LAB REPORT

25th February 2025

Volatile Memory Acquisition Practical

Name : Sarthak Das

Session : 11th February – 22nd April 2025

For the class of Computer Forensic, taught by

Drabanti Boral

Contents

1 Introduction

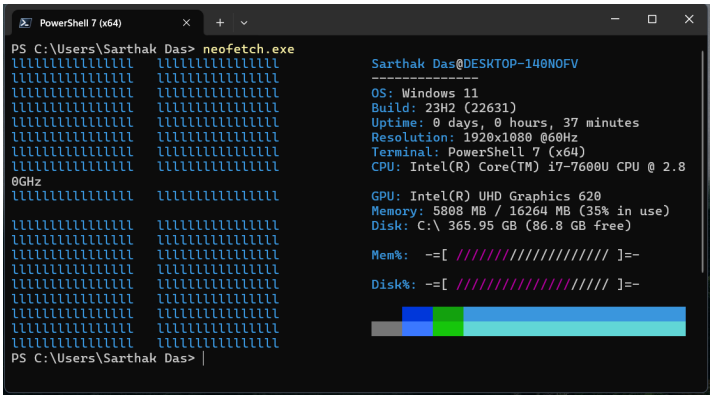
1.1 Objectives

This report is a documentation of my lab work as assigned on 20th February, 2025. The primary objectives of this lab are two-fold:

- Live capture of RAM and memory dump generation.
- Extracting process list from memory dump files.

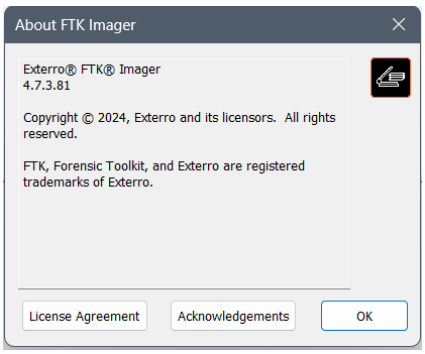
1.2 System Information

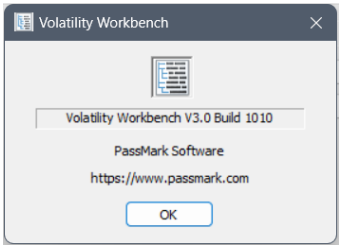
For the purposes of this lab, a Lenovo ThinkPad X270 was used, having the following system specifications: Intel Core i7-7600U CPU @ 2.80GHz with Intel UHD Graphics 620, 16GB RAM, 1TB SSD running operating system Windows 11 23H2 (Build 22631).



1.3 Software Used

The software used for this volatile memory acquisition practical are Exterro FTK Imager version 4.7.3.81, Belkasoft Live RAM Capturer, and Passmark Volatility Workbench version 3.0 Build 1010 (a GUI for Volatility 3 Framework version 2.11.0).

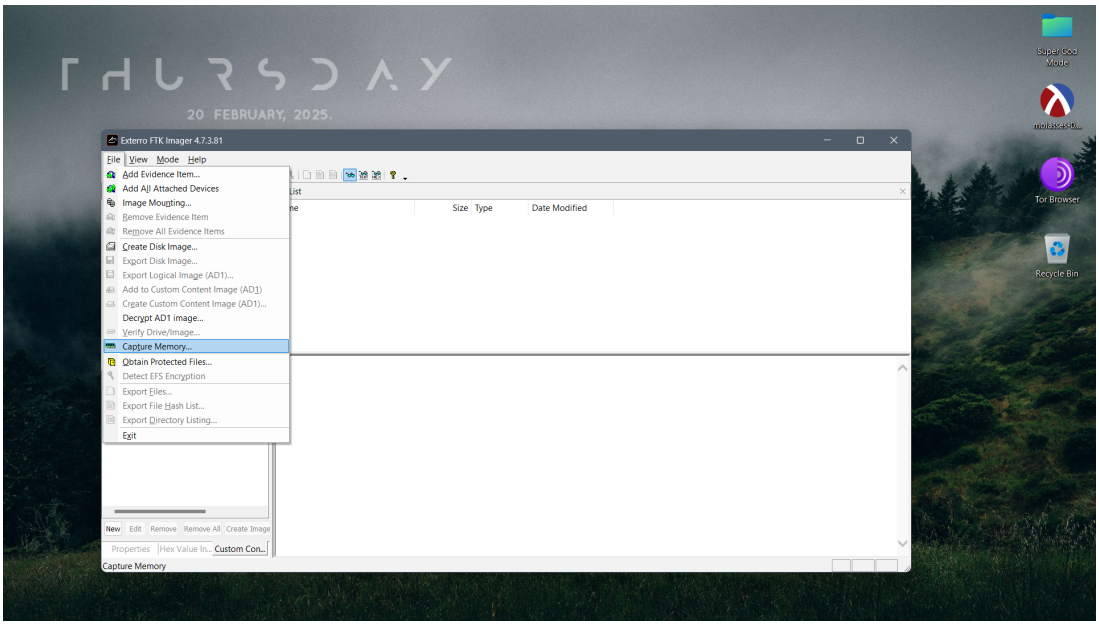




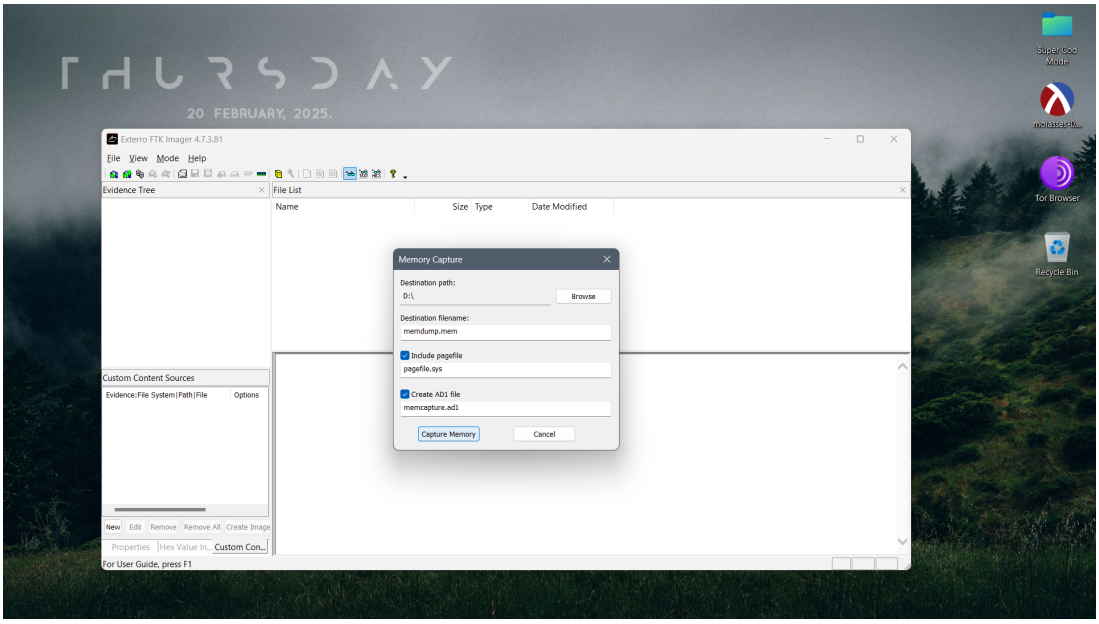
2 Objective 1: Generating Memory Dump

2.1 Methodology: Exterro FTK Imager

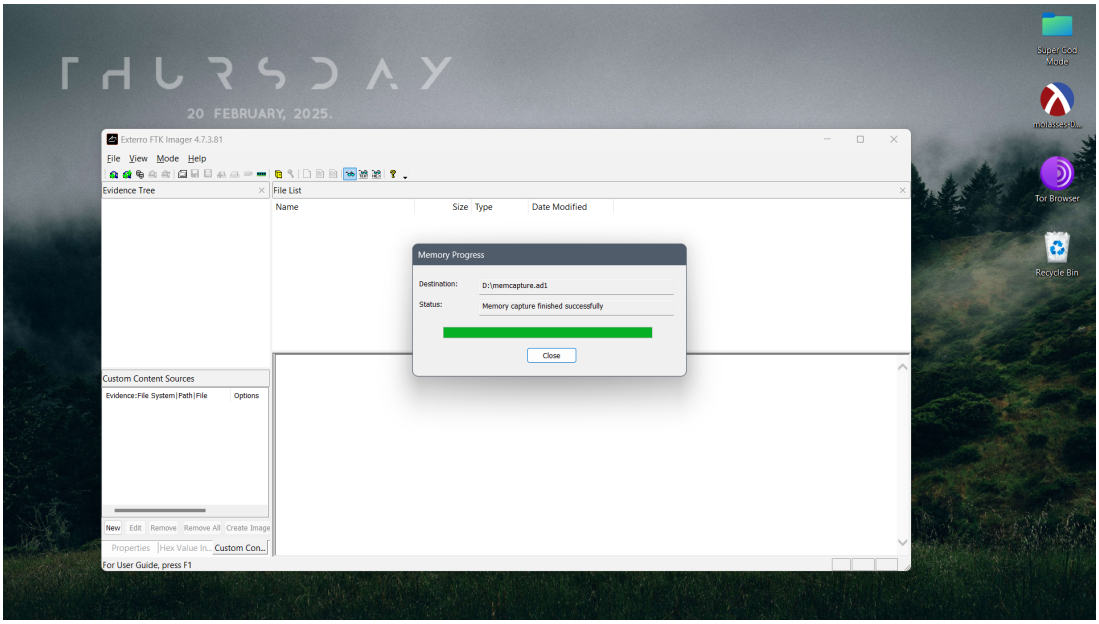
We begin by opening Exterro FTK Imager, and selecting **File** > *Capture Memory*.



We select the destination path, uncheck the boxes *Include pagefile* and *Create AD1 file*, and click **Capture Memory**.

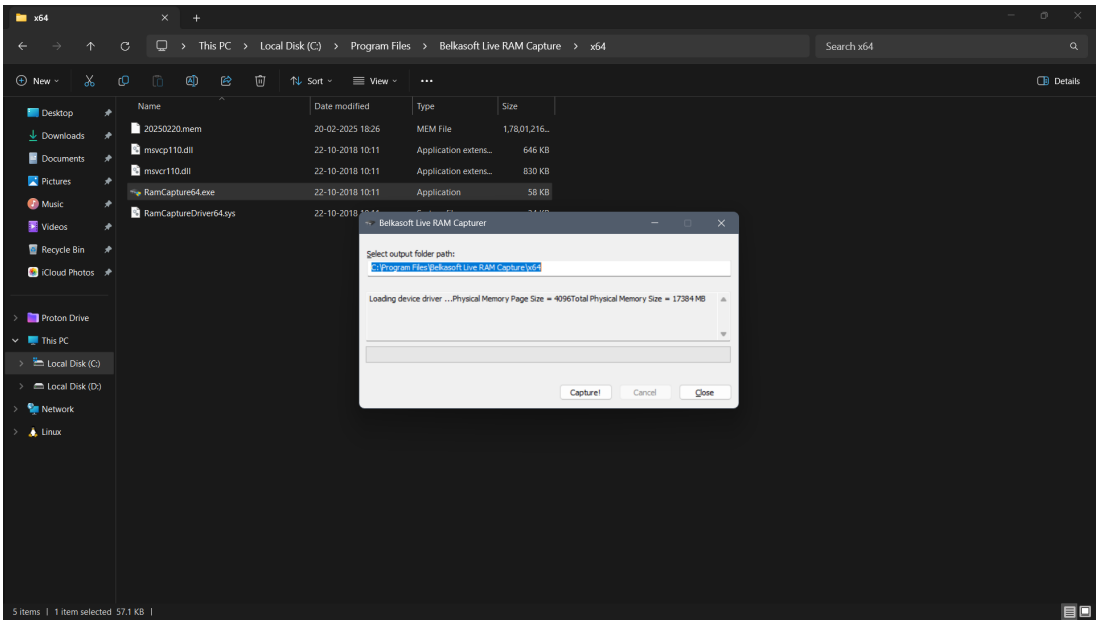


After some time, it shows that the memory capture was successful and the memory dump was generated.

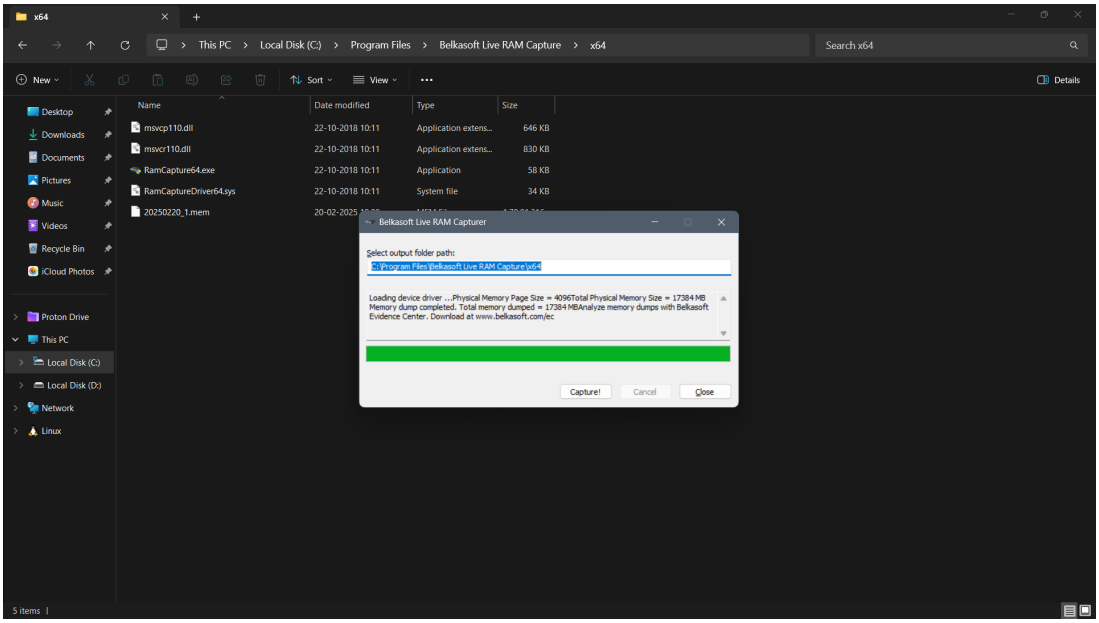


2.2 Methodology: Belkasoft Live RAM Capturer

We begin by opening Belkasoft Live RAM Capturer, selecting the output folder path, and clicking **Capture!**



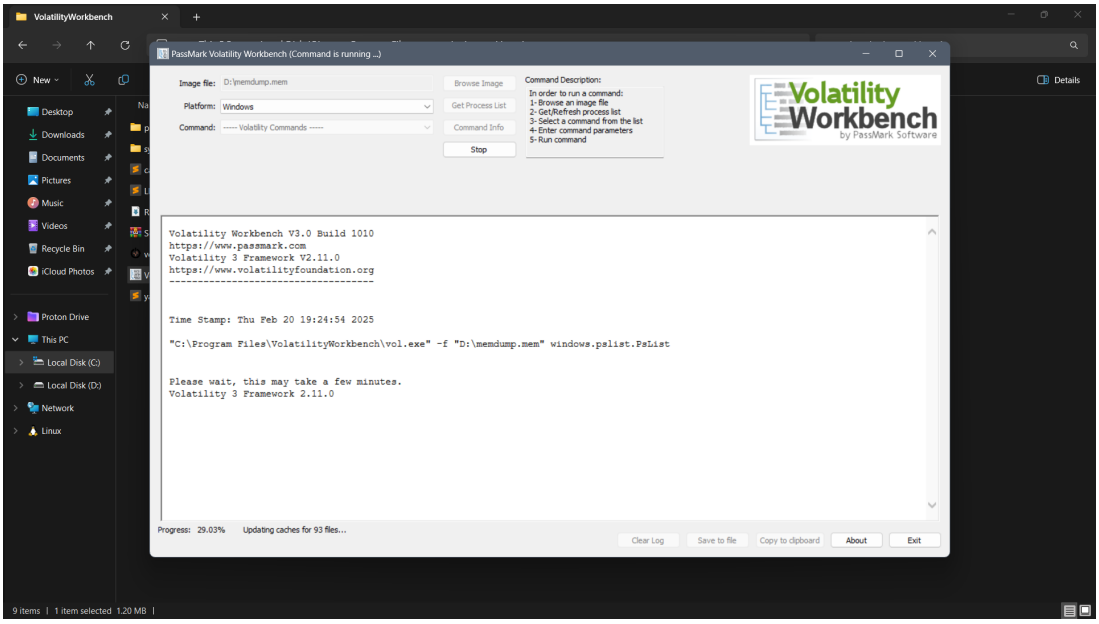
After some time, it shows that the memory dump was completed.



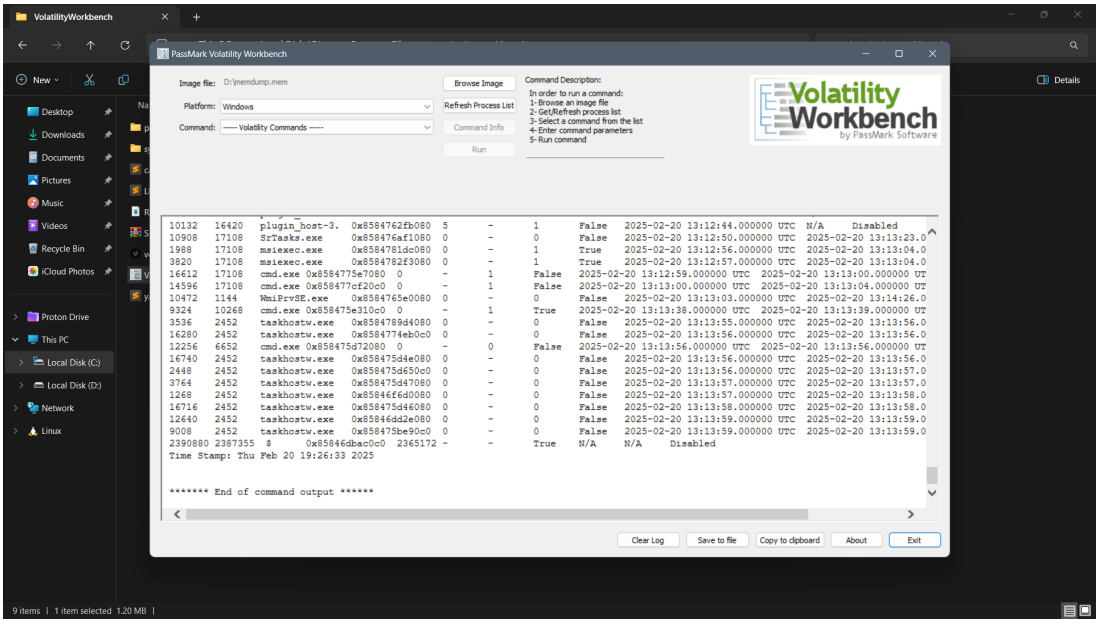
3 Objective 2: Analyzing Memory Dump

3.1 Methodology

In order to analyze a memdump file, we open Volatility Workbench, select our memdump file and click **Get Process List**.



Upon completion, we can click **Save to file** to save the command output to a text file.



3.2 Command Output for Memdump generated by Exterro FTK Imager

Command Output generated by Volatility Workbench

```
PassMark Volatility Workbench Log file  -  http://www.passmark.com
================================================================
Volatility Workbench Version: V3.0 Build 1010
Volatility 3 Framework Version: 2.11.0
Log Date: Thu Feb 20 19:28:07 2025


Time Stamp: Thu Feb 20 19:24:54 2025

"C:\Program Files\VolatilityWorkbench\vol.exe" -f "D:\memdump.mem" windows.pslist.PsList
Volatility 3 Framework 2.11.0
PID	PPID	ImageFileName	OffsetV	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
4	0	System	0x858464cca040	266	-	N/A	False	2025-02-20 13:05:42.000000 UTC	N/A	Disabled
76	4	Secure System	0x858464d3e040	0	-	N/A	False	2025-02-20 13:05:37.000000 UTC	N/A	Disabled
120	4	Registry	0x858464df0040	4	-	N/A	False	2025-02-20 13:05:37.000000 UTC	N/A	Disabled
596	4	smss.exe	0x8584677ea040	2	-	N/A	False	2025-02-20 13:05:42.000000 UTC	N/A	Disabled
896	880	csrss.exe	0x85846b795140	11	-	0	False	2025-02-20 13:05:47.000000 UTC	N/A	Disabled
984	880	wininit.exe	0x85846c9770c0	2	-	0	False	2025-02-20 13:05:47.000000 UTC	N/A	Disabled
1004	976	csrss.exe	0x85846c9550c0	15	-	1	False	2025-02-20 13:05:47.000000 UTC	N/A	Disabled
836	984	services.exe	0x85846c9f0080	10	-	0	False	2025-02-20 13:05:47.000000 UTC	N/A	Disabled
856	984	WerFault.exe	0x85846c9f8080	0	-	0	False	2025-02-20 13:05:48.000000 UTC	2025-02-20 13:08:31.000000 U
876	984	LsaIso.exe	0x85846ca84080	3	-	0	False	2025-02-20 13:05:48.000000 UTC	N/A	Disabled
884	984	lsass.exe	0x85846ca870c0	10	-	0	False	2025-02-20 13:05:48.000000 UTC	N/A	Disabled
1144	836	svchost.exe	0x85846cb38080	26	-	0	False	2025-02-20 13:05:48.000000 UTC	N/A	Disabled
1172	836	svchost.exe	0x85846cb5f080	12	-	0	False	2025-02-20 13:05:48.000000 UTC	N/A	Disabled
1180	984	fontdrvhost.ex	0x85846cb5c080	5	-	0	False	2025-02-20 13:05:48.000000 UTC	N/A	Disabled
1284	836	svchost.exe	0x85846cc6d080	10	-	0	False	2025-02-20 13:05:48.000000 UTC	N/A	Disabled
1308	836	svchost.exe	0x85846ccc50c0	5	-	0	False	2025-02-20 13:05:48.000000 UTC	N/A	Disabled
1420	976	winlogon.exe	0x85846cde60c0	5	-	1	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1472	1420	fontdrvhost.ex	0x85846ce4e080	5	-	1	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1544	836	svchost.exe	0x85846ce5d080	2	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1596	836	svchost.exe	0x85846ceb0080	3	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1600	836	svchost.exe	0x85846ceac0c0	4	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1612	836	svchost.exe	0x85846ceb3080	4	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1620	836	svchost.exe	0x85846ceaf080	6	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1716	836	svchost.exe	0x85846ceed080	7	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1724	836	svchost.exe	0x85846ceef080	3	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1808	836	svchost.exe	0x85846d05a080	4	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1892	836	IntelCpHDCPSvc	0x85846d073180	4	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
```

1916	836	svchost.exe	0x85846d074080	15	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1928	836	svchost.exe	0x85846d07e080	5	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1964	836	svchost.exe	0x85846d09d080	10	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2012	836	svchost.exe	0x85846d0c2080	5	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1212	1420	dwm.exe	0x85846d12e0c0	20	-	1	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1712	836	svchost.exe	0x85846d137080	8	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2120	836	svchost.exe	0x85846d1b4080	5	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2140	836	IntelCpHeciSvc	0x85846d1b9180	4	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2372	836	svchost.exe	0x85846cf9a0c0	6	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2408	836	svchost.exe	0x85846cfd6080	2	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2452	836	svchost.exe	0x85846d2240c0	12	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2460	836	svchost.exe	0x85846d227080	9	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2484	836	WUDFHost.exe	0x85846d226080	6	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2540	836	svchost.exe	0x85846d23d080	2	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2716	836	svchost.exe	0x85846d2ed080	1	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2736	836	svchost.exe	0x85846d2f0080	1	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2804	836	svchost.exe	0x85846d393080	5	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2944	836	ibmpmsvc.exe	0x85846d3c1180	11	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
2952	836	LITSSvc.exe	0x85846d3c9180	6	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
2960	836	svchost.exe	0x85846d3c4080	6	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
2092	836	svchost.exe	0x85846d454080	7	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3108	836	svchost.exe	0x85846d47b080	4	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3196	836	svchost.exe	0x85846d4c60c0	5	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3208	836	svchost.exe	0x85846d4c4080	8	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3216	836	svchost.exe	0x85846d4c9080	3	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3300	4	MemCompression	0x85846d4eb040	30	-	N/A	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3316	836	svchost.exe	0x85846d5650c0	2	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3340	836	igfxCUIService	0x85846d5aa180	4	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3396	836	svchost.exe	0x85846d6020c0	7	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3404	836	svchost.exe	0x85846d5d2080	2	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3600	836	svchost.exe	0x858464c98080	7	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3656	836	svchost.exe	0x85846d83b080	11	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3724	836	svchost.exe	0x85846d8820c0	3	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3732	836	svchost.exe	0x85846d8a3080	6	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3804	836	RtkAudioServic	0x85846d8ee080	3	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3904	836	svchost.exe	0x85846da85080	16	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4004	3656	audiodg.exe	0x85846da94140	9	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4020	836	svchost.exe	0x85846dbde0c0	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4036	836	svchost.exe	0x85846dbe3080	13	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4048	836	svchost.exe	0x85846dbe2080	7	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4084	836	svchost.exe	0x85846dc37080	16	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4132	836	svchost.exe	0x85846dc31080	1	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled

4504	836	svchost.exe	0x85846dd65080	11	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4544	836	svchost.exe	0x85846ddb0080	2	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4616	836	spoolsv.exe	0x85846de320c0	7	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4624	836	svchost.exe	0x85846de390c0	1	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4704	836	svchost.exe	0x85846e18a0c0	5	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4836	4504	wlanext.exe	0x85846e1350c0	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4860	4836	conhost.exe	0x85846e0df0c0	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4884	836	svchost.exe	0x85846e19b0c0	1	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4892	836	svchost.exe	0x85846e0350c0	5	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4916	836	avp.exe	0x85846dedc0c0	148	-	0	True	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4952	836	svchost.exe	0x85846e175080	4	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4960	836	mDNSResponder.	0x85846deda080	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4968	836	svchost.exe	0x85846dedb080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4976	836	svchost.exe	0x85846dfeb080	10	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4984	836	OfficeClickToR	0x85846e133140	17	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5000	836	svchost.exe	0x85846dfec080	16	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5032	836	esif_uf.exe	0x85846e188080	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5076	836	MainDaemon.exe	0x85846e022080	8	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5100	836	MainService.ex	0x85846e166080	22	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4204	836	httpd.exe	0x85846e033100	5	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4876	836	OneApp.IGCC.Wi	0x85846de551c0	9	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5140	836	LicenseService	0x85846e0bb0c0	14	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5152	836	RestService.ex	0x85846de890c0	7	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5220	836	TPMProvisionin	0x85846e4e7080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5276	836	jhi_service.ex	0x85846e4eb180	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5324	836	IntelAudioServ	0x85846e2d5100	9	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5384	836	svchost.exe	0x85846e2f0080	6	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5436	836	nimxs.exe	0x85846e2f7080	8	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5576	836	niauth_daemon.	0x85846e5c9100	9	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5608	836	nisvcloc.exe	0x85846e5da100	3	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5628	836	CoordService.e	0x85846e5e80c0	12	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5636	836	BuildService.e	0x85846e5e9080	13	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5644	836	nfsclnt.exe	0x85846e5ec080	8	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5704	836	openvpnserv2.e	0x85846e330080	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5764	836	openvpnserv.ex	0x85846e389080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5772	836	lkads.exe	0x85846e33e080	12	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5780	836	erlsrv.exe	0x85846e33b080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5800	836	sqlwriter.exe	0x85846e3e10c0	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5836	836	SynTPEnhServic	0x85846e3e3080	6	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5916	836	tphkload.exe	0x85846e61d180	9	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5952	836	svchost.exe	0x85846e610080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5964	836	vmware-authd.e	0x85846e66d0c0	5	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled

6016	836	vmnetdhcp.exe	0x85846e6bd080	3	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6028	836	vmware-usbarbi	0x85846e6c1100	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6104	836	vmnat.exe	0x85846e73a080	5	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5700	836	svchost.exe	0x85846e7670c0	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6188	836	wfcs.exe	0x85846e76a0c0	24	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6196	836	windhawk.exe	0x85846e7780c0	4	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6212	836	WMIRegistratio	0x85846e73e080	4	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6220	1144	WmiPrvSE.exe	0x85846e740080	8	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6252	836	wslservice.exe	0x85846e784080	5	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6260	836	CptService.exe	0x85846e789100	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6336	836	lktsrv.exe	0x85846e782080	17	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6344	836	nidmsrv.exe	0x85846e7e6100	15	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6388	836	tagsrv.exe	0x85846e7e90c0	33	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6480	836	nimdnsResponde	0x85846e89a140	3	-	0	True	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
6512	5636	redis-server.e	0x85846e8970c0	0	-	0	False	2025-02-20 13:05:53.000000 UTC	2025-02-20 13:06:06.0000	
6652	5780	erl.exe	0x85846e8a4080	93	-	0	False	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
6848	6652	conhost.exe	0x85846e9d31c0	4	-	0	False	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
7212	836	niDiscSvc.exe	0x85846ed7f140	13	-	0	True	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
7356	6652	epmd.exe	0x85846efc7080	2	-	0	False	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
7844	4204	httpd.exe	0x85846f164180	132	-	0	False	2025-02-20 13:05:54.000000 UTC	N/A	Disabled
8180	836	SystemWebServe	0x85846f186140	9	-	0	True	2025-02-20 13:05:54.000000 UTC	N/A	Disabled
8400	836	svchost.exe	0x85846f226080	25	-	0	False	2025-02-20 13:05:55.000000 UTC	N/A	Disabled
8992	6212	mofcomp.exe	0x85846f4e4140	0	-	0	True	2025-02-20 13:05:55.000000 UTC	2025-02-20 13:05:57.000000 U	
9036	1144	WmiPrvSE.exe	0x85846eace080	4	-	0	False	2025-02-20 13:05:55.000000 UTC	N/A	Disabled
9504	836	ApplicationWeb	0x85846f77e180	10	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9512	8180	NIWebServiceCo	0x85846f7df180	8	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9584	8180	NIWebServiceCo	0x85846f7f0180	8	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9636	4976	AggregatorHost	0x85846e3e4080	4	-	0	False	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9772	8180	NIWebServiceCo	0x85846f860180	8	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9868	8180	NIWebServiceCo	0x85846ef8a180	8	-	0	True	2025-02-20 13:05:57.000000 UTC	N/A	Disabled
9960	4916	avp.exe	0x85846f8ac0c0	8	-	0	True	2025-02-20 13:05:57.000000 UTC	N/A	Disabled
10052	6212	mofcomp.exe	0x85846f8b4140	0	-	0	True	2025-02-20 13:05:57.000000 UTC	2025-02-20 13:05:58.000000	
10644	9504	NIWebServiceCo	0x85846fa71180	8	-	0	True	2025-02-20 13:05:58.000000 UTC	N/A	Disabled
10944	836	svchost.exe	0x85846fb92080	9	-	0	False	2025-02-20 13:05:59.000000 UTC	N/A	Disabled
11092	5916	tposd.exe	0x85846fca90c0	8	-	1	False	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
11112	5836	SynTPEnh.exe	0x85846fcb0080	12	-	1	False	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
11168	6196	windhawk.exe	0x85846fcc1080	3	-	1	True	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
11204	3804	RAVBg64.exe	0x8584675eb080	5	-	1	False	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
10152	5916	shtctky.exe	0x8584674ec080	8	-	1	False	2025-02-20 13:06:01.000000 UTC	N/A	Disabled
11088	1712	sihost.exe	0x85846fcab080	18	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11308	836	svchost.exe	0x85846fe11080	1	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled

11316	836	svchost.exe	0x85846fe550c0	8	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11364	836	svchost.exe	0x85846feb80c0	2	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11384	836	svchost.exe	0x85846fec1080	12	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11428	2452	taskhostw.exe	0x85846feba080	9	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11452	2452	PIconStartup.e	0x85846febe080	0	-	1	True	2025-02-20 13:06:02.000000 UTC	2025-02-20 13:09:26.0000	
11480	2452	NIUpdateServic	0x85846fec90c0	0	-	1	False	2025-02-20 13:06:02.000000 UTC	2025-02-20 13:08:21.000	
11500	2452	opushutil.exe	0x85846fed2080	0	-	1	False	2025-02-20 13:06:03.000000 UTC	2025-02-20 13:06:40.0000	
11528	2452	MicrosoftEdgeU	0x85846fed5100	6	-	0	True	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11536	2452	ConditionalApp	0x85846feda0c0	0	-	1	True	2025-02-20 13:06:03.000000 UTC	2025-02-20 13:09:23.0000	
11544	2452	PowerMgr.exe	0x85846fed7080	11	-	1	True	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11560	836	PresentationFo	0x85846fed8080	5	-	0	False	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11716	836	svchost.exe	0x85846ff49080	5	-	0	False	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11724	2452	taskhostw.exe	0x85846ff4d080	0	-	1	False	2025-02-20 13:06:03.000000 UTC	2025-02-20 13:06:06.0000	
11820	836	svchost.exe	0x8584700020c0	7	-	0	False	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
12096	4916	avpui.exe	0x8584700ce0c0	26	-	1	True	2025-02-20 13:06:05.000000 UTC	N/A	Disabled
12112	11112	SynTPEnh.exe	0x8584700c50c0	0	-	1	False	2025-02-20 13:06:05.000000 UTC	2025-02-20 13:06:10.0000	
12268	2452	PowerToys.exe	0x85846ec8b080	18	-	1	False	2025-02-20 13:06:06.000000 UTC	N/A	Disabled
11392	3340	igfxEM.exe	0x858470185080	5	-	1	False	2025-02-20 13:06:06.000000 UTC	N/A	Disabled
9644	836	svchost.exe	0x85846ec8c080	8	-	0	False	2025-02-20 13:06:06.000000 UTC	N/A	Disabled
6964	12112	SynTPHelper.ex	0x85846eb560c0	2	-	1	False	2025-02-20 13:06:07.000000 UTC	N/A	Disabled
12156	836	svchost.exe	0x8584701d90c0	14	-	0	False	2025-02-20 13:06:07.000000 UTC	N/A	Disabled
12428	1420	userinit.exe	0x85846ee95080	0	-	1	False	2025-02-20 13:06:08.000000 UTC	2025-02-20 13:06:41.00000	
12612	12428	explorer.exe	0x8584702df080	115	-	1	False	2025-02-20 13:06:10.000000 UTC	N/A	Disabled
13104	12268	PowerToys.Adva	0x858470671080	15	-	1	False	2025-02-20 13:06:14.000000 UTC	N/A	Disabled
13304	6652	win32sysinfo.e	0x858470827080	2	-	0	False	2025-02-20 13:06:16.000000 UTC	N/A	Disabled
12880	1144	igfxext.exe	0x858470aa0080	3	-	1	False	2025-02-20 13:06:19.000000 UTC	N/A	Disabled
12360	1144	Widgets.exe	0x858470bdd080	10	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
12412	1144	SearchHost.exe	0x858470bcf080	39	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
1576	1144	StartMenuExper	0x858470c4a080	16	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
13320	1144	RuntimeBroker.	0x858470e8e0c0	5	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
13404	1144	RuntimeBroker.	0x858470e0e0c0	20	-	1	False	2025-02-20 13:06:21.000000 UTC	N/A	Disabled
13448	836	svchost.exe	0x858470e1f0c0	3	-	0	False	2025-02-20 13:06:21.000000 UTC	N/A	Disabled
13584	836	svchost.exe	0x858470e7d0c0	6	-	1	False	2025-02-20 13:06:22.000000 UTC	N/A	Disabled
13852	12268	PowerToys.Alwa	0x8584710f9080	4	-	1	False	2025-02-20 13:06:23.000000 UTC	N/A	Disabled
13860	12268	PowerToys.Awak	0x8584710fa080	14	-	1	False	2025-02-20 13:06:23.000000 UTC	N/A	Disabled
13924	12268	PowerToys.Colo	0x8584711760c0	0	-	1	False	2025-02-20 13:06:24.000000 UTC	2025-02-20 13:06:31.00	
14104	1144	dllhost.exe	0x85847136a080	7	-	1	False	2025-02-20 13:06:25.000000 UTC	N/A	Disabled
14324	836	svchost.exe	0x8584713cf080	4	-	0	False	2025-02-20 13:06:25.000000 UTC	N/A	Disabled
12708	12268	PowerToys.Crop	0x8584714d0080	4	-	1	False	2025-02-20 13:06:26.000000 UTC	N/A	Disabled
14452	12268	PowerToys.Fanc	0x85847153c080	7	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled
14508	12268	PowerToys.Keyb	0x85847153a080	4	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled
14564	12268	PowerToys.Mous	0x85847153b080	10	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled

14576	12268	PowerToys.Mous	0x858471539080	17	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled
14696	12268	PowerToys.Peek	0x858471196080	14	-	1	False	2025-02-20 13:06:28.000000 UTC	N/A	Disabled
14916	12268	PowerToys.Powe	0x858471188080	22	-	1	False	2025-02-20 13:06:28.000000 UTC	N/A	Disabled
14936	12268	PowerToys.Powe	0x858471189080	12	-	1	False	2025-02-20 13:06:28.000000 UTC	N/A	Disabled
15056	12268	PowerToys.Powe	0x858471194080	9	-	1	False	2025-02-20 13:06:29.000000 UTC	N/A	Disabled
15324	836	svchost.exe	0x8584710bf080	11	-	1	False	2025-02-20 13:06:30.000000 UTC	N/A	Disabled
1532	3724	ctfmon.exe	0x858470f8b080	13	-	1	False	2025-02-20 13:06:32.000000 UTC	N/A	Disabled
14792	2452	RAVBg64.exe	0x858470f460c0	5	-	1	False	2025-02-20 13:06:33.000000 UTC	N/A	Disabled
14828	2452	RAVBg64.exe	0x8584713f20c0	0	-	1	False	2025-02-20 13:06:33.000000 UTC	2025-02-20 13:06:42.000000	
14836	2452	RAVBg64.exe	0x858470fdf0c0	5	-	1	False	2025-02-20 13:06:33.000000 UTC	N/A	Disabled
14364	836	SearchIndexer.	0x8584713ec080	13	-	0	False	2025-02-20 13:06:34.000000 UTC	N/A	Disabled
11156	6652	inet_gethost.e	0x858470e8f080	5	-	0	False	2025-02-20 13:06:34.000000 UTC	N/A	Disabled
5748	836	svchost.exe	0x858471bd0080	3	-	0	False	2025-02-20 13:06:35.000000 UTC	N/A	Disabled
3960	836	svchost.exe	0x858471cd60c0	0	-	0	False	2025-02-20 13:06:37.000000 UTC	2025-02-20 13:15:14.000000 U	
15580	14828	RAVCpl64.exe	0x858470e1e080	7	-	1	False	2025-02-20 13:06:41.000000 UTC	N/A	Disabled
15772	1144	smartscreen.ex	0x8584710ca0c0	8	-	1	False	2025-02-20 13:06:50.000000 UTC	N/A	Disabled
15820	12612	brave.exe	0x8584701f60c0	47	-	1	False	2025-02-20 13:06:50.000000 UTC	N/A	Disabled
15896	15820	brave.exe	0x858471be90c0	9	-	1	False	2025-02-20 13:06:51.000000 UTC	N/A	Disabled
16076	15820	brave.exe	0x858470ee50c0	20	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
16084	15820	brave.exe	0x858470ee10c0	17	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
16108	15820	brave.exe	0x8584720500c0	10	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
16140	15820	brave.exe	0x85847204a0c0	9	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
15384	15820	brave.exe	0x8584723b00c0	28	-	1	False	2025-02-20 13:06:59.000000 UTC	N/A	Disabled
15720	12612	SecurityHealth	0x858472433080	4	-	1	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
116	836	SecurityHealth	0x85847245b080	19	-	0	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
1000	15820	brave.exe	0x85847245c080	17	-	1	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
11828	15820	brave.exe	0x858472459080	23	-	1	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
1924	836	svchost.exe	0x858470e8b080	17	-	0	False	2025-02-20 13:07:03.000000 UTC	N/A	Disabled
1948	2452	kpm_tray.exe	0x85847241a080	4	-	1	True	2025-02-20 13:07:03.000000 UTC	N/A	Disabled
3436	836	svchost.exe	0x85847238d080	5	-	0	False	2025-02-20 13:07:05.000000 UTC	N/A	Disabled
5312	2452	taskhostw.exe	0x8584723be080	3	-	1	False	2025-02-20 13:07:09.000000 UTC	N/A	Disabled
7468	15820	brave.exe	0x8584724dc0c0	29	-	1	False	2025-02-20 13:07:11.000000 UTC	N/A	Disabled
6952	12612	wfcUI.exe	0x8584740f20c0	26	-	1	False	2025-02-20 13:07:34.000000 UTC	N/A	Disabled
3608	1144	ShellExperienc	0x8584743d70c0	23	-	1	False	2025-02-20 13:07:46.000000 UTC	N/A	Disabled
11952	1144	RuntimeBroker.	0x8584745c50c0	19	-	1	False	2025-02-20 13:07:48.000000 UTC	N/A	Disabled
12220	836	aesm_service.e	0x8584756ee180	3	-	0	False	2025-02-20 13:07:57.000000 UTC	N/A	Disabled
5284	836	ksde.exe	0x8584747e60c0	38	-	0	True	2025-02-20 13:08:00.000000 UTC	N/A	Disabled
13424	836	LMS.exe	0x8584750c40c0	9	-	0	True	2025-02-20 13:08:01.000000 UTC	N/A	Disabled
3812	836	svchost.exe	0x8584747ee0c0	1	-	1	False	2025-02-20 13:08:02.000000 UTC	N/A	Disabled
16324	4916	avp.exe	0x8584756ed0c0	14	-	0	True	2025-02-20 13:08:02.000000 UTC	N/A	Disabled
2668	11088	TranslucentTB.	0x858474ac80c0	8	-	1	False	2025-02-20 13:08:07.000000 UTC	N/A	Disabled
13444	1144	unsecapp.exe	0x8584754d70c0	4	-	0	False	2025-02-20 13:08:08.000000 UTC	N/A	Disabled

2908	836	svchost.exe	0x8584750c60c0	0	-	0	False	2025-02-20 13:08:11.000000 UTC	2025-02-20 13:15:19.000000 U
10032	1144	RuntimeBroker.	0x8584753d1080	2	-	1	False	2025-02-20 13:08:16.000000 UTC	N/A	Disabled
10284	836	uhssvc.exe	0x8584752ce080	4	-	0	False	2025-02-20 13:08:18.000000 UTC	N/A	Disabled
12964	836	svchost.exe	0x858477ba3080	10	-	0	False	2025-02-20 13:08:21.000000 UTC	N/A	Disabled
13208	5284	ksdeui.exe	0x858477c10080	8	-	1	True	2025-02-20 13:08:24.000000 UTC	N/A	Disabled
6780	15820	brave.exe	0x8584753dc080	0	-	1	False	2025-02-20 13:08:25.000000 UTC	2025-02-20 13:14:13.000000 U
4560	15820	brave.exe	0x858477a66080	0	-	1	False	2025-02-20 13:08:27.000000 UTC	2025-02-20 13:14:14.000000 U
3064	12612	runonce.exe	0x858474acb080	0	-	1	True	2025-02-20 13:08:40.000000 UTC	2025-02-20 13:09:12.000000
3672	12612	Rainmeter.exe	0x858477b20080	10	-	1	False	2025-02-20 13:08:41.000000 UTC	N/A	Disabled
13868	3064	KeyScrambler.e	0x8584776e00c0	7	-	1	True	2025-02-20 13:08:41.000000 UTC	N/A	Disabled
12624	13868	KeyScrambler.e	0x8584776da080	4	-	1	False	2025-02-20 13:08:43.000000 UTC	N/A	Disabled
3776	11452	PrivacyIconCli	0x858475b5a080	6	-	1	False	2025-02-20 13:09:26.000000 UTC	N/A	Disabled
6676	15820	brave.exe	0x858477cf5080	0	-	1	False	2025-02-20 13:10:30.000000 UTC	2025-02-20 13:16:12.000000 U
15700	15820	brave.exe	0x858475eb5080	0	-	1	False	2025-02-20 13:10:34.000000 UTC	2025-02-20 13:16:12.000000
9376	15820	brave.exe	0x858475f240c0	0	-	1	False	2025-02-20 13:10:40.000000 UTC	2025-02-20 13:16:12.000000 U
3280	15820	brave.exe	0x858475dba0c0	17	-	1	False	2025-02-20 13:10:40.000000 UTC	N/A	Disabled
2396	1144	dllhost.exe	0x85847258b080	5	-	0	True	2025-02-20 13:10:56.000000 UTC	N/A	Disabled
13552	15820	brave.exe	0x858476ec6080	0	-	1	False	2025-02-20 13:10:56.000000 UTC	2025-02-20 13:16:12.000000
14080	15820	brave.exe	0x8584760680c0	9	-	1	False	2025-02-20 13:11:03.000000 UTC	N/A	Disabled
4012	15820	brave.exe	0x858475f06080	16	-	1	False	2025-02-20 13:11:06.000000 UTC	N/A	Disabled
5604	15820	brave.exe	0x858475f07080	15	-	1	False	2025-02-20 13:11:09.000000 UTC	N/A	Disabled
13804	14576	PowerToys.Mous	0x858476047080	0	-	1	False	2025-02-20 13:11:25.000000 UTC	2025-02-20 13:14:24.00
4244	15820	Exterro_FTK_Im	0x858475d60080	0	-	1	True	2025-02-20 13:11:25.000000 UTC	2025-02-20 13:13:39.0000
10268	4244	Exterro_FTK_Im	0x8584761e90c0	0	-	1	True	2025-02-20 13:11:26.000000 UTC	2025-02-20 13:13:39.0000
14384	836	svchost.exe	0x8584762450c0	4	-	1	False	2025-02-20 13:11:27.000000 UTC	N/A	Disabled
13708	1144	SystemSettings	0x858476027080	17	-	1	False	2025-02-20 13:11:27.000000 UTC	N/A	Disabled
12568	836	svchost.exe	0x85847625c0c0	2	-	0	False	2025-02-20 13:11:28.000000 UTC	N/A	Disabled
7180	836	svchost.exe	0x8584760720c0	14	-	0	False	2025-02-20 13:11:29.000000 UTC	N/A	Disabled
3128	836	svchost.exe	0x858476228080	5	-	1	False	2025-02-20 13:11:32.000000 UTC	N/A	Disabled
17108	836	msiexec.exe	0x85847620c080	8	-	0	False	2025-02-20 13:11:40.000000 UTC	N/A	Disabled
17204	17108	msiexec.exe	0x8584763cf080	0	-	1	True	2025-02-20 13:11:41.000000 UTC	2025-02-20 13:13:35.000000
3988	14364	SearchProtocol	0x8584763ca0c0	0	-	0	False	2025-02-20 13:12:03.000000 UTC	2025-02-20 13:14:45.000
16820	14364	SearchFilterHo	0x858474cc4080	0	-	0	False	2025-02-20 13:12:03.000000 UTC	2025-02-20 13:14:34.00
10520	836	VSSVC.exe	0x85846d378080	0	-	0	False	2025-02-20 13:12:10.000000 UTC	2025-02-20 13:16:01.000000 UT
10920	836	svchost.exe	0x8584764a9080	4	-	0	False	2025-02-20 13:12:10.000000 UTC	N/A	Disabled
16420	12612	sublime_text.e	0x858476268080	16	-	1	False	2025-02-20 13:12:42.000000 UTC	N/A	Disabled
4444	16420	crash_handler.	0x8584760510c0	8	-	1	False	2025-02-20 13:12:42.000000 UTC	N/A	Disabled
13484	16420	plugin_host-3.	0x8584762750c0	5	-	1	False	2025-02-20 13:12:43.000000 UTC	N/A	Disabled
10132	16420	plugin_host-3.	0x8584762fb080	5	-	1	False	2025-02-20 13:12:44.000000 UTC	N/A	Disabled
10908	17108	SrTasks.exe	0x858476af1080	0	-	0	False	2025-02-20 13:12:50.000000 UTC	2025-02-20 13:13:23.00000
1988	17108	msiexec.exe	0x8584781dc080	0	-	1	True	2025-02-20 13:12:56.000000 UTC	2025-02-20 13:13:04.000000
3820	17108	msiexec.exe	0x8584782f3080	0	-	1	True	2025-02-20 13:12:57.000000 UTC	2025-02-20 13:13:04.000000

```
16612   17108   cmd.exe   0x8584775e7080   0   -   1   False   2025-02-20 13:12:59.000000 UTC   2025-02-20 13:13:00.000000 UT
14596   17108   cmd.exe   0x858477cf20c0   0   -   1   False   2025-02-20 13:13:00.000000 UTC   2025-02-20 13:13:04.000000 UT
10472   1144   WmiPrvSE.exe   0x8584765e0080   0   -   0   False   2025-02-20 13:13:03.000000 UTC   2025-02-20 13:14:26.00000
9324   10268   cmd.exe   0x858475e310c0   0   -   1   True   2025-02-20 13:13:38.000000 UTC   2025-02-20 13:13:39.000000 UTC
3536   2452   taskhostw.exe   0x8584789d4080   0   -   0   False   2025-02-20 13:13:55.000000 UTC   2025-02-20 13:13:56.00000
16280   2452   taskhostw.exe   0x8584774eb0c0   0   -   0   False   2025-02-20 13:13:56.000000 UTC   2025-02-20 13:13:56.0000
12256   6652   cmd.exe   0x858475d72080   0   -   0   False   2025-02-20 13:13:56.000000 UTC   2025-02-20 13:13:56.000000 UTC
16740   2452   taskhostw.exe   0x858475d4e080   0   -   0   False   2025-02-20 13:13:56.000000 UTC   2025-02-20 13:13:56.0000
2448   2452   taskhostw.exe   0x858475d650c0   0   -   0   False   2025-02-20 13:13:56.000000 UTC   2025-02-20 13:13:57.00000
3764   2452   taskhostw.exe   0x858475d47080   0   -   0   False   2025-02-20 13:13:57.000000 UTC   2025-02-20 13:13:57.00000
1268   2452   taskhostw.exe   0x85846f6d0080   0   -   0   False   2025-02-20 13:13:57.000000 UTC   2025-02-20 13:13:58.00000
16716   2452   taskhostw.exe   0x858475d46080   0   -   0   False   2025-02-20 13:13:58.000000 UTC   2025-02-20 13:13:58.0000
12640   2452   taskhostw.exe   0x85846dd2e080   0   -   0   False   2025-02-20 13:13:59.000000 UTC   2025-02-20 13:13:59.0000
9008   2452   taskhostw.exe   0x858475be90c0   0   -   0   False   2025-02-20 13:13:59.000000 UTC   2025-02-20 13:13:59.00000
2390880   2387355   $   0x85846dbac0c0   2365172   -   -   True   N/A   N/A   Disabled

Time Stamp: Thu Feb 20 19:26:33 2025
```

3.3 Command Output for Memdump generated by Belkasoft Live RAM Capturer

Command Output generated by Volatility Workbench

```
PassMark Volatility Workbench Log file  -  http://www.passmark.com

================================================================

Volatility Workbench Version: V3.0 Build 1010

Volatility 3 Framework Version: 2.11.0

Log Date: Thu Feb 20 19:23:53 2025


Time Stamp: Thu Feb 20 19:20:07 2025

"C:\Program Files\VolatilityWorkbench\vol.exe" -f "C:\Program Files\Belkasoft Live RAM Capture\x64\20250220_1.mem" windows.pslist.PsList

Volatility 3 Framework 2.11.0

PID        PPID        ImageFileName        OffsetV        Threads        Handles        SessionId        Wow64        CreateTime        ExitTime        File output

4        0        System        0x858464cca040        280        -        N/A        False        2025-02-20 13:05:42.000000 UTC        N/A        Disabled

76        4        Secure System        0x858464d3e040        0        -        N/A        False        2025-02-20 13:05:37.000000 UTC        N/A        Disabled

120        4        Registry        0x858464df0040        4        -        N/A        False        2025-02-20 13:05:37.000000 UTC        N/A        Disabled

596        4        smss.exe        0x8584677ea040        2        -        N/A        False        2025-02-20 13:05:42.000000 UTC        N/A        Disabled

896        880        csrss.exe        0x85846b795140        12        -        0        False        2025-02-20 13:05:47.000000 UTC        N/A        Disabled

984        880        wininit.exe        0x85846c9770c0        2        -        0        False        2025-02-20 13:05:47.000000 UTC        N/A        Disabled

1004        976        csrss.exe        0x85846c9550c0        15        -        1        False        2025-02-20 13:05:47.000000 UTC        N/A        Disabled

836        984        services.exe        0x85846c9f0080        8        -        0        False        2025-02-20 13:05:47.000000 UTC        N/A        Disabled

856        984        WerFault.exe        0x85846c9f8080        0        -        0        False        2025-02-20 13:05:48.000000 UTC        2025-02-20 13:08:31.000000 U

876        984        LsaIso.exe        0x85846ca84080        1        -        0        False        2025-02-20 13:05:48.000000 UTC        N/A        Disabled

884        984        lsass.exe        0x85846ca870c0        11        -        0        False        2025-02-20 13:05:48.000000 UTC        N/A        Disabled

1144        836        svchost.exe        0x85846cb38080        21        -        0        False        2025-02-20 13:05:48.000000 UTC        N/A        Disabled

1172        836        svchost.exe        0x85846cb5f080        12        -        0        False        2025-02-20 13:05:48.000000 UTC        N/A        Disabled

1180        984        fontdrvhost.ex        0x85846cb5c080        5        -        0        False        2025-02-20 13:05:48.000000 UTC        N/A        Disabled

1284        836        svchost.exe        0x85846cc6d080        6        -        0        False        2025-02-20 13:05:48.000000 UTC        N/A        Disabled

1308        836        svchost.exe        0x85846ccc50c0        5        -        0        False        2025-02-20 13:05:48.000000 UTC        N/A        Disabled

1420        976        winlogon.exe        0x85846cde60c0        7        -        1        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1472        1420        fontdrvhost.ex        0x85846ce4e080        5        -        1        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1544        836        svchost.exe        0x85846ce5d080        2        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1596        836        svchost.exe        0x85846ceb0080        3        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1600        836        svchost.exe        0x85846ceac0c0        3        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1612        836        svchost.exe        0x85846ceb3080        3        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1620        836        svchost.exe        0x85846ceaf080        6        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1716        836        svchost.exe        0x85846ceed080        4        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1724        836        svchost.exe        0x85846ceef080        1        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1808        836        svchost.exe        0x85846d05a080        4        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled

1892        836        IntelCpHDCPSvc        0x85846d073180        4        -        0        False        2025-02-20 13:05:49.000000 UTC        N/A        Disabled
```

1916	836	svchost.exe	0x85846d074080	15	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1928	836	svchost.exe	0x85846d07e080	4	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1964	836	svchost.exe	0x85846d09d080	10	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2012	836	svchost.exe	0x85846d0c2080	5	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1212	1420	dwm.exe	0x85846d12e0c0	20	-	1	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
1712	836	svchost.exe	0x85846d137080	6	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2120	836	svchost.exe	0x85846d1b4080	5	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2140	836	IntelCpHeciSvc	0x85846d1b9180	4	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2372	836	svchost.exe	0x85846cf9a0c0	6	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2408	836	svchost.exe	0x85846cfd6080	2	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2452	836	svchost.exe	0x85846d2240c0	11	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2460	836	svchost.exe	0x85846d227080	12	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2484	836	WUDFHost.exe	0x85846d226080	6	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2540	836	svchost.exe	0x85846d23d080	2	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2716	836	svchost.exe	0x85846d2ed080	1	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2736	836	svchost.exe	0x85846d2f0080	1	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2804	836	svchost.exe	0x85846d393080	7	-	0	False	2025-02-20 13:05:49.000000 UTC	N/A	Disabled
2944	836	ibmpmsvc.exe	0x85846d3c1180	11	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
2952	836	LITSSvc.exe	0x85846d3c9180	6	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
2960	836	svchost.exe	0x85846d3c4080	5	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
2092	836	svchost.exe	0x85846d454080	7	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3108	836	svchost.exe	0x85846d47b080	10	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3196	836	svchost.exe	0x85846d4c60c0	6	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3208	836	svchost.exe	0x85846d4c4080	4	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3216	836	svchost.exe	0x85846d4c9080	3	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3300	4	MemCompression	0x85846d4eb040	22	-	N/A	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3316	836	svchost.exe	0x85846d5650c0	2	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3340	836	igfxCUIService	0x85846d5aa180	3	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3396	836	svchost.exe	0x85846d6020c0	8	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3404	836	svchost.exe	0x85846d5d2080	2	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3600	836	svchost.exe	0x858464c98080	7	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3656	836	svchost.exe	0x85846d83b080	12	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3724	836	svchost.exe	0x85846d8820c0	3	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3732	836	svchost.exe	0x85846d8a3080	6	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3804	836	RtkAudioServic	0x85846d8ee080	3	-	0	False	2025-02-20 13:05:50.000000 UTC	N/A	Disabled
3904	836	svchost.exe	0x85846da85080	16	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4004	3656	audiodg.exe	0x85846da94140	11	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4020	836	svchost.exe	0x85846dbde0c0	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4036	836	svchost.exe	0x85846dbe3080	12	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4048	836	svchost.exe	0x85846dbe2080	8	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4132	836	svchost.exe	0x85846dc31080	1	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled

4504	836	svchost.exe	0x85846dd65080	12	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4544	836	svchost.exe	0x85846ddb0080	2	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4616	836	spoolsv.exe	0x85846de320c0	7	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4624	836	svchost.exe	0x85846de390c0	1	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4704	836	svchost.exe	0x85846e18a0c0	5	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4836	4504	wlanext.exe	0x85846e1350c0	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4860	4836	conhost.exe	0x85846e0df0c0	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4884	836	svchost.exe	0x85846e19b0c0	1	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4892	836	svchost.exe	0x85846e0350c0	5	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4916	836	avp.exe	0x85846dedc0c0	152	-	0	True	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4952	836	svchost.exe	0x85846e175080	5	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4960	836	mDNSResponder.	0x85846deda080	3	-	0	False	2025-02-20 13:05:51.000000 UTC	N/A	Disabled
4968	836	svchost.exe	0x85846dedb080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4976	836	svchost.exe	0x85846dfeb080	10	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4984	836	OfficeClickToR	0x85846e133140	17	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5000	836	svchost.exe	0x85846dfec080	16	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5032	836	esif_uf.exe	0x85846e188080	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5076	836	MainDaemon.exe	0x85846e022080	8	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5100	836	MainService.ex	0x85846e166080	21	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4204	836	httpd.exe	0x85846e033100	5	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
4876	836	OneApp.IGCC.Wi	0x85846de551c0	8	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5140	836	LicenseService	0x85846e0bb0c0	14	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5152	836	RestService.ex	0x85846de890c0	7	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5220	836	TPMProvisionin	0x85846e4e7080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5276	836	jhi_service.ex	0x85846e4eb180	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5324	836	IntelAudioServ	0x85846e2d5100	9	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5384	836	svchost.exe	0x85846e2f0080	6	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5436	836	nimxs.exe	0x85846e2f7080	8	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5576	836	niauth_daemon.	0x85846e5c9100	9	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5608	836	nisvcloc.exe	0x85846e5da100	3	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5628	836	CoordService.e	0x85846e5e80c0	12	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5636	836	BuildService.e	0x85846e5e9080	13	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5644	836	nfsclnt.exe	0x85846e5ec080	6	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5704	836	openvpnserv2.e	0x85846e330080	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5764	836	openvpnserv.ex	0x85846e389080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5772	836	lkads.exe	0x85846e33e080	12	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5780	836	erlsrv.exe	0x85846e33b080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5800	836	sqlwriter.exe	0x85846e3e10c0	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5836	836	SynTPEnhServic	0x85846e3e3080	6	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5916	836	tphkload.exe	0x85846e61d180	8	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5952	836	svchost.exe	0x85846e610080	3	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5964	836	vmware-authd.e	0x85846e66d0c0	5	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled

6016	836	vmnetdhcp.exe	0x85846e6bd080	3	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6028	836	vmware-usbarbi	0x85846e6c1100	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6104	836	vmnat.exe	0x85846e73a080	5	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
5700	836	svchost.exe	0x85846e7670c0	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6188	836	wfcs.exe	0x85846e76a0c0	23	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6196	836	windhawk.exe	0x85846e7780c0	3	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6212	836	WMIRegistratio	0x85846e73e080	3	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6220	1144	WmiPrvSE.exe	0x85846e740080	7	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6252	836	wslservice.exe	0x85846e784080	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6260	836	CptService.exe	0x85846e789100	4	-	0	False	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6336	836	lktsrv.exe	0x85846e782080	17	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6344	836	nidmsrv.exe	0x85846e7e6100	15	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6388	836	tagsrv.exe	0x85846e7e90c0	33	-	0	True	2025-02-20 13:05:52.000000 UTC	N/A	Disabled
6480	836	nimdnsResponde	0x85846e89a140	3	-	0	True	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
6512	5636	redis-server.e	0x85846e8970c0	0	-	0	False	2025-02-20 13:05:53.000000 UTC	2025-02-20 13:06:06.0000	
6652	5780	erl.exe	0x85846e8a4080	93	-	0	False	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
6848	6652	conhost.exe	0x85846e9d31c0	4	-	0	False	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
7212	836	niDiscSvc.exe	0x85846ed7f140	13	-	0	True	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
7356	6652	epmd.exe	0x85846efc7080	2	-	0	False	2025-02-20 13:05:53.000000 UTC	N/A	Disabled
7844	4204	httpd.exe	0x85846f164180	132	-	0	False	2025-02-20 13:05:54.000000 UTC	N/A	Disabled
8180	836	SystemWebServe	0x85846f186140	9	-	0	True	2025-02-20 13:05:54.000000 UTC	N/A	Disabled
8992	6212	mofcomp.exe	0x85846f4e4140	0	-	0	True	2025-02-20 13:05:55.000000 UTC	2025-02-20 13:05:57.000000 U	
9504	836	ApplicationWeb	0x85846f77e180	10	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9512	8180	NIWebServiceCo	0x85846f7df180	8	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9584	8180	NIWebServiceCo	0x85846f7f0180	8	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9636	4976	AggregatorHost	0x85846e3e4080	2	-	0	False	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9772	8180	NIWebServiceCo	0x85846f860180	8	-	0	True	2025-02-20 13:05:56.000000 UTC	N/A	Disabled
9868	8180	NIWebServiceCo	0x85846ef8a180	8	-	0	True	2025-02-20 13:05:57.000000 UTC	N/A	Disabled
9960	4916	avp.exe	0x85846f8ac0c0	8	-	0	True	2025-02-20 13:05:57.000000 UTC	N/A	Disabled
10052	6212	mofcomp.exe	0x85846f8b4140	0	-	0	True	2025-02-20 13:05:57.000000 UTC	2025-02-20 13:05:58.000000	
10644	9504	NIWebServiceCo	0x85846fa71180	8	-	0	True	2025-02-20 13:05:58.000000 UTC	N/A	Disabled
10944	836	svchost.exe	0x85846fb92080	7	-	0	False	2025-02-20 13:05:59.000000 UTC	N/A	Disabled
11092	5916	tposd.exe	0x85846fca90c0	7	-	1	False	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
11112	5836	SynTPEnh.exe	0x85846fcb0080	11	-	1	False	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
11168	6196	windhawk.exe	0x85846fcc1080	2	-	1	True	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
11204	3804	RAVBg64.exe	0x8584675eb080	5	-	1	False	2025-02-20 13:06:00.000000 UTC	N/A	Disabled
10152	5916	shtctky.exe	0x8584674ec080	6	-	1	False	2025-02-20 13:06:01.000000 UTC	N/A	Disabled
11088	1712	sihost.exe	0x85846fcab080	18	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11308	836	svchost.exe	0x85846fe11080	1	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11316	836	svchost.exe	0x85846fe550c0	6	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11364	836	svchost.exe	0x85846feb80c0	2	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11384	836	svchost.exe	0x85846fec1080	11	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled

11428	2452	taskhostw.exe	0x85846feba080	9	-	1	False	2025-02-20 13:06:02.000000 UTC	N/A	Disabled
11452	2452	PIconStartup.e	0x85846febe080	0	-	1	True	2025-02-20 13:06:02.000000 UTC	2025-02-20 13:09:26.0000	
11480	2452	NIUpdateServic	0x85846fec90c0	0	-	1	False	2025-02-20 13:06:02.000000 UTC	2025-02-20 13:08:21.000	
11500	2452	opushutil.exe	0x85846fed2080	0	-	1	False	2025-02-20 13:06:03.000000 UTC	2025-02-20 13:06:40.0000	
11528	2452	MicrosoftEdgeU	0x85846fed5100	5	-	0	True	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11536	2452	ConditionalApp	0x85846feda0c0	0	-	1	True	2025-02-20 13:06:03.000000 UTC	2025-02-20 13:09:23.0000	
11544	2452	PowerMgr.exe	0x85846fed7080	10	-	1	True	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11560	836	PresentationFo	0x85846fed8080	5	-	0	False	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11716	836	svchost.exe	0x85846ff49080	4	-	0	False	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
11724	2452	taskhostw.exe	0x85846ff4d080	0	-	1	False	2025-02-20 13:06:03.000000 UTC	2025-02-20 13:06:06.0000	
11820	836	svchost.exe	0x8584700020c0	2	-	0	False	2025-02-20 13:06:03.000000 UTC	N/A	Disabled
12096	4916	avpui.exe	0x8584700ce0c0	26	-	1	True	2025-02-20 13:06:05.000000 UTC	N/A	Disabled
12112	11112	SynTPEnh.exe	0x8584700c50c0	0	-	1	False	2025-02-20 13:06:05.000000 UTC	2025-02-20 13:06:10.0000	
12268	2452	PowerToys.exe	0x85846ec8b080	17	-	1	False	2025-02-20 13:06:06.000000 UTC	N/A	Disabled
11392	3340	igfxEM.exe	0x858470185080	4	-	1	False	2025-02-20 13:06:06.000000 UTC	N/A	Disabled
9644	836	svchost.exe	0x85846ec8c080	7	-	0	False	2025-02-20 13:06:06.000000 UTC	N/A	Disabled
6964	12112	SynTPHelper.ex	0x85846eb560c0	2	-	1	False	2025-02-20 13:06:07.000000 UTC	N/A	Disabled
12156	836	svchost.exe	0x8584701d90c0	16	-	0	False	2025-02-20 13:06:07.000000 UTC	N/A	Disabled
12428	1420	userinit.exe	0x85846ee95080	0	-	1	False	2025-02-20 13:06:08.000000 UTC	2025-02-20 13:06:41.00000	
12612	12428	explorer.exe	0x8584702df080	127	-	1	False	2025-02-20 13:06:10.000000 UTC	N/A	Disabled
13104	12268	PowerToys.Adva	0x858470671080	14	-	1	False	2025-02-20 13:06:14.000000 UTC	N/A	Disabled
13304	6652	win32sysinfo.e	0x858470827080	2	-	0	False	2025-02-20 13:06:16.000000 UTC	N/A	Disabled
12880	1144	igfxext.exe	0x858470aa0080	3	-	1	False	2025-02-20 13:06:19.000000 UTC	N/A	Disabled
12360	1144	Widgets.exe	0x858470bdd080	10	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
12412	1144	SearchHost.exe	0x858470bcf080	39	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
1576	1144	StartMenuExper	0x858470c4a080	11	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
13320	1144	RuntimeBroker.	0x858470e8e0c0	3	-	1	False	2025-02-20 13:06:20.000000 UTC	N/A	Disabled
13404	1144	RuntimeBroker.	0x858470e0e0c0	18	-	1	False	2025-02-20 13:06:21.000000 UTC	N/A	Disabled
13448	836	svchost.exe	0x858470e1f0c0	2	-	0	False	2025-02-20 13:06:21.000000 UTC	N/A	Disabled
13584	836	svchost.exe	0x858470e7d0c0	2	-	1	False	2025-02-20 13:06:22.000000 UTC	N/A	Disabled
13852	12268	PowerToys.Alwa	0x8584710f9080	4	-	1	False	2025-02-20 13:06:23.000000 UTC	N/A	Disabled
13860	12268	PowerToys.Awak	0x8584710fa080	12	-	1	False	2025-02-20 13:06:23.000000 UTC	N/A	Disabled
13924	12268	PowerToys.Colo	0x8584711760c0	0	-	1	False	2025-02-20 13:06:24.000000 UTC	2025-02-20 13:06:31.00	
14104	1144	dllhost.exe	0x85847136a080	6	-	1	False	2025-02-20 13:06:25.000000 UTC	N/A	Disabled
14324	836	svchost.exe	0x8584713cf080	2	-	0	False	2025-02-20 13:06:25.000000 UTC	N/A	Disabled
12708	12268	PowerToys.Crop	0x8584714d0080	4	-	1	False	2025-02-20 13:06:26.000000 UTC	N/A	Disabled
14452	12268	PowerToys.Fanc	0x85847153c080	7	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled
14508	12268	PowerToys.Keyb	0x85847153a080	4	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled
14564	12268	PowerToys.Mous	0x85847153b080	10	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled
14576	12268	PowerToys.Mous	0x858471539080	16	-	1	False	2025-02-20 13:06:27.000000 UTC	N/A	Disabled
14696	12268	PowerToys.Peek	0x858471196080	14	-	1	False	2025-02-20 13:06:28.000000 UTC	N/A	Disabled
14916	12268	PowerToys.Powe	0x858471188080	20	-	1	False	2025-02-20 13:06:28.000000 UTC	N/A	Disabled

14936	12268	PowerToys.Powe	0x858471189080	12	-	1	False	2025-02-20 13:06:28.000000 UTC	N/A	Disabled
15056	12268	PowerToys.Powe	0x858471194080	9	-	1	False	2025-02-20 13:06:29.000000 UTC	N/A	Disabled
15324	836	svchost.exe	0x8584710bf080	13	-	1	False	2025-02-20 13:06:30.000000 UTC	N/A	Disabled
1532	3724	ctfmon.exe	0x858470f8b080	11	-	1	False	2025-02-20 13:06:32.000000 UTC	N/A	Disabled
14792	2452	RAVBg64.exe	0x858470f460c0	5	-	1	False	2025-02-20 13:06:33.000000 UTC	N/A	Disabled
14828	2452	RAVBg64.exe	0x8584713f20c0	0	-	1	False	2025-02-20 13:06:33.000000 UTC	2025-02-20 13:06:42.000000	
14836	2452	RAVBg64.exe	0x858470fdf0c0	5	-	1	False	2025-02-20 13:06:33.000000 UTC	N/A	Disabled
14364	836	SearchIndexer.	0x8584713ec080	13	-	0	False	2025-02-20 13:06:34.000000 UTC	N/A	Disabled
11156	6652	inet_gethost.e	0x858470e8f080	5	-	0	False	2025-02-20 13:06:34.000000 UTC	N/A	Disabled
5748	836	svchost.exe	0x858471bd0080	3	-	0	False	2025-02-20 13:06:35.000000 UTC	N/A	Disabled
15580	14828	RAVCpl64.exe	0x858470e1e080	7	-	1	False	2025-02-20 13:06:41.000000 UTC	N/A	Disabled
15820	12612	brave.exe	0x8584701f60c0	46	-	1	False	2025-02-20 13:06:50.000000 UTC	N/A	Disabled
15896	15820	brave.exe	0x858471be90c0	8	-	1	False	2025-02-20 13:06:51.000000 UTC	N/A	Disabled
16076	15820	brave.exe	0x858470ee50c0	20	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
16084	15820	brave.exe	0x858470ee10c0	18	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
16108	15820	brave.exe	0x8584720500c0	10	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
16140	15820	brave.exe	0x85847204a0c0	9	-	1	False	2025-02-20 13:06:53.000000 UTC	N/A	Disabled
15384	15820	brave.exe	0x8584723b00c0	21	-	1	False	2025-02-20 13:06:59.000000 UTC	N/A	Disabled
15720	12612	SecurityHealth	0x858472433080	2	-	1	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
116	836	SecurityHealth	0x85847245b080	11	-	0	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
1000	15820	brave.exe	0x85847245c080	13	-	1	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
11828	15820	brave.exe	0x858472459080	21	-	1	False	2025-02-20 13:07:02.000000 UTC	N/A	Disabled
1924	836	svchost.exe	0x858470e8b080	17	-	0	False	2025-02-20 13:07:03.000000 UTC	N/A	Disabled
1948	2452	kpm_tray.exe	0x85847241a080	3	-	1	True	2025-02-20 13:07:03.000000 UTC	N/A	Disabled
3436	836	svchost.exe	0x85847238d080	5	-	0	False	2025-02-20 13:07:05.000000 UTC	N/A	Disabled
7468	15820	brave.exe	0x8584724dc0c0	27	-	1	False	2025-02-20 13:07:11.000000 UTC	N/A	Disabled
6952	12612	wfcUI.exe	0x8584740f20c0	22	-	1	False	2025-02-20 13:07:34.000000 UTC	N/A	Disabled
3608	1144	ShellExperienc	0x8584743d70c0	35	-	1	False	2025-02-20 13:07:46.000000 UTC	N/A	Disabled
11952	1144	RuntimeBroker.	0x8584745c50c0	18	-	1	False	2025-02-20 13:07:48.000000 UTC	N/A	Disabled
12220	836	aesm_service.e	0x8584756ee180	3	-	0	False	2025-02-20 13:07:57.000000 UTC	N/A	Disabled
5284	836	ksde.exe	0x8584747e60c0	35	-	0	True	2025-02-20 13:08:00.000000 UTC	N/A	Disabled
13424	836	LMS.exe	0x8584750c40c0	10	-	0	True	2025-02-20 13:08:01.000000 UTC	N/A	Disabled
3812	836	svchost.exe	0x8584747ee0c0	2	-	1	False	2025-02-20 13:08:02.000000 UTC	N/A	Disabled
16324	4916	avp.exe	0x8584756ed0c0	8	-	0	True	2025-02-20 13:08:02.000000 UTC	N/A	Disabled
2668	11088	TranslucentTB.	0x858474ac80c0	7	-	1	False	2025-02-20 13:08:07.000000 UTC	N/A	Disabled
13444	1144	unsecapp.exe	0x8584754d70c0	4	-	0	False	2025-02-20 13:08:08.000000 UTC	N/A	Disabled
10032	1144	RuntimeBroker.	0x8584753d1080	3	-	1	False	2025-02-20 13:08:16.000000 UTC	N/A	Disabled
10284	836	uhssvc.exe	0x8584752ce080	4	-	0	False	2025-02-20 13:08:18.000000 UTC	N/A	Disabled
12964	836	svchost.exe	0x858477ba3080	7	-	0	False	2025-02-20 13:08:21.000000 UTC	N/A	Disabled
13208	5284	ksdeui.exe	0x858477c10080	8	-	1	True	2025-02-20 13:08:24.000000 UTC	N/A	Disabled
3064	12612	runonce.exe	0x858474acb080	0	-	1	True	2025-02-20 13:08:40.000000 UTC	2025-02-20 13:09:12.000000	

3672	12612	Rainmeter.exe	0x858477b20080	9	-	1	False	2025-02-20 13:08:41.000000 UTC	N/A	Disabled
13868	3064	KeyScrambler.e	0x8584776e00c0	7	-	1	True	2025-02-20 13:08:41.000000 UTC	N/A	Disabled
12624	13868	KeyScrambler.e	0x8584776da080	4	-	1	False	2025-02-20 13:08:43.000000 UTC	N/A	Disabled
3776	11452	PrivacyIconCli	0x858475b5a080	6	-	1	False	2025-02-20 13:09:26.000000 UTC	N/A	Disabled
3280	15820	brave.exe	0x858475dba0c0	17	-	1	False	2025-02-20 13:10:40.000000 UTC	N/A	Disabled
2396	1144	dllhost.exe	0x85847258b080	5	-	0	True	2025-02-20 13:10:56.000000 UTC	N/A	Disabled
4012	15820	brave.exe	0x858475f06080	15	-	1	False	2025-02-20 13:11:06.000000 UTC	N/A	Disabled
14384	836	svchost.exe	0x8584762450c0	4	-	1	False	2025-02-20 13:11:27.000000 UTC	N/A	Disabled
13708	1144	SystemSettings	0x858476027080	19	-	1	False	2025-02-20 13:11:27.000000 UTC	N/A	Disabled
12568	836	svchost.exe	0x85847625c0c0	1	-	0	False	2025-02-20 13:11:28.000000 UTC	N/A	Disabled
7180	836	svchost.exe	0x8584760720c0	11	-	0	False	2025-02-20 13:11:29.000000 UTC	N/A	Disabled
3128	836	svchost.exe	0x858476228080	2	-	1	False	2025-02-20 13:11:32.000000 UTC	N/A	Disabled
17204	17108	msiexec.exe	0x8584763cf080	0	-	1	True	2025-02-20 13:11:41.000000 UTC	2025-02-20 13:13:35.000000	
16420	12612	sublime_text.e	0x858476268080	14	-	1	False	2025-02-20 13:12:42.000000 UTC	N/A	Disabled
4444	16420	crash_handler.	0x8584760510c0	7	-	1	False	2025-02-20 13:12:42.000000 UTC	N/A	Disabled
13484	16420	plugin_host-3.	0x8584762750c0	4	-	1	False	2025-02-20 13:12:43.000000 UTC	N/A	Disabled
10132	16420	plugin_host-3.	0x8584762fb080	4	-	1	False	2025-02-20 13:12:44.000000 UTC	N/A	Disabled
1988	17108	msiexec.exe	0x8584781dc080	0	-	1	True	2025-02-20 13:12:56.000000 UTC	2025-02-20 13:13:04.000000	
3820	17108	msiexec.exe	0x8584782f3080	0	-	1	True	2025-02-20 13:12:57.000000 UTC	2025-02-20 13:13:04.000000	
3896	836	svchost.exe	0x8584776f7080	0	-	0	False	2025-02-20 13:15:35.000000 UTC	2025-02-20 13:15:44.000000	U
16480	836	svchost.exe	0x858475cce080	7	-	0	False	2025-02-20 13:15:35.000000 UTC	N/A	Disabled
12884	836	svchost.exe	0x858478dba0c0	7	-	0	False	2025-02-20 13:15:35.000000 UTC	N/A	Disabled
14856	12612	FTK Imager.exe	0x858478f2c080	0	-	1	False	2025-02-20 13:16:31.000000 UTC	2025-02-20 13:37:39.00	
4268	14576	PowerToys.Mous	0x858478f6e080	0	-	1	False	2025-02-20 13:16:31.000000 UTC	2025-02-20 13:38:13.000	
2036	1144	dllhost.exe	0x858478fb90c0	5	-	1	False	2025-02-20 13:16:44.000000 UTC	N/A	Disabled
13992	1144	WmiPrvSE.exe	0x858478fb10c0	3	-	0	True	2025-02-20 13:17:05.000000 UTC	N/A	Disabled
13744	836	svchost.exe	0x858478fcf0c0	5	-	0	False	2025-02-20 13:17:13.000000 UTC	N/A	Disabled
5360	1144	SDXHelper.exe	0x85846d74c080	17	-	1	False	2025-02-20 13:21:10.000000 UTC	N/A	Disabled
9852	15820	brave.exe	0x858478eb90c0	16	-	1	False	2025-02-20 13:23:54.000000 UTC	N/A	Disabled
6052	15820	brave.exe	0x858476beb080	15	-	1	False	2025-02-20 13:23:55.000000 UTC	N/A	Disabled
3616	1144	DataExchangeHo	0x858475d650c0	4	-	1	False	2025-02-20 13:26:06.000000 UTC	N/A	Disabled
13328	15820	brave.exe	0x8584765ef080	15	-	1	False	2025-02-20 13:27:29.000000 UTC	N/A	Disabled
16728	15820	brave.exe	0x858478f7f180	15	-	1	False	2025-02-20 13:32:32.000000 UTC	N/A	Disabled
12704	836	svchost.exe	0x858471d020c0	3	-	0	False	2025-02-20 13:33:16.000000 UTC	N/A	Disabled
4772	1144	smartscreen.ex	0x85847785f0c0	7	-	1	False	2025-02-20 13:33:16.000000 UTC	N/A	Disabled
6992	15820	brave.exe	0x858470de1080	0	-	1	False	2025-02-20 13:33:16.000000 UTC	2025-02-20 13:36:50.000000	U
9108	15820	brave.exe	0x858477cc70c0	9	-	1	False	2025-02-20 13:33:48.000000 UTC	N/A	Disabled
4440	15820	brave.exe	0x85846fb8b080	0	-	1	False	2025-02-20 13:33:49.000000 UTC	2025-02-20 13:36:50.000000	U
3920	15820	brave.exe	0x858475e97080	0	-	1	False	2025-02-20 13:33:51.000000 UTC	2025-02-20 13:36:50.000000	U
3576	15820	brave.exe	0x85846dbac0c0	0	-	1	False	2025-02-20 13:34:01.000000 UTC	2025-02-20 13:36:40.000000	U
15176	14364	SearchProtocol	0x858471bcc080	0	-	0	False	2025-02-20 13:34:40.000000 UTC	2025-02-20 13:36:42.00	
2348	2452	taskhostw.exe	0x858475f130c0	0	-	0	False	2025-02-20 13:34:56.000000 UTC	2025-02-20 13:34:57.00000	

```
17068   6652    cmd.exe         0x858472aec080  0       -       0       False   2025-02-20 13:34:57.000000 UTC  2025-02-20 13:34:57.000000 UTC
9380    15820   brave.exe       0x8584722ac080  0       -       1       False   2025-02-20 13:34:58.000000 UTC  2025-02-20 13:35:04.000000 U
1876    2452    taskhostw.exe   0x8584723ea080  0       -       0       False   2025-02-20 13:34:58.000000 UTC  2025-02-20 13:34:58.00000
16464   2452    taskhostw.exe   0x85847634c080  0       -       0       False   2025-02-20 13:34:59.000000 UTC  2025-02-20 13:35:00.0000
16884   6652    cmd.exe         0x858478d830c0  0       -       0       False   2025-02-20 13:35:00.000000 UTC  2025-02-20 13:35:00.000000 UTC
16848   2452    taskhostw.exe   0x858472fea080  0       -       0       False   2025-02-20 13:35:01.000000 UTC  2025-02-20 13:35:02.0000
6520    2452    taskhostw.exe   0x858478c020c0  0       -       0       False   2025-02-20 13:35:02.000000 UTC  2025-02-20 13:35:03.00000
13824   2452    taskhostw.exe   0x858477cb60c0  0       -       0       False   2025-02-20 13:35:04.000000 UTC  2025-02-20 13:35:04.0000
13760   6652    cmd.exe         0x858478c5a080  0       -       0       False   2025-02-20 13:35:05.000000 UTC  2025-02-20 13:35:05.000000 UTC
8384    6652    cmd.exe         0x858478011080  0       -       0       False   2025-02-20 13:35:07.000000 UTC  2025-02-20 13:35:07.000000 UTC
9240    6652    cmd.exe         0x8584783dc080  0       -       0       False   2025-02-20 13:35:10.000000 UTC  2025-02-20 13:35:10.000000 UTC
10980   6652    cmd.exe         0x8584742c3080  0       -       0       False   2025-02-20 13:35:15.000000 UTC  2025-02-20 13:35:15.000000 UTC
17272   6652    cmd.exe         0x858476ae7080  0       -       0       False   2025-02-20 13:35:17.000000 UTC  2025-02-20 13:35:17.000000 UTC
3980    6652    cmd.exe         0x858472437080  0       -       0       False   2025-02-20 13:35:20.000000 UTC  2025-02-20 13:35:20.000000 UTC
4248    6652    cmd.exe         0x858474bdd080  0       -       0       False   2025-02-20 13:35:25.000000 UTC  2025-02-20 13:35:25.000000 UTC
14376   6652    cmd.exe         0x8584758e9080  0       -       0       False   2025-02-20 13:35:27.000000 UTC  2025-02-20 13:35:27.000000 UTC
16924   6652    cmd.exe         0x858478d6d080  0       -       0       False   2025-02-20 13:35:30.000000 UTC  2025-02-20 13:35:30.000000 UTC
16460   6652    cmd.exe         0x858477bb4080  0       -       0       False   2025-02-20 13:35:35.000000 UTC  2025-02-20 13:35:35.000000 UTC
12936   6652    cmd.exe         0x858477bb8080  0       -       0       False   2025-02-20 13:35:37.000000 UTC  2025-02-20 13:35:37.000000 UTC
17292   6652    cmd.exe         0x8584763d8080  0       -       0       False   2025-02-20 13:35:40.000000 UTC  2025-02-20 13:35:40.000000 UTC
7612    2452    taskhostw.exe   0x8584725540c0  0       -       0       False   2025-02-20 13:35:43.000000 UTC  2025-02-20 13:35:43.00000
10412   6652    cmd.exe         0x858478fde0c0  0       -       0       False   2025-02-20 13:35:45.000000 UTC  2025-02-20 13:35:45.000000 UTC
5044    2452    taskhostw.exe   0x8584765020c0  0       -       0       False   2025-02-20 13:35:45.000000 UTC  2025-02-20 13:35:45.00000
10920   2452    taskhostw.exe   0x858477f350c0  0       -       0       False   2025-02-20 13:35:45.000000 UTC  2025-02-20 13:35:46.0000
11980   2452    taskhostw.exe   0x85847241c080  0       -       0       False   2025-02-20 13:35:46.000000 UTC  2025-02-20 13:35:46.0000
13812   2452    taskhostw.exe   0x858470e26080  0       -       0       False   2025-02-20 13:35:46.000000 UTC  2025-02-20 13:35:47.0000
2724    6652    cmd.exe         0x858478fcd0c0  0       -       0       False   2025-02-20 13:35:47.000000 UTC  2025-02-20 13:35:47.000000 UTC
17136   2452    taskhostw.exe   0x858475ee6080  0       -       0       False   2025-02-20 13:35:47.000000 UTC  2025-02-20 13:35:48.0000
260     2452    taskhostw.exe   0x8584714c9080  0       -       0       False   2025-02-20 13:35:48.000000 UTC  2025-02-20 13:35:48.000000
16932   2452    taskhostw.exe   0x858476269080  0       -       0       False   2025-02-20 13:35:50.000000 UTC  2025-02-20 13:35:50.0000
15872   6652    cmd.exe         0x85847620f080  0       -       0       False   2025-02-20 13:35:50.000000 UTC  2025-02-20 13:35:50.000000 UTC
15888   2452    taskhostw.exe   0x85846d378080  0       -       0       False   2025-02-20 13:35:52.000000 UTC  2025-02-20 13:35:53.0000
13956   2452    taskhostw.exe   0x858472470080  0       -       0       False   2025-02-20 13:35:53.000000 UTC  2025-02-20 13:35:53.0000
8352    2452    taskhostw.exe   0x85847aa45080  0       -       0       False   2025-02-20 13:35:53.000000 UTC  2025-02-20 13:35:54.00000
1680    2452    taskhostw.exe   0x858475eae080  0       -       0       False   2025-02-20 13:35:55.000000 UTC  2025-02-20 13:35:55.00000
6452    6652    cmd.exe         0x8584706ed080  0       -       0       False   2025-02-20 13:35:55.000000 UTC  2025-02-20 13:35:55.000000 UTC
7256    2452    taskhostw.exe   0x85846f22a080  0       -       0       False   2025-02-20 13:35:56.000000 UTC  2025-02-20 13:35:57.00000
16484   6652    cmd.exe         0x858476247080  0       -       0       False   2025-02-20 13:35:57.000000 UTC  2025-02-20 13:35:57.000000 UTC
10456   6652    cmd.exe         0x8584759d60c0  0       -       0       False   2025-02-20 13:36:00.000000 UTC  2025-02-20 13:36:00.000000 UTC
432     15820   brave.exe       0x8584723020c0  15      -       1       False   2025-02-20 13:36:01.000000 UTC  N/A     Disabled
12364   6652    cmd.exe         0x8584760020c0  0       -       0       False   2025-02-20 13:36:05.000000 UTC  2025-02-20 13:36:05.000000 UTC
1140    6652    cmd.exe         0x858475d760c0  0       -       0       False   2025-02-20 13:36:07.000000 UTC  2025-02-20 13:36:07.000000 UTC
```

```
14612   6652    cmd.exe     0x8584707e90c0  0   -   0   False   2025-02-20 13:36:10.000000 UTC   2025-02-20 13:36:10.000000 UTC
16652   6652    cmd.exe     0x858475d430c0  0   -   0   False   2025-02-20 13:36:15.000000 UTC   2025-02-20 13:36:15.000000 UTC
10792   6652    cmd.exe     0x85846fbbc0c0  0   -   0   False   2025-02-20 13:36:17.000000 UTC   2025-02-20 13:36:17.000000 UTC
12192   6652    cmd.exe     0x858474dc20c0  0   -   0   False   2025-02-20 13:36:20.000000 UTC   2025-02-20 13:36:20.000000 UTC
6184    6652    cmd.exe     0x8584763ca0c0  0   -   0   False   2025-02-20 13:36:25.000000 UTC   2025-02-20 13:36:26.000000 UTC
5060    6652    cmd.exe     0x858475e9b0c0  0   -   0   False   2025-02-20 13:36:27.000000 UTC   2025-02-20 13:36:27.000000 UTC
17268   6652    cmd.exe     0x858471cd60c0  0   -   0   False   2025-02-20 13:36:31.000000 UTC   2025-02-20 13:36:31.000000 UTC
4100    6652    cmd.exe     0x85847aa430c0  0   -   0   False   2025-02-20 13:36:36.000000 UTC   2025-02-20 13:36:36.000000 UTC
3236    6652    cmd.exe     0x858475a950c0  0   -   0   False   2025-02-20 13:36:37.000000 UTC   2025-02-20 13:36:37.000000 UTC
15528   6652    cmd.exe     0x8584777b10c0  0   -   0   False   2025-02-20 13:36:41.000000 UTC   2025-02-20 13:36:41.000000 UTC
1060    15820   brave.exe   0x8584746e40c0  13  -   1   False   2025-02-20 13:36:43.000000 UTC   N/A   Disabled
2308    6652    cmd.exe     0x8584760790c0  0   -   0   False   2025-02-20 13:36:46.000000 UTC   2025-02-20 13:36:46.000000 UTC
3832    6652    cmd.exe     0x8584764560c0  0   -   0   False   2025-02-20 13:36:47.000000 UTC   2025-02-20 13:36:47.000000 UTC
16500   6652    cmd.exe     0x8584710ec0c0  0   -   0   False   2025-02-20 13:36:51.000000 UTC   2025-02-20 13:36:51.000000 UTC
4256    6652    cmd.exe     0x858478d6f080  0   -   0   False   2025-02-20 13:36:56.000000 UTC   2025-02-20 13:36:56.000000 UTC
3172    6652    cmd.exe     0x8584789db0c0  0   -   0   False   2025-02-20 13:36:57.000000 UTC   2025-02-20 13:36:57.000000 UTC
16724   6652    cmd.exe     0x858478c38080  0   -   0   False   2025-02-20 13:37:01.000000 UTC   2025-02-20 13:37:01.000000 UTC
16304   2452    taskhostw.exe   0x8584758c50c0  0   -   0   False   2025-02-20 13:37:04.000000 UTC   2025-02-20 13:37:04.0000
10420   6652    cmd.exe     0x858472df4080  0   -   0   False   2025-02-20 13:37:06.000000 UTC   2025-02-20 13:37:06.000000 UTC
5924    2452    taskhostw.exe   0x858478edb0c0  0   -   0   False   2025-02-20 13:37:06.000000 UTC   2025-02-20 13:37:07.00000
12512   6652    cmd.exe     0x85846ee93080  0   -   0   False   2025-02-20 13:37:07.000000 UTC   2025-02-20 13:37:08.000000 UTC
1912    2452    taskhostw.exe   0x8584704a60c0  0   -   0   False   2025-02-20 13:37:11.000000 UTC   2025-02-20 13:37:11.00000
4388    6652    cmd.exe     0x8584742c20c0  0   -   0   False   2025-02-20 13:37:11.000000 UTC   2025-02-20 13:37:11.000000 UTC
2160    2452    taskhostw.exe   0x8584780e70c0  0   -   0   False   2025-02-20 13:37:12.000000 UTC   2025-02-20 13:37:13.00000
11188   12612   SnippingTool.e  0x85847245f080  0   -   1   False   2025-02-20 13:37:16.000000 UTC   2025-02-20 13:37:21.00
1264    836     svchost.exe     0x858478c41080  0   -   1   False   2025-02-20 13:37:16.000000 UTC   2025-02-20 13:37:16.000000 U
4288    6652    cmd.exe     0x858478a420c0  0   -   0   False   2025-02-20 13:37:16.000000 UTC   2025-02-20 13:37:16.000000 UTC
10484   2452    taskhostw.exe   0x85847649d080  0   -   0   False   2025-02-20 13:37:17.000000 UTC   2025-02-20 13:37:17.0000
17248   6652    cmd.exe     0x8584756c50c0  0   -   0   False   2025-02-20 13:37:18.000000 UTC   2025-02-20 13:37:18.000000 UTC
13676   2452    taskhostw.exe   0x85847aae80c0  0   -   0   False   2025-02-20 13:37:20.000000 UTC   2025-02-20 13:37:21.0000
6708    14364   SearchProtocol  0x8584755e70c0  9   -   0   False   2025-02-20 13:37:21.000000 UTC   N/A   Disabled

12020   14364   SearchFilterHo  0x858475f240c0  6   -   0   False   2025-02-20 13:37:21.000000 UTC   N/A   Disabled
2976    6652    cmd.exe     0x8584759e70c0  0   -   0   False   2025-02-20 13:37:21.000000 UTC   2025-02-20 13:37:21.000000 UTC
2204    2452    taskhostw.exe   0x858471d130c0  0   -   0   False   2025-02-20 13:37:23.000000 UTC   2025-02-20 13:37:23.00000
10348   6652    cmd.exe     0x85846f4e30c0  0   -   0   False   2025-02-20 13:37:26.000000 UTC   2025-02-20 13:37:26.000000 UTC
12296   6652    cmd.exe     0x858477f980c0  0   -   0   False   2025-02-20 13:37:28.000000 UTC   2025-02-20 13:37:28.000000 UTC
1936    2452    taskhostw.exe   0x8584722650c0  0   -   0   False   2025-02-20 13:37:29.000000 UTC   2025-02-20 13:37:29.00000
10124   2452    taskhostw.exe   0x8584724ed0c0  0   -   0   False   2025-02-20 13:37:31.000000 UTC   2025-02-20 13:37:31.0000
9052    6652    cmd.exe     0x8584722980c0  0   -   0   False   2025-02-20 13:37:31.000000 UTC   2025-02-20 13:37:32.000000 UTC
17388   2452    taskhostw.exe   0x8584722a90c0  0   -   0   False   2025-02-20 13:37:33.000000 UTC   2025-02-20 13:37:33.0000
14872   6652    cmd.exe     0x858478d940c0  0   -   0   False   2025-02-20 13:37:37.000000 UTC   2025-02-20 13:37:37.000000 UTC
11348   2452    taskhostw.exe   0x8584762cb0c0  0   -   0   False   2025-02-20 13:37:37.000000 UTC   2025-02-20 13:37:38.0000
```

```
7436    6652    cmd.exe         0x8584762660c0  0       -       0       False   2025-02-20 13:37:38.000000 UTC  2025-02-20 13:37:38.000000 UTC
6432    2452    taskhostw.exe   0x858478fbc0c0  0       -       0       False   2025-02-20 13:37:39.000000 UTC  2025-02-20 13:37:39.00000
13876   2452    taskhostw.exe   0x858474cc20c0  0       -       0       False   2025-02-20 13:37:40.000000 UTC  2025-02-20 13:37:40.0000
13892   6652    cmd.exe         0x858478c560c0  0       -       0       False   2025-02-20 13:37:42.000000 UTC  2025-02-20 13:37:42.000000 UTC
16604   6652    cmd.exe         0x858475e310c0  0       -       0       False   2025-02-20 13:37:47.000000 UTC  2025-02-20 13:37:47.000000 UTC
9252    2452    taskhostw.exe   0x8584761e90c0  0       -       0       False   2025-02-20 13:37:47.000000 UTC  2025-02-20 13:37:48.00000
13420   6652    cmd.exe         0x8584710a80c0  0       -       0       False   2025-02-20 13:37:48.000000 UTC  2025-02-20 13:37:48.000000 UTC
12420   6652    cmd.exe         0x858470a910c0  0       -       0       False   2025-02-20 13:37:52.000000 UTC  2025-02-20 13:37:52.000000 UTC
2416    6652    cmd.exe         0x858476429080  0       -       0       False   2025-02-20 13:37:57.000000 UTC  2025-02-20 13:37:57.000000 UTC
6268    6652    cmd.exe         0x858478d2e0c0  0       -       0       False   2025-02-20 13:37:58.000000 UTC  2025-02-20 13:37:58.000000 UTC
14292   6652    cmd.exe         0x858472c020c0  0       -       0       False   2025-02-20 13:38:02.000000 UTC  2025-02-20 13:38:02.000000 UTC
692     2452    taskhostw.exe   0x858477b4e080  0       -       0       False   2025-02-20 13:38:02.000000 UTC  2025-02-20 13:38:02.000000
10724   2452    taskhostw.exe   0x8584786c50c0  0       -       0       False   2025-02-20 13:38:02.000000 UTC  2025-02-20 13:38:03.0000
11404   2452    taskhostw.exe   0x858478c340c0  0       -       0       False   2025-02-20 13:38:05.000000 UTC  2025-02-20 13:38:06.0000
13900   2452    taskhostw.exe   0x8584782e80c0  0       -       0       False   2025-02-20 13:38:07.000000 UTC  2025-02-20 13:38:07.0000
2192    6652    cmd.exe         0x8584772d60c0  0       -       0       False   2025-02-20 13:38:07.000000 UTC  2025-02-20 13:38:07.000000 UTC
10900   6652    cmd.exe         0x8584762230c0  0       -       0       False   2025-02-20 13:38:08.000000 UTC  2025-02-20 13:38:08.000000 UTC
12516   2452    taskhostw.exe   0x858478db60c0  0       -       0       False   2025-02-20 13:38:10.000000 UTC  2025-02-20 13:38:11.0000
3596    6652    cmd.exe         0x8584791240c0  0       -       0       False   2025-02-20 13:38:12.000000 UTC  2025-02-20 13:38:12.000000 UTC
9760    2452    taskhostw.exe   0x85847647b0c0  0       -       0       False   2025-02-20 13:38:12.000000 UTC  2025-02-20 13:38:12.00000
16976   12612   RamCapture64.e  0x858478fab0c0  0       -       1       False   2025-02-20 13:38:13.000000 UTC  2025-02-20 13:38:13.00
6776    11716   consent.exe     0x858478e860c0  0       -       1       False   2025-02-20 13:38:13.000000 UTC  2025-02-20 13:38:15.000000
10004   3724    ctfmon.exe      0x858478b920c0  0       -       1       False   2025-02-20 13:38:13.000000 UTC  2025-02-20 13:38:18.000000
15368   2452    taskhostw.exe   0x8584760130c0  0       -       0       False   2025-02-20 13:38:13.000000 UTC  2025-02-20 13:38:14.0000
12016   2452    taskhostw.exe   0x8584713d70c0  0       -       0       False   2025-02-20 13:38:15.000000 UTC  2025-02-20 13:38:15.0000
4384    12612   RamCapture64.e  0x8584789ca0c0  8       -       1       False   2025-02-20 13:38:15.000000 UTC  N/A     Disabled
10676   4384    conhost.exe     0x8584710ca0c0  10      -       1       False   2025-02-20 13:38:15.000000 UTC  N/A     Disabled
2840    14576   PowerToys.Mous  0x858477b1f080  19      -       1       False   2025-02-20 13:38:15.000000 UTC  N/A     Disabled
11756   6652    cmd.exe         0x8584742c8080  0       -       0       False   2025-02-20 13:38:17.000000 UTC  2025-02-20 13:38:17.000000 UTC
1132    6652    cmd.exe         0x858475be90c0  0       -       0       False   2025-02-20 13:38:18.000000 UTC  2025-02-20 13:38:18.000000 UTC
11752   12612   SnippingTool.e  0x858471bdc080  0       -       1       False   2025-02-20 13:38:21.000000 UTC  2025-02-20 13:38:25.00
3928    836     svchost.exe     0x858470e60080  0       -       1       False   2025-02-20 13:38:22.000000 UTC  2025-02-20 13:38:22.000000 U
16640   6652    cmd.exe         0x858478eba080  0       -       0       False   2025-02-20 13:38:22.000000 UTC  2025-02-20 13:38:22.000000 UTC
428     2452    taskhostw.exe   0x858475d69080  0       -       0       False   2025-02-20 13:38:22.000000 UTC  2025-02-20 13:38:23.000000
13236   2452    taskhostw.exe   0x858478c03080  0       -       0       False   2025-02-20 13:38:25.000000 UTC  2025-02-20 13:38:25.0000
16468   6652    cmd.exe         0x85846d864080  0       -       0       False   2025-02-20 13:38:27.000000 UTC  2025-02-20 13:38:27.000000 UTC
16780   6652    cmd.exe         0x858470839080  0       -       0       False   2025-02-20 13:38:28.000000 UTC  2025-02-20 13:38:28.000000 UTC
5604    2452    taskhostw.exe   0x85846fb5d080  0       -       0       False   2025-02-20 13:38:28.000000 UTC  2025-02-20 13:38:28.00000
5008    6652    cmd.exe         0x8584780ef080  0       -       0       False   2025-02-20 13:38:32.000000 UTC  2025-02-20 13:38:32.000000 UTC
10364   2452    taskhostw.exe   0x858475ad3080  0       -       0       False   2025-02-20 13:38:36.000000 UTC  2025-02-20 13:38:37.0000
17368   6652    cmd.exe         0x8584761f4080  0       -       0       False   2025-02-20 13:38:37.000000 UTC  2025-02-20 13:38:37.000000 UTC
9416    2452    taskhostw.exe   0x8584704ba080  0       -       0       False   2025-02-20 13:30:21.000000 UTC  2025-02-20 13:30:21.00000
```

```
Time Stamp: Thu Feb 20 19:23:04 2025
```
