652    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
2788    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p
3136    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s ShellHWDetection
3168    svchost.exe     C:\Windows\system32\svchost.exe -k NetSvcs -s nvagent
3276    spoolsv.exe     C:\Windows\System32\spoolsv.exe
3320    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
3368    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetworkFirewall -p
3440    svchost.exe     C:\Windows\System32\svchost.exe -k NetworkService -p -s LanmanWorkstation
3596    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s SharedAccess
3708    MsMpEng.exe     "C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24020.7-0\MsMpEng.exe"
3940    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Winmgmt
3892    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
4968    svchost.exe     C:\Windows\System32\svchost.exe -k NetSvcs -p -s iphlpsvc
4976    svchost.exe     C:\Windows\System32\svchost.exe -k utcsvc -p
4984    svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNoNetwork -p -s DPS
5012    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s TrkWks
```

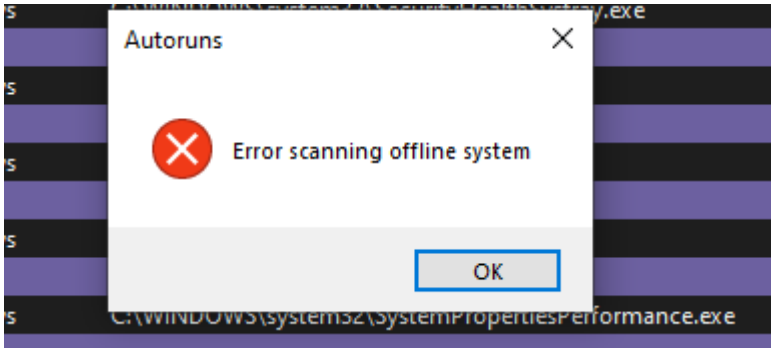
```
5060    VGAuthService.  "C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
5072    vm3dservice.ex  C:\Windows\system32\vm3dservice.exe
5080    vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
5100    wlms.exe        C:\Windows\system32\wlms\wlms.exe
5116    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s WpnService
3836    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s LanmanServer
4172    vm3dservice.ex  vm3dservice.exe -n
4392    svchost.exe     C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s WdiSystemHost
4588    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc
4896    AggregatorHost  AggregatorHost.exe
948     svchost.exe     C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -s RmSvc
4468    svchost.exe     C:\Windows\system32\svchost.exe -k WebThreatDefense -p -s webthreatdefsvc
5140    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
5240    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s fhsvc
5248    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s wuauserv
5340    sihost.exe      sihost.exe
5360    svchost.exe     C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc
5396    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s webthreatdefusersvc
5440    svchost.exe     C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService
5592    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s TokenBroker
5716    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s CDPSvc
5808    userinit.exe    Required memory at 0xdefb2e4020 is not valid (process exited?)
5832    explorer.exe    C:\Windows\Explorer.EXE
5860    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
6068    taskhostw.exe   taskhostw.exe {222A245B-E637-4AE9-A93F-A59CA119A75E}
6092    taskhostw.exe   taskhostw.exe
6484    dllhost.exe     C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
6544    VMwareResoluti  Required memory at 0x7b88179020 is not valid (process exited?)
6604    msdtc.exe       C:\Windows\System32\msdtc.exe
6696    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s Appinfo
6800    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s LicenseManager
7072    svchost.exe     C:\Windows\system32\svchost.exe -k osprivacy -p -s camsvc
6320    ctfmon.exe      "ctfmon.exe"
6992    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s lfsvc
7484    msedge.exe      Required memory at 0x704b558020 is not valid (process exited?)
7312    svchost.exe     C:\Windows\system32\svchost.exe -k ClipboardSvcGroup -p -s cbdhsvc
7912    SearchHost.exe  "C:\Windows\SystemApps\MicrosoftWindows.Client.CBS_cw5n1h2txyewy\SearchHost.exe" -ServerName:CortanaUI.AppXstmwaab17q5s3y22tp6apqz7a45vwv65.mca
7492    StartMenuExper  "C:\Windows\SystemApps\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy\StartMenuExperienceHost.exe" -ServerName:App.AppXywbrabmsek0gm3tkwpr5kwzbs55tkqay.mca
8024    Widgets.exe     "C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience_424.1301.310.0_x64__cw5n1h2txyewy\Dashboard\Widgets.exe" -ServerName:Microsoft.Windows.DashboardServer
6148    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
8056    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
7268    svchost.exe     C:\Windows\system32\svchost.exe -k UdkSvcGroup -s UdkUserSvc
8408    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s UsoSvc
8924    dllhost.exe     C:\Windows\System32\DllHost.exe /Processid:{973D20D7-562D-44B9-B70B-5A0F49CCDF3F}
8760    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation -p -s SSDPSRV
3780    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s StorSvc
4184    SecurityHealth  "C:\Windows\System32\SecurityHealthSystray.exe"
7552    SecurityHealth  C:\Windows\system32\SecurityHealthService.exe
8240    vmtoolsd.exe    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
7992    OneDrive.exe     /updateInstalled /background
3376    Microsoft.Shar  Required memory at 0xb6f335020 is not valid (process exited?)
2512    uhssvc.exe      "C:\Program Files\Microsoft Update Health Tools\uhssvc.exe"
9012    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s wscsvc
5232    svchost.exe     C:\Windows\system32\svchost.exe -k UnistackSvcGroup
2540    WidgetService.  "C:\Program Files\WindowsApps\MicrosoftWindows.Client.WebExperience_424.1301.310.0_x64__cw5n1h2txyewy\Dashboard\widgetservice.exe" -RegisterProcessAsComServer -Embedding
6640    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkService -p
7512    ShellExperienc  "C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienceHost.exe" -ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
1172    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s NPSMSvc
6744    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
5096    SystemSettings  C:\Windows\System32\SystemSettingsBroker.exe -Embedding
7128    svchost.exe     C:\Windows\system32\svchost.exe -k LocalService -p -s SstpSvc
5980    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs
2516    svchost.exe     C:\Windows\system32\svchost.exe -k InvSvcGroup -p -s InventorySvc
4036    svchost.exe     C:\Windows\System32\svchost.exe -k wsappx -p -s AppXSvc
5676    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p
7700    MoUsoCoreWorke  "C:\Windows\uus\packages\preview\AMD64\MoUsoCoreWorker.exe" useprivatenamespaces
1824    SearchProtocol  "C:\Windows\System32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe3_ Global\UsGthrCtrlFltPipeMssGthrPipe3 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\Program
Data\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
6404    TrustedInstall  C:\Windows\servicing\TrustedInstaller.exe
2080    TiWorker.exe    C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.22621.3294_none_e96368b442c95c86\TiWorker.exe -Embedding
808     MoNotification  Required memory at 0x94072d9020 is not valid (process exited?)
6624    svchost.exe     C:\Windows\System32\svchost.exe -k swprv
```

```
1596    smartscreen.ex  C:\Windows\System32\smartscreen.exe -Embedding
7924    MoNotification  Required memory at 0x9ed798d020 is not valid (process exited?)
8568    MoNotification  Required memory at 0x61eb2a020 is not valid (process exited?)
6452    svchost.exe     C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p -s DisplayEnhancementService
8164    svchost.exe     C:\Windows\system32\svchost.exe -k netsvcs -p -s wlidsvc
4828    setup.exe       "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\124.0.2478.97\Installer\setup.exe" --msedgewebview --delete-old-versions --system-level --verbose-logging
8632    setup.exe       Required memory at 0x1fca2003958 is inaccessible (swapped)
1928    msedgewebview2  "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\124.0.2478.97\msedgewebview2.exe" --embedded-browser-webview=1 --webview-exe-name=Widgets.exe --webview-exe-version=424.1301.2810.0 --user-data-dir="C:\Users\User\AppData\Local\Packages\Mic
rosoftWindows.Client.WebExperience_cw5n1h2txyewy\LocalState\EBWebView" --noerrdialogs --disk-cache-size=52428800 --edge-webview-is-background --enable-features=MojoIpcz,msWebView2TreatAppSuspendAsDeviceSuspend,UseNativeThreadPool,UseBackgroundNativeThreadPool --lang=en-U
S --accept-lang=en-US --mojo-named-platform-channel-pipe=8024.2600.10930987773641015903 /pfhostedapp:017373b2a5c4ead1a08d36a47bf86195c1909a61
7940    msedgewebview2  "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\124.0.2478.97\msedgewebview2.exe" --type=crashpad-handler --user-data-dir=C:\Users\User\AppData\Local\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\LocalState\EBWebView /pref
etch:4 /pfhostedapp:017373b2a5c4ead1a08d36a47bf86195c1909a61 --monitor-self-annotation=ptype=crashpad-handler --database=C:\Users\User\AppData\Local\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\LocalState\EBWebView\Crashpad --annotation=IsOfficialBuild=1
--annotation=channel= --annotation=chromium-version=124.0.6367.201 "--annotation=exe=C:\Program Files (x86)\Microsoft\EdgeWebView\Application\124.0.2478.97\msedgewebview2.exe" --annotation=plat=Win64 "--annotation=prod=Edge WebView2" --annotation=ver=124.0.2478.97 --init
ial-client-data=0x188,0x18c,0x190,0x164,0xfc,0x7ff97d14ceb8,0x7ff97d14cec4,0x7ff97d14ced0
516     msedgewebview2  "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\124.0.2478.97\msedgewebview2.exe" --type=gpu-process --noerrdialogs --user-data-dir="C:\Users\User\AppData\Local\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\LocalState\EBWe
bView" --webview-exe-name=Widgets.exe --webview-exe-version=424.1301.2810.0 --embedded-browser-webview=1 --no-appcompat-clear --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAAABgAAEAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAA
ACAAAAAAAAAAIAAAAAAAAAA== --field-trial-handle=1792,i,9908701659734863087,13320741331555279057,262144 --enable-features=MojoIpcz,UseBackgroundNativeThreadPool,UseNativeThreadPool,msWebView2TreatAppSuspendAsDeviceSuspend --variations-seed-version --mojo-platform-channel-h
andle=1780 /prefetch:2 /pfhostedapp:017373b2a5c4ead1a08d36a47bf86195c1909a61
3896    msedgewebview2  "C:\Program Files (x86)\Microsoft\EdgeWebView\Application\124.0.2478.97\msedgewebview2.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --noerrdialogs --user-data-dir="C:\Users\User\AppDa
ta\Local\Packages\MicrosoftWindows.Client.WebExperience_cw5n1h2txyewy\LocalState\EBWebView" --webview-exe-name=Widgets.exe --webview-exe-version=424.1301.2810.0 --embedded-browser-webview=1 --no-appcompat-clear --field-trial-handle=2040,i,9908701659734863087,133207413315
55279057,262144 --enable-features=MojoIpcz,UseBackgroundNativeThreadPool,UseNativeThreadPool,msWebView2TreatAppSuspendAsDeviceSuspend --variations-seed-version --mojo-platform-channel-handle=2052 /prefetch:3 /pfhostedapp:017373b2a5c4ead1a08d36a47bf86195c1909a61
1772    msedgewebview2  Required memory at 0x1b5c8203ec8 is inaccessible (swapped)
6948    msedgewebview2  Required memory at 0x2370f003478 is inaccessible (swapped)
9200    svchost.exe     C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
5172    msedge.exe      Required memory at 0x109d7dd020 is not valid (process exited?)
11252   MoNotification  Required memory at 0x6ffd78f020 is not valid (process exited?)
10716   ApplicationFra  C:\Windows\system32\ApplicationFrameHost.exe -Embedding
11432   MoNotification  Required memory at 0x45e88af020 is not valid (process exited?)
12216   svchost.exe     C:\Windows\system32\svchost.exe -k DevicesFlow -s DevicesFlowUserSvc
7880    FileCoAuth.exe  "C:\Users\User\AppData\Local\Microsoft\OneDrive\24.086.0428.0003\FileCoAuth.exe" -Embedding
1780    msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window
10524   msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=crashpad-handler "--user-data-dir=C:\Users\User\AppData\Local\Microsoft\Edge\User Data" /prefetch:4 --monitor-self-annotation=ptype=crashpad-handler "--database=C:\Users\User\Ap
pData\Local\Microsoft\Edge\User Data\Crashpad" --annotation=IsOfficialBuild=1 --annotation=channel= --annotation=chromium-version=125.0.6422.60 "--annotation=exe=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --annotation=plat=Win64 "--annotation=prod=Micr
osoft Edge" --annotation=ver=125.0.2535.51 --initial-client-data=0x278,0x27c,0x280,0x274,0x26c,0x7ff96e984ef8,0x7ff96e984f04,0x7ff96e984f10
7884    msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=gpu-process --gpu-preferences=WAAAAAAAAADgAAAMAAAAAAAAAAAAAAAAAAABgAAEAAAA4AAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAAAAAAAYAAAAAAAAAAgAAAAAAAAACAAAAAAAAAAIAAAAAAA
AAA== --field-trial-handle=2376,i,17037322556382253008,2625893060075047516,262144 --variations-seed-version --mojo-platform-channel-handle=2368 /prefetch:2
11744   msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --field-trial-handle=2216,i,17037322556382253008,2625893060075047516,262144 --va
riations-seed-version --mojo-platform-channel-handle=2652 /prefetch:3
9544    msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=storage.mojom.StorageService --lang=en-US --service-sandbox-type=service --field-trial-handle=2792,i,17037322556382253008,2625893060075047516,262144 -
-variations-seed-version --mojo-platform-channel-handle=2904 /prefetch:8
7188    msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --instant-process --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=11
 --time-ticks-at-unix-epoch=-1716364876661551 --launch-time-ticks=1002053753 --field-trial-handle=5988,i,17037322556382253008,2625893060075047516,262144 --variations-seed-version --mojo-platform-channel-handle=5492 /prefetch:1
4768    msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=renderer --lang=en-US --js-flags=--ms-user-locale= --device-scale-factor=1 --num-raster-threads=2 --enable-main-frame-before-activation --renderer-client-id=12 --time-ticks-at-u
nix-epoch=-1716364876661551 --launch-time-ticks=1002105427 --field-trial-handle=5896,i,17037322556382253008,2625893060075047516,262144 --variations-seed-version --mojo-platform-channel-handle=5844 /prefetch:1
11628   Microsoft.Phot  Required memory at 0x22676a039f8 is inaccessible (swapped)
11492   RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
5912    CHXSmartScreen  "C:\Windows\SystemApps\Microsoft.Windows.AppRep.ChxApp_cw5n1h2txyewy\CHXSmartScreen.exe" -ServerName:App.AppXk7vvv12h4qrkhkbvf6j86ja45mzj5km9.mca
11904   VSSVC.exe       C:\Windows\system32\vssvc.exe
11588   mshta.exe       "C:\Windows\System32\mshta.exe" "C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta"
2848    mshta.exe       "C:\Windows\System32\mshta.exe" "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Info.hta"
10816   svchost.exe     C:\Windows\system32\svchost.exe -k wusvcs -p -s WaaSMedicSvc
9240    RuntimeBroker.  C:\Windows\System32\RuntimeBroker.exe -Embedding
11040   msedge.exe      "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.mojom.AssetStoreService --lang=en-US --service-sandbox-type=asset_store_service --field-trial-handle=1192,i,17037322556382253008,262589306
0075047516,262144 --variations-seed-version --mojo-platform-channel-handle=4176 /prefetch:8
PS E:\volatility3>
```




```
PS C:\Program Files (x86)\VMware\VMware Workstation> .\vmware-vdiskmanager.exe -r "E:\vm\infected_windows\windows-disk1-c11.vmdk" -t 0 "E:\vm\dump_disk\windows_disk1.raw"
SSLConfigLoad: Failed to load OpenSSL config file.
Creating disk 'E:\vm\dump_disk\windows_disk1.raw'
  Convert: 100% done.
Virtual disk conversion successful.
PS C:\Program Files (x86)\VMware\VMware Workstation>
```


Arsenal Image Mounter
File BitLocker Advanced Help
E:\vm\dump_disk\windows_disk1.raw
Id: 000000
Online/Offline: Online
Volumes:
Disk device: PhysicalDrive1
Partition layout: None
Signature: N/A
Disk size: 42.6 GB
Read/write: Read only
Fixed/removable: Fixed disk
Mount disk image
Mount VSCs
Launch VM
Remove
Remove all
Refresh
ARSENAL RECON


Autoruns
Error scanning offline system
OK
C:\WINDOWS\system32\SystemPropertiesPerformance.exe