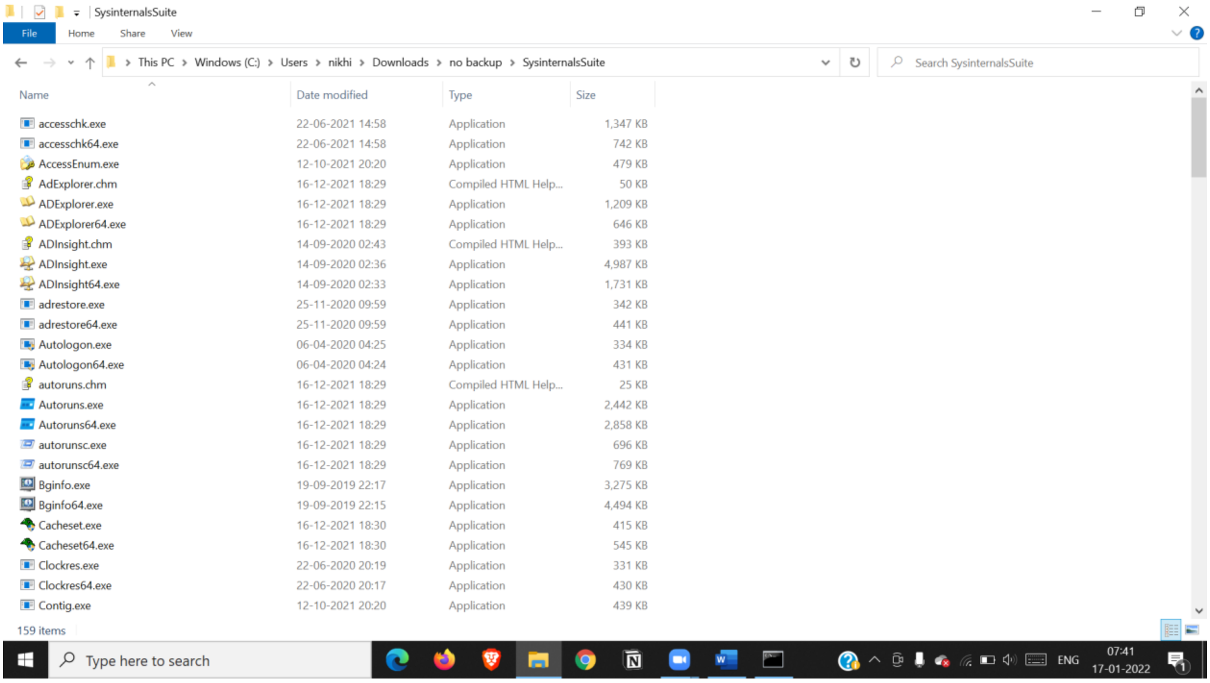
Practical 6
cf

AIM: Using Sysinternals tools for Network Tracking and Process Monitoring : - Check Sysinternals tools - Monitor Live Processes - Capture RAM - Capture TCP/UDP packets - Monitor Hard Disk - Monitor Virtual Memory - Monitor Cache Memory

Sysinternal tools

The SysInternals suite of tools is simply a set of Windows applications that can be downloaded for free from their section of the Microsoft Technet web site. They are all portable, which means that not only do you not have to install them, you can stick them on a flash drive and use them from any PC

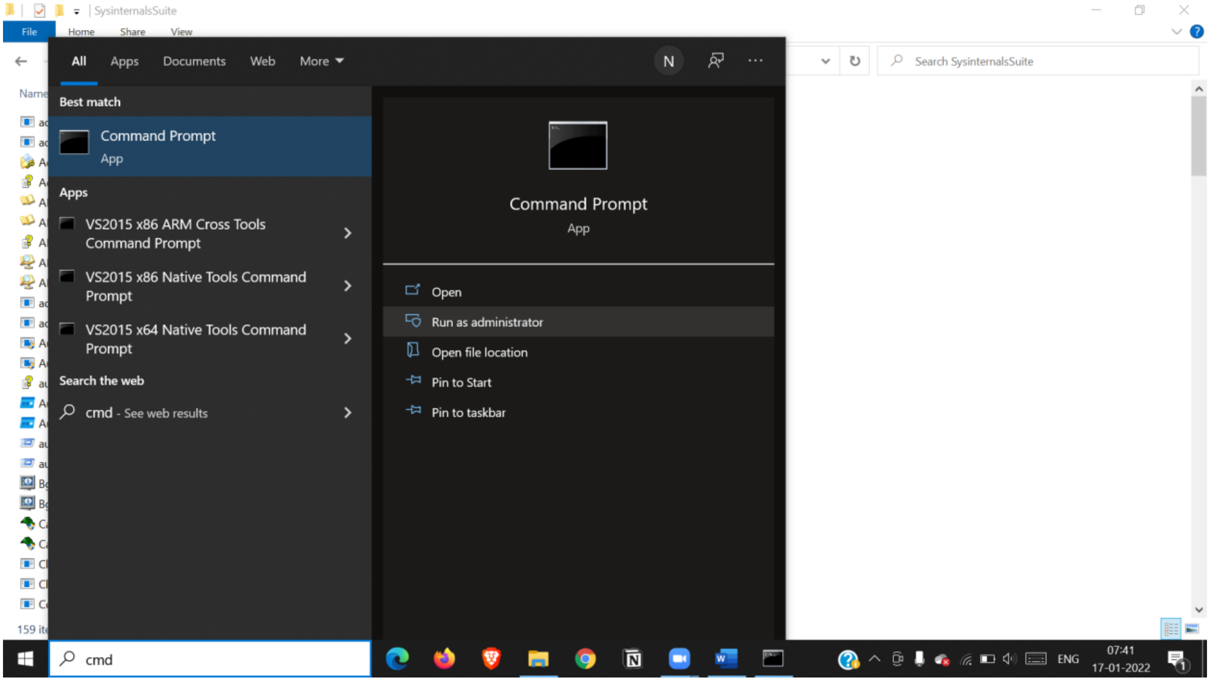
The Sysinternals tools are divided into six categories: File and Disk Utilities, Networking Utilities, Processes Utilities, Security Utilities, System Information and Miscellaneous Utilities. There are many tools, but the widely known are AutoRuns, Process Monitor, Process Explorer, TCPView and RootkitRevealer.

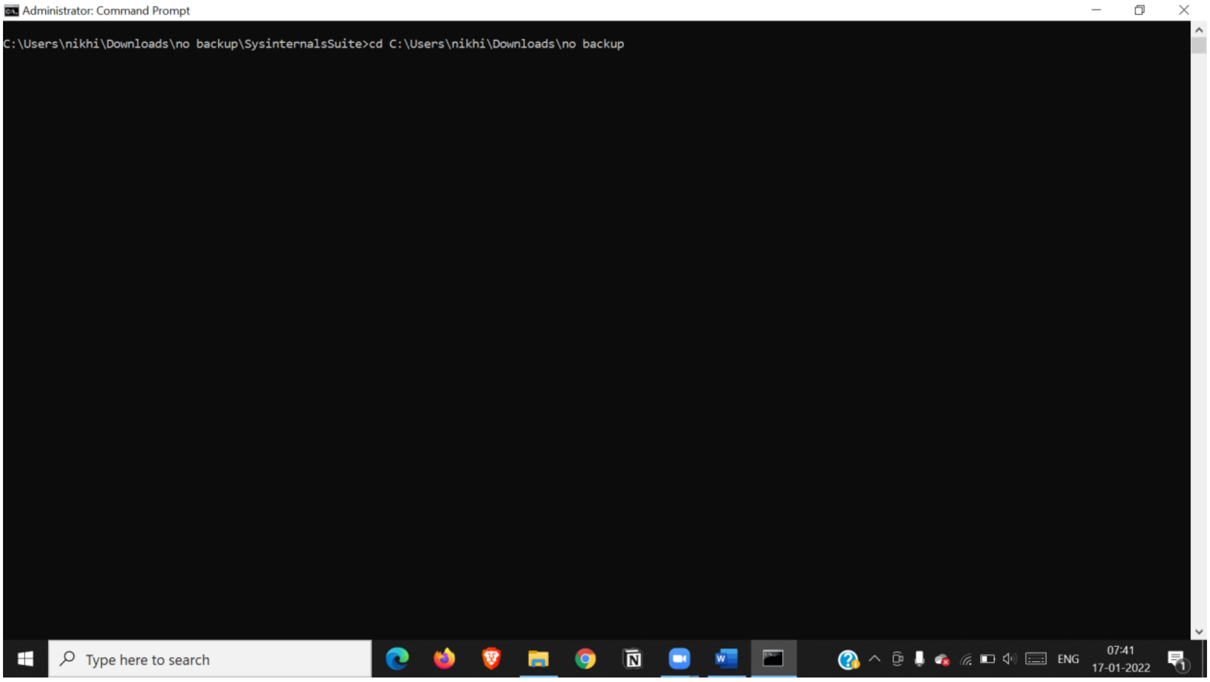

SysinternalsSuite
File
Home
Share
View
This PC > Windows (C:) > Users > nikhi > Downloads > no backup > SysinternalsSuite
Search SysinternalsSuite

Name	Date modified	Type	Size
accesschk.exe	22-06-2021 14:58	Application	1,347 KB
accesschk64.exe	22-06-2021 14:58	Application	742 KB
AccessEnum.exe	12-10-2021 20:20	Application	479 KB
AdExplorer.chm	16-12-2021 18:29	Compiled HTML Help...	50 KB
ADExplorer.exe	16-12-2021 18:29	Application	1,209 KB
ADExplorer64.exe	16-12-2021 18:29	Application	646 KB
ADInsight.chm	14-09-2020 02:43	Compiled HTML Help...	393 KB
ADInsight.exe	14-09-2020 02:36	Application	4,987 KB
ADInsight64.exe	14-09-2020 02:33	Application	1,731 KB
adrestore.exe	25-11-2020 09:59	Application	342 KB
adrestore64.exe	25-11-2020 09:59	Application	441 KB
Autologon.exe	06-04-2020 04:25	Application	334 KB
Autologon64.exe	06-04-2020 04:24	Application	431 KB
autoruns.chm	16-12-2021 18:29	Compiled HTML Help...	25 KB
Autoruns.exe	16-12-2021 18:29	Application	2,442 KB
Autoruns64.exe	16-12-2021 18:29	Application	2,858 KB
autorunsc.exe	16-12-2021 18:29	Application	696 KB
autorunsc64.exe	16-12-2021 18:29	Application	769 KB
Bginfo.exe	19-09-2019 22:17	Application	3,275 KB
Bginfo64.exe	19-09-2019 22:15	Application	4,494 KB
Cacheset.exe	16-12-2021 18:30	Application	415 KB
Cacheset64.exe	16-12-2021 18:30	Application	545 KB
Clockres.exe	22-06-2020 20:19	Application	331 KB
Clockres64.exe	22-06-2020 20:17	Application	430 KB
Contig.exe	12-10-2021 20:20	Application	439 KB

159 items

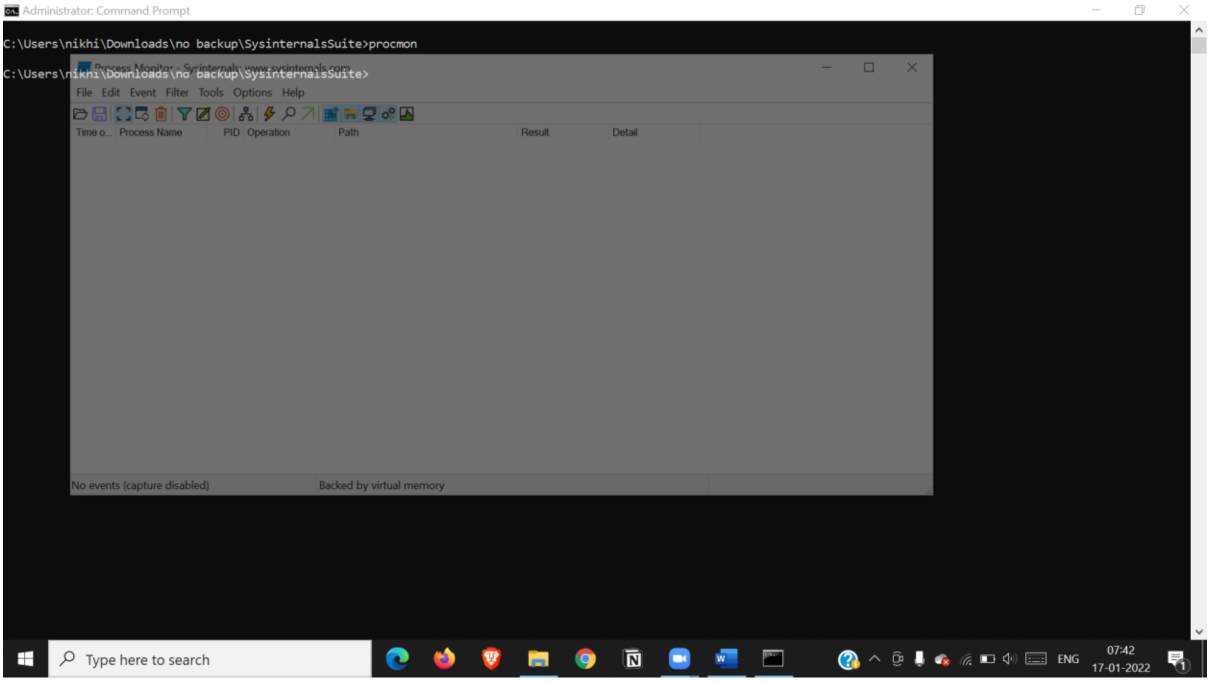
Practical 6
cf





```
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>cd C:\Users\nikhi\Downloads\no backup
```

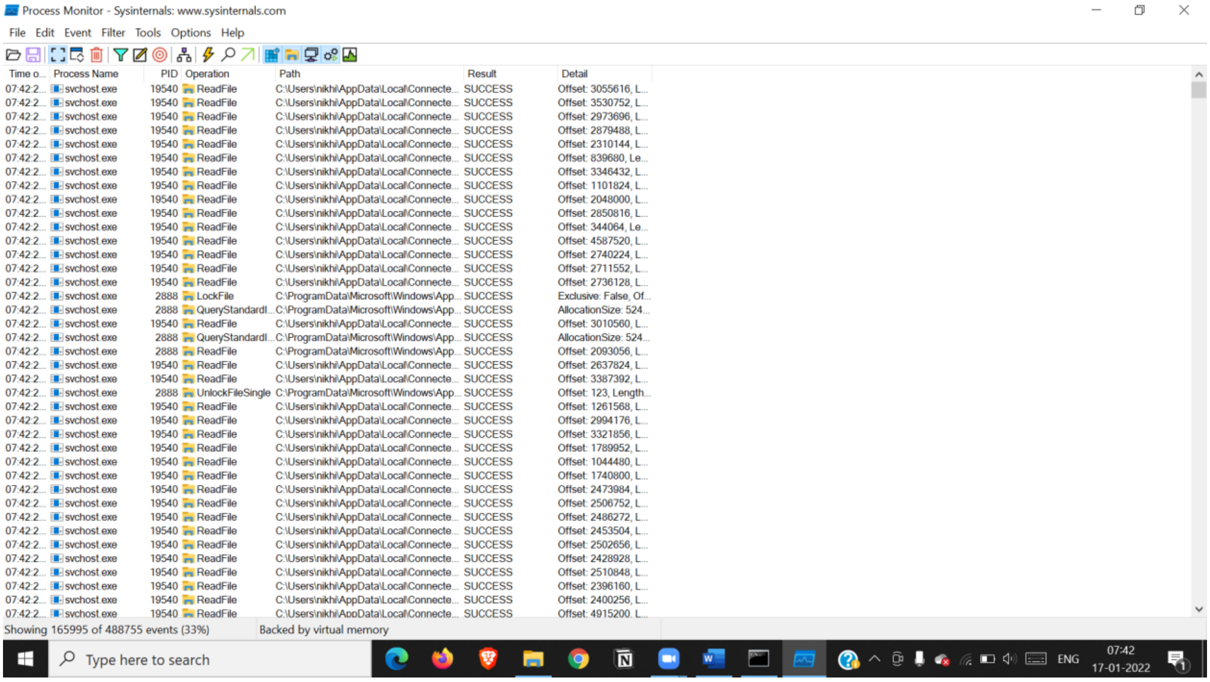
Practical 6
cf


Administrator: Command Prompt
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time o... Process Name PID Operation Path Result Detail
Type here to search
ENG
07:42
17-01-2022

```
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>procmon

C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
```

No events (capture disabled) Backed by virtual memory

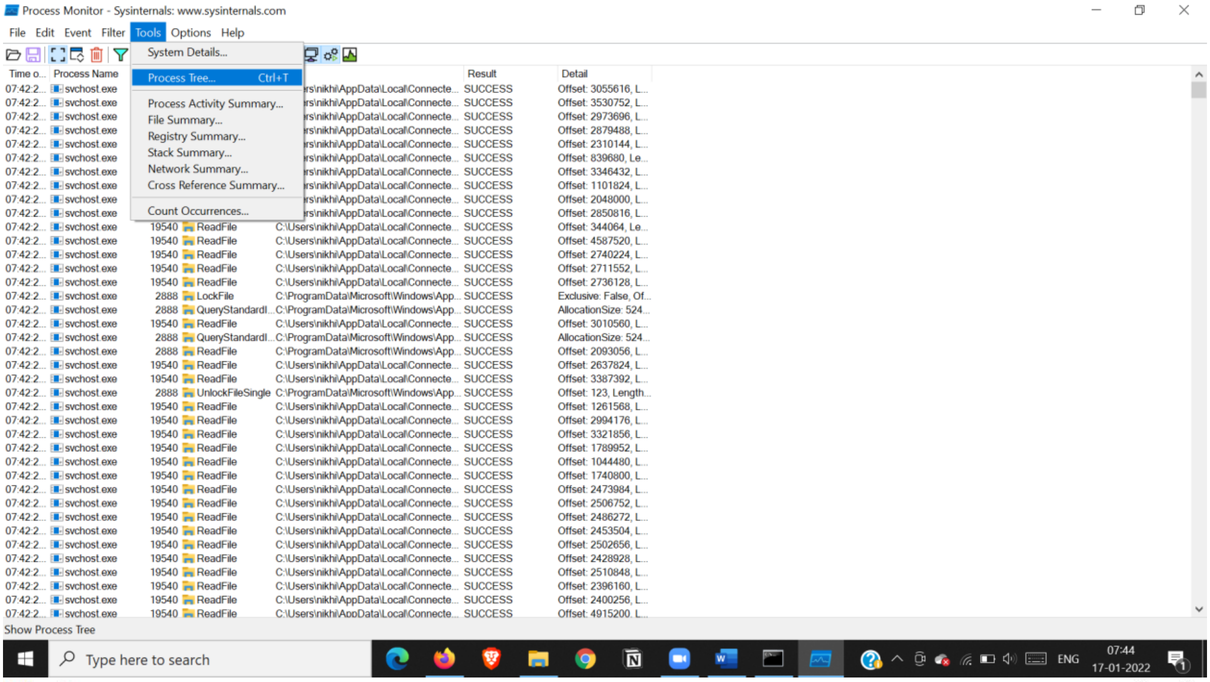

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Type here to search
ENG
07:42
17-01-2022

Time o...	Process Name	PID	Operation	Path	Result	Detail
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3055616, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3530752, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2973696, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2879488, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2310144, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 839680, Le...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3346432, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1101824, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2048000, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2850816, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 344064, Le...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 4587520, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2740224, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2711552, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2736128, L...
07:42:2...	svchost.exe	2888	LockFile	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	Exclusive: False, Of...
07:42:2...	svchost.exe	2888	QueryStandardI...	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	AllocationSize: 524...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3010560, L...
07:42:2...	svchost.exe	2888	QueryStandardI...	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	AllocationSize: 524...
07:42:2...	svchost.exe	2888	ReadFile	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	Offset: 2093056, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2637824, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3387392, L...
07:42:2...	svchost.exe	2888	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	Offset: 123, Length...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1261568, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2994176, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3321856, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1789952, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1044480, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1740800, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2473984, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2506752, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2486272, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2453504, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2502656, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2428928, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2510848, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2396160, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2400256, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 4915200, L...

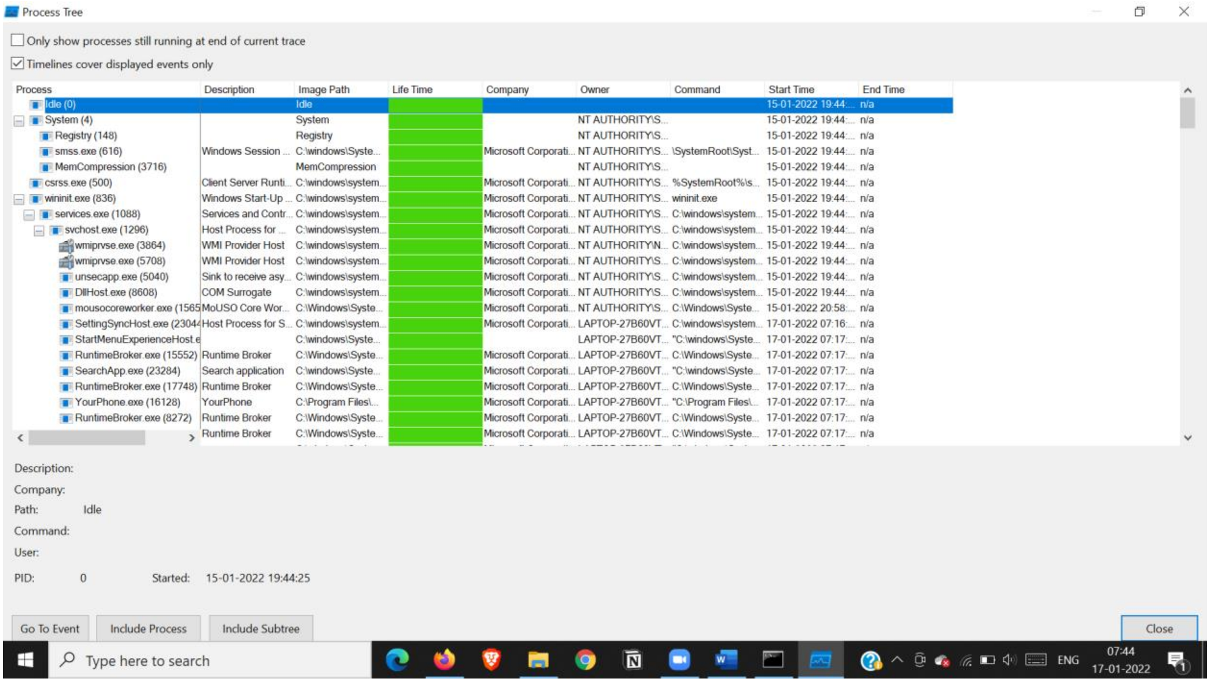
Showing 165995 of 488755 events (33%) Backed by virtual memory

Practical 6

cf



Time o...	Process Name				Result	Detail
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3055616, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3530752, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2973696, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2879488, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2310144, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 839680, Le...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3346432, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1101824, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2048000, L...
07:42:2...	svchost.exe			rs\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2850816, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 344064, Le...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 4587520, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2740224, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2711552, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2736128, L...
07:42:2...	svchost.exe	2888	LockFile	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	Exclusive: False, Of...
07:42:2...	svchost.exe	2888	QueryStandardI...	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	AllocationSize: 524...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3010560, L...
07:42:2...	svchost.exe	2888	QueryStandardI...	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	AllocationSize: 524...
07:42:2...	svchost.exe	2888	ReadFile	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	Offset: 2093056, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2637824, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3387392, L...
07:42:2...	svchost.exe	2888	UnlockFileSingle	C:\ProgramData\Microsoft\Windows\App...	SUCCESS	Offset: 123, Length...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1261568, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2994176, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 3321856, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1789952, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1044480, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 1740800, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2473984, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2506752, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2486272, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2453504, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2502656, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2428928, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2510848, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2396160, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 2400256, L...
07:42:2...	svchost.exe	19540	ReadFile	C:\Users\nikhi\AppData\Local\Connecte...	SUCCESS	Offset: 4915200, L...



☐ Only show processes still running at end of current trace

☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
Idle (0)		Idle	🟩				15-01-2022 19:44:...	n/a
System (4)		System	🟩		NT AUTHORITY\S...		15-01-2022 19:44:...	n/a
Registry (148)		Registry	🟩		NT AUTHORITY\S...		15-01-2022 19:44:...	n/a
smss.exe (616)	Windows Session ...	C:\windows\Syste...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	\SystemRoot\Syst...	15-01-2022 19:44:...	n/a
MemCompression (3716)		MemCompression	🟩		NT AUTHORITY\S...		15-01-2022 19:44:...	n/a
csrss.exe (500)	Client Server Runti...	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	%SystemRoot%\s...	15-01-2022 19:44:...	n/a
wininit.exe (836)	Windows Start-Up ...	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	wininit.exe	15-01-2022 19:44:...	n/a
services.exe (1088)	Services and Contr...	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	C:\windows\system...	15-01-2022 19:44:...	n/a
svchost.exe (1296)	Host Process for ...	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	C:\windows\system...	15-01-2022 19:44:...	n/a
wmiprvse.exe (3864)	WMI Provider Host	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\N...	C:\windows\system...	15-01-2022 19:44:...	n/a
wmiprvse.exe (5708)	WMI Provider Host	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	C:\windows\system...	15-01-2022 19:44:...	n/a
unsecapp.exe (5040)	Sink to receive asy...	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	C:\windows\system...	15-01-2022 19:44:...	n/a
DllHost.exe (8608)	COM Surrogate	C:\windows\system...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	C:\windows\system...	15-01-2022 19:44:...	n/a
mousocoreworker.exe (1565	MoUSO Core Wor...	C:\Windows\Syste...	🟩	Microsoft Corporati...	NT AUTHORITY\S...	C:\Windows\Syste...	15-01-2022 20:58:...	n/a
SettingSyncHost.exe (23044	Host Process for S...	C:\windows\system...	🟩	Microsoft Corporati...	LAPTOP-27B60VT...	C:\windows\system...	17-01-2022 07:16:...	n/a
StartMenuExperienceHost.e		C:\windows\Syste...	🟩		LAPTOP-27B60VT...	"C:\windows\Syste...	17-01-2022 07:17:...	n/a
RuntimeBroker.exe (15552)	Runtime Broker	C:\Windows\Syste...	🟩	Microsoft Corporati...	LAPTOP-27B60VT...	C:\Windows\Syste...	17-01-2022 07:17:...	n/a
SearchApp.exe (23284)	Search application	C:\windows\Syste...	🟩	Microsoft Corporati...	LAPTOP-27B60VT...	"C:\windows\Syste...	17-01-2022 07:17:...	n/a
RuntimeBroker.exe (17748)	Runtime Broker	C:\Windows\Syste...	🟩	Microsoft Corporati...	LAPTOP-27B60VT...	C:\Windows\Syste...	17-01-2022 07:17:...	n/a
YourPhone.exe (16128)	YourPhone	C:\Program Files\...	🟩	Microsoft Corporati...	LAPTOP-27B60VT...	"C:\Program Files\...	17-01-2022 07:17:...	n/a
RuntimeBroker.exe (8272)	Runtime Broker	C:\Windows\Syste...	🟩	Microsoft Corporati...	LAPTOP-27B60VT...	C:\Windows\Syste...	17-01-2022 07:17:...	n/a
	Runtime Broker	C:\Windows\Syste...	🟩	Microsoft Corporati...	LAPTOP-27B60VT...	C:\Windows\Syste...	17-01-2022 07:17:...	n/a

Description:

Company:

Path: Idle

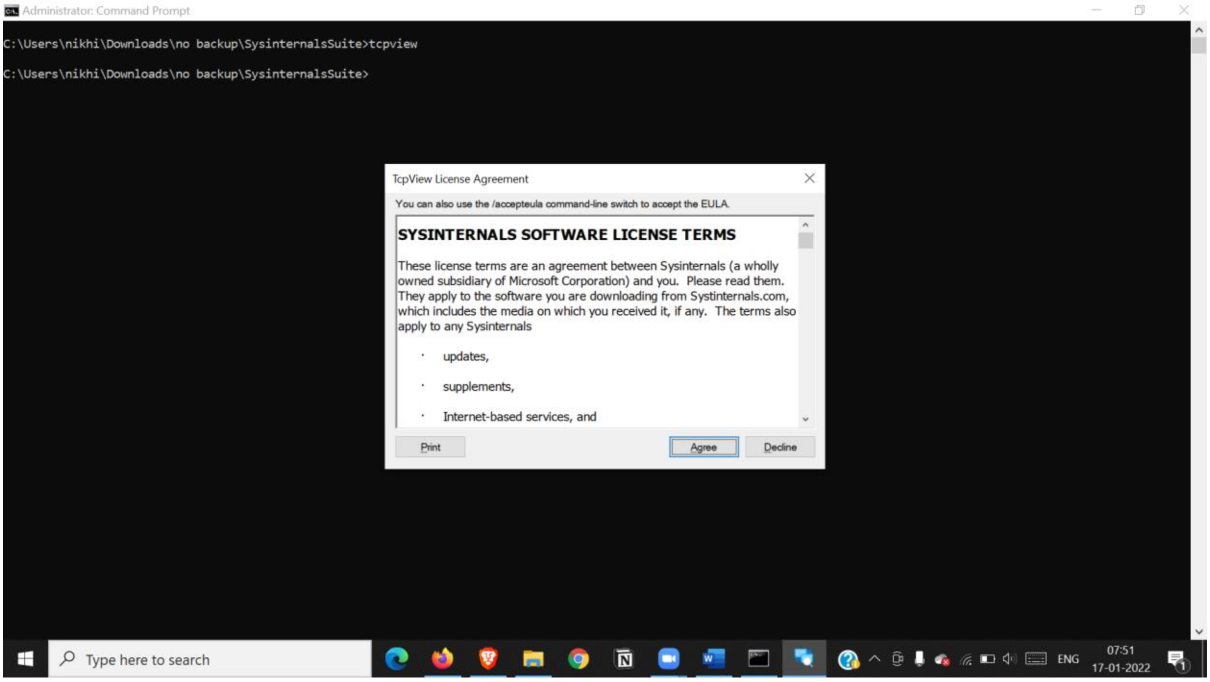
Command:

User:

PID: 0 Started: 15-01-2022 19:44:25

Practical 6
cf

Tcp -udp packets



```
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>tcpview

C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
```

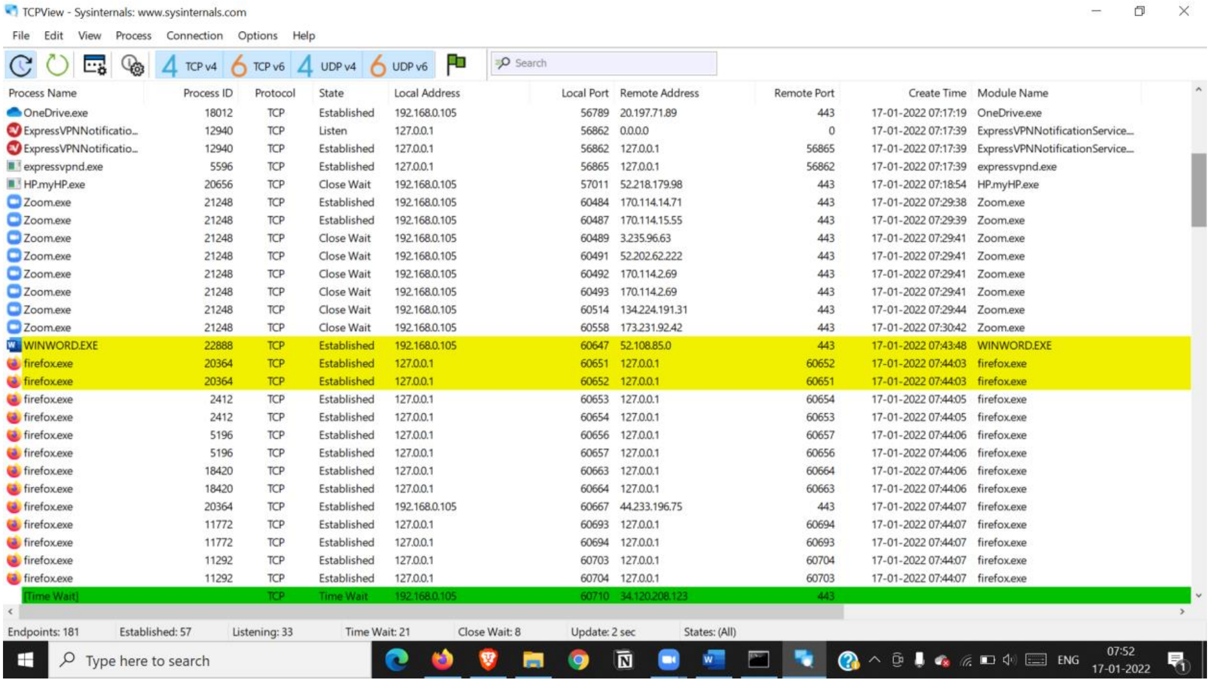
TcpView License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

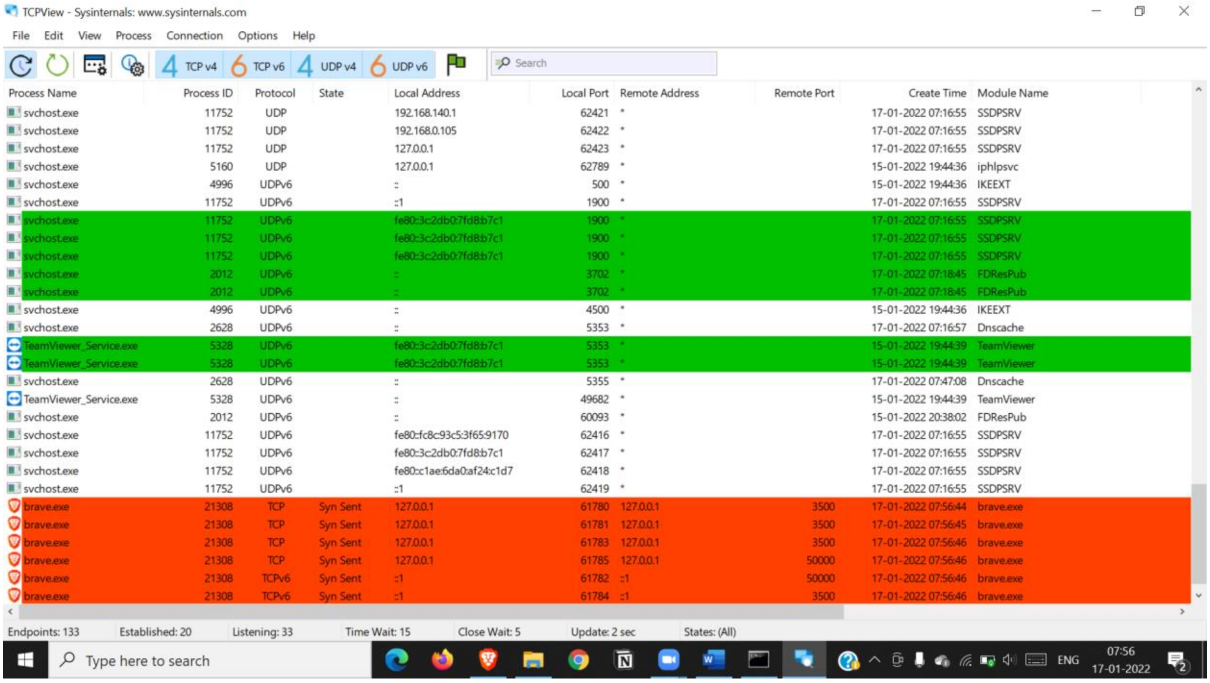
- updates,
- supplements,
- Internet-based services, and



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
OneDrive.exe	18012	TCP	Established	192.168.0.105	56789	20.197.71.89	443	17-01-2022 07:17:19	OneDrive.exe
ExpressVPNNotificatio...	12940	TCP	Listen	127.0.0.1	56862	0.0.0.0	0	17-01-2022 07:17:39	ExpressVPNNotificationService...
ExpressVPNNotificatio...	12940	TCP	Established	127.0.0.1	56862	127.0.0.1	56865	17-01-2022 07:17:39	ExpressVPNNotificationService...
expressvpnd.exe	5596	TCP	Established	127.0.0.1	56865	127.0.0.1	56862	17-01-2022 07:17:39	expressvpnd.exe
HP.myHP.exe	20656	TCP	Close Wait	192.168.0.105	57011	52.218.179.98	443	17-01-2022 07:18:54	HP.myHP.exe
Zoom.exe	21248	TCP	Established	192.168.0.105	60484	170.114.14.71	443	17-01-2022 07:29:38	Zoom.exe
Zoom.exe	21248	TCP	Established	192.168.0.105	60487	170.114.15.55	443	17-01-2022 07:29:39	Zoom.exe
Zoom.exe	21248	TCP	Close Wait	192.168.0.105	60489	3.235.96.63	443	17-01-2022 07:29:41	Zoom.exe
Zoom.exe	21248	TCP	Close Wait	192.168.0.105	60491	52.202.62.222	443	17-01-2022 07:29:41	Zoom.exe
Zoom.exe	21248	TCP	Close Wait	192.168.0.105	60492	170.114.2.69	443	17-01-2022 07:29:41	Zoom.exe
Zoom.exe	21248	TCP	Close Wait	192.168.0.105	60493	170.114.2.69	443	17-01-2022 07:29:41	Zoom.exe
Zoom.exe	21248	TCP	Close Wait	192.168.0.105	60514	134.224.191.31	443	17-01-2022 07:29:44	Zoom.exe
Zoom.exe	21248	TCP	Close Wait	192.168.0.105	60558	173.231.92.42	443	17-01-2022 07:30:42	Zoom.exe
WINWORD.EXE	22888	TCP	Established	192.168.0.105	60647	52.108.85.0	443	17-01-2022 07:43:48	WINWORD.EXE
firefox.exe	20364	TCP	Established	127.0.0.1	60651	127.0.0.1	60652	17-01-2022 07:44:03	firefox.exe
firefox.exe	20364	TCP	Established	127.0.0.1	60652	127.0.0.1	60651	17-01-2022 07:44:03	firefox.exe
firefox.exe	2412	TCP	Established	127.0.0.1	60653	127.0.0.1	60654	17-01-2022 07:44:05	firefox.exe
firefox.exe	2412	TCP	Established	127.0.0.1	60654	127.0.0.1	60653	17-01-2022 07:44:05	firefox.exe
firefox.exe	5196	TCP	Established	127.0.0.1	60656	127.0.0.1	60657	17-01-2022 07:44:06	firefox.exe
firefox.exe	5196	TCP	Established	127.0.0.1	60657	127.0.0.1	60656	17-01-2022 07:44:06	firefox.exe
firefox.exe	18420	TCP	Established	127.0.0.1	60663	127.0.0.1	60664	17-01-2022 07:44:06	firefox.exe
firefox.exe	18420	TCP	Established	127.0.0.1	60664	127.0.0.1	60663	17-01-2022 07:44:06	firefox.exe
firefox.exe	20364	TCP	Established	192.168.0.105	60667	44.233.196.75	443	17-01-2022 07:44:07	firefox.exe
firefox.exe	11772	TCP	Established	127.0.0.1	60693	127.0.0.1	60694	17-01-2022 07:44:07	firefox.exe
firefox.exe	11772	TCP	Established	127.0.0.1	60694	127.0.0.1	60693	17-01-2022 07:44:07	firefox.exe
firefox.exe	11292	TCP	Established	127.0.0.1	60703	127.0.0.1	60704	17-01-2022 07:44:07	firefox.exe
firefox.exe	11292	TCP	Established	127.0.0.1	60704	127.0.0.1	60703	17-01-2022 07:44:07	firefox.exe
[Time Wait]		TCP	Time Wait	192.168.0.105	60710	34.120.208.123	443		

Endpoints: 181   Established: 57   Listening: 33   Time Wait: 21   Close Wait: 8   Update: 2 sec   States: (All)

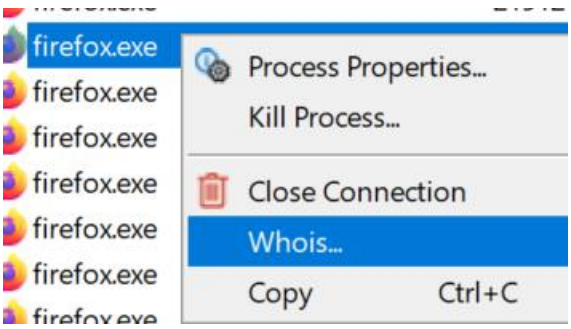
Practical 6
cf

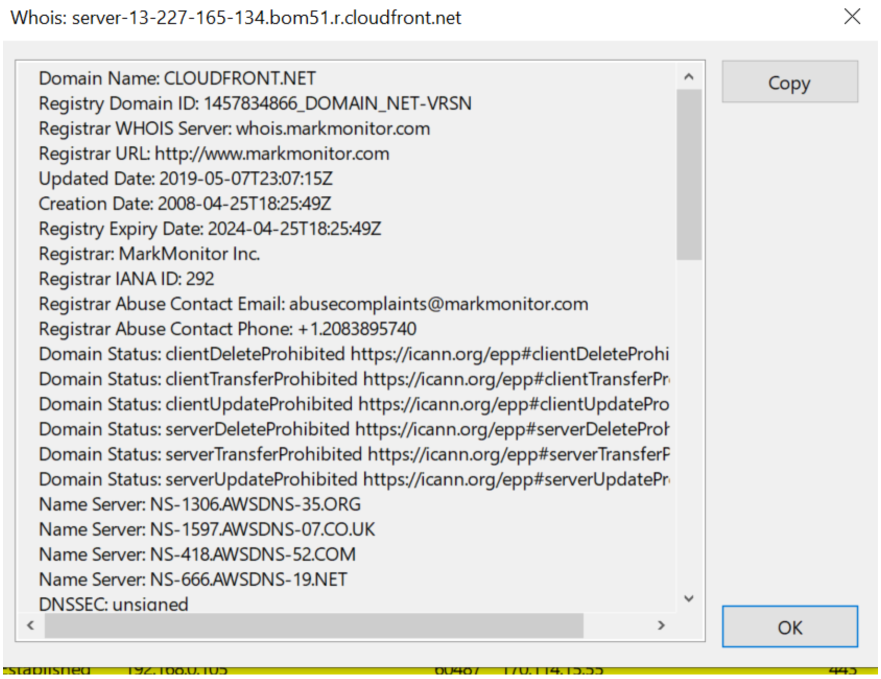


TCPView - Sysinternals: www.sysinternals.com

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	11752	UDP		192.168.140.1	62421	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDP		192.168.0.105	62422	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDP		127.0.0.1	62423	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	5160	UDP		127.0.0.1	62789	*		15-01-2022 19:44:36	iphlpsvc
svchost.exe	4996	UDPv6		::	500	*		15-01-2022 19:44:36	IKEEXT
svchost.exe	11752	UDPv6		::1	1900	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDPv6		fe80::3c:2db0:7fd8:b7c1	1900	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDPv6		fe80::3c:2db0:7fd8:b7c1	1900	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDPv6		fe80::3c:2db0:7fd8:b7c1	1900	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	2012	UDPv6		::	3702	*		17-01-2022 07:18:45	FDResPub
svchost.exe	2012	UDPv6		::	3702	*		17-01-2022 07:18:45	FDResPub
svchost.exe	4996	UDPv6		::	4500	*		15-01-2022 19:44:36	IKEEXT
svchost.exe	2628	UDPv6		::	5353	*		17-01-2022 07:16:57	Dnscache
TeamViewer_Service.exe	5328	UDPv6		fe80::3c:2db0:7fd8:b7c1	5353	*		15-01-2022 19:44:39	TeamViewer
TeamViewer_Service.exe	5328	UDPv6		fe80::3c:2db0:7fd8:b7c1	5353	*		15-01-2022 19:44:39	TeamViewer
svchost.exe	2628	UDPv6		::	5355	*		17-01-2022 07:47:08	Dnscache
TeamViewer_Service.exe	5328	UDPv6		::	49682	*		15-01-2022 19:44:39	TeamViewer
svchost.exe	2012	UDPv6		::	60093	*		15-01-2022 20:38:02	FDResPub
svchost.exe	11752	UDPv6		fe80::fc8c:93c5:3f65:9170	62416	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDPv6		fe80::3c:2db0:7fd8:b7c1	62417	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDPv6		fe80::c1ae:6da0:af24:c1d7	62418	*		17-01-2022 07:16:55	SSDPSRV
svchost.exe	11752	UDPv6		::1	62419	*		17-01-2022 07:16:55	SSDPSRV
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61780	127.0.0.1	3500	17-01-2022 07:56:44	brave.exe
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61781	127.0.0.1	3500	17-01-2022 07:56:45	brave.exe
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61783	127.0.0.1	3500	17-01-2022 07:56:46	brave.exe
brave.exe	21308	TCP	Syn Sent	127.0.0.1	61785	127.0.0.1	50000	17-01-2022 07:56:46	brave.exe
brave.exe	21308	TCPv6	Syn Sent	::1	61782	::1	50000	17-01-2022 07:56:46	brave.exe
brave.exe	21308	TCPv6	Syn Sent	::1	61784	::1	3500	17-01-2022 07:56:46	brave.exe

Endpoints: 133 Established: 20 Listening: 33 Time Wait: 15 Close Wait: 5 Update: 2 sec States: (All)



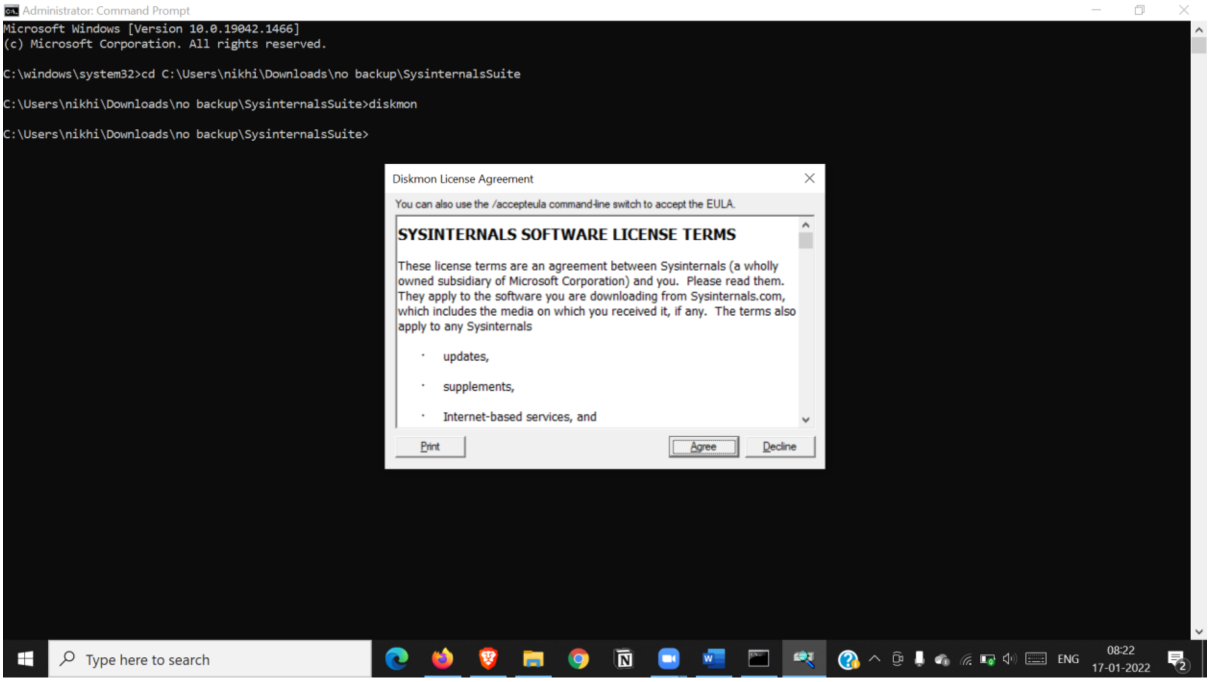


Whois: server-13-227-165-134.bom51.r.cloudfront.net

```
Domain Name: CLOUDFRONT.NET
Registry Domain ID: 1457834866_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-05-07T23:07:15Z
Creation Date: 2008-04-25T18:25:49Z
Registry Expiry Date: 2024-04-25T18:25:49Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhi
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPr
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePro
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProl
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferF
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdatePr
Name Server: NS-1306.AWSDNS-35.ORG
Name Server: NS-1597.AWSDNS-07.CO.UK
Name Server: NS-418.AWSDNS-52.COM
Name Server: NS-666.AWSDNS-19.NET
DNSSEC: unsigned
```

Practical 6
cf

Diskmonitoring



Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.19042.1466]
(c) Microsoft Corporation. All rights reserved.

C:\windows\system32>cd C:\Users\nikhi\Downloads\no backup\SysinternalsSuite

C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>diskmon

C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
```

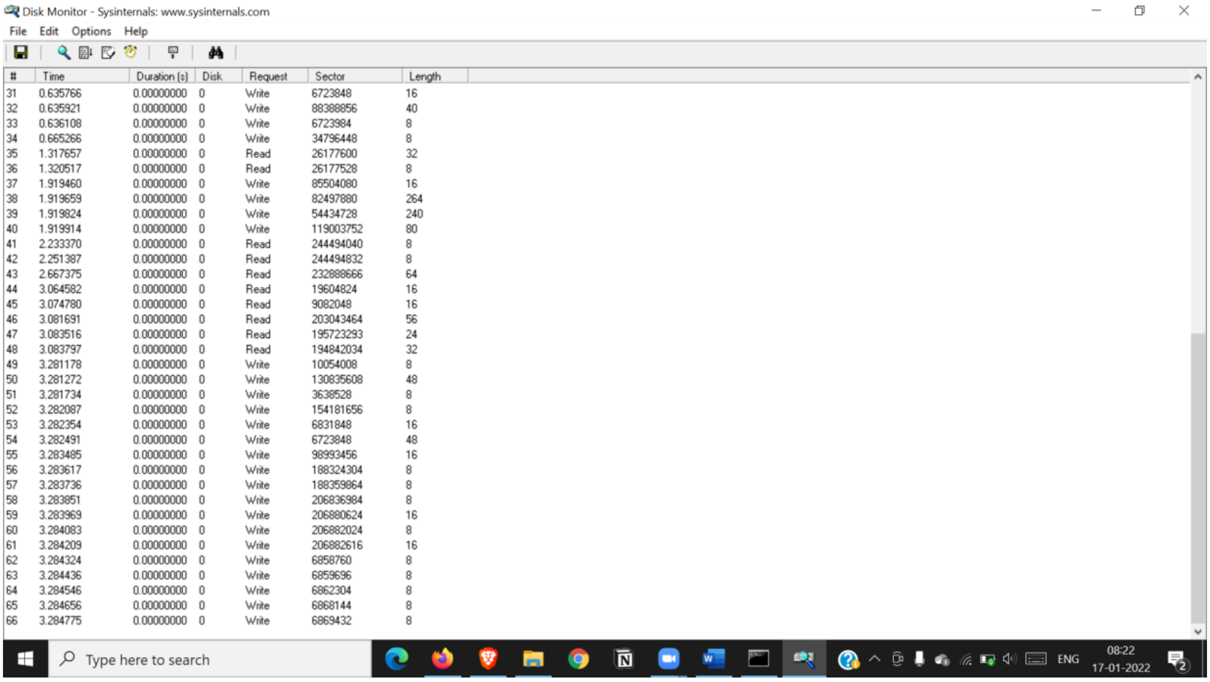
Diskmon License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

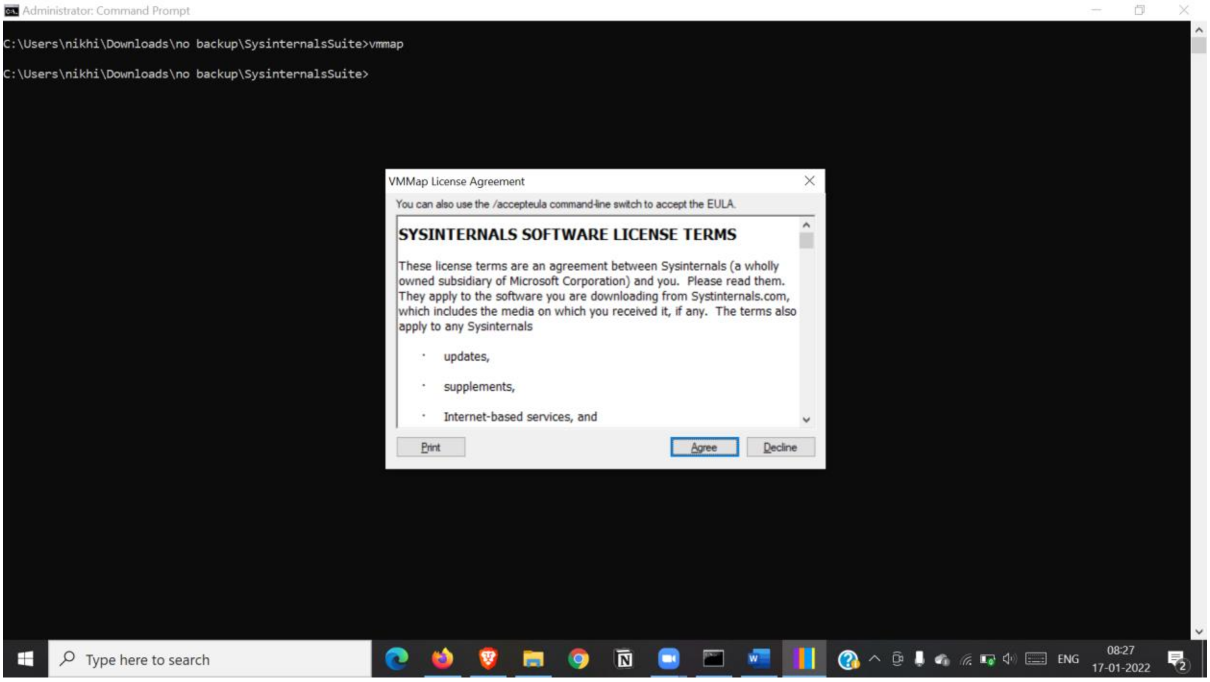
- updates,
- supplements,
- Internet-based services, and



Disk Monitor - Sysinternals: www.sysinternals.com

#	Time	Duration (s)	Disk	Request	Sector	Length
31	0.635766	0.00000000	0	Write	6723848	16
32	0.635921	0.00000000	0	Write	88388856	40
33	0.636108	0.00000000	0	Write	6723984	8
34	0.665266	0.00000000	0	Write	34796448	8
35	1.317657	0.00000000	0	Read	26177600	32
36	1.320517	0.00000000	0	Read	26177528	8
37	1.919460	0.00000000	0	Write	85504080	16
38	1.919659	0.00000000	0	Write	82497880	264
39	1.919824	0.00000000	0	Write	54434728	240
40	1.919914	0.00000000	0	Write	119003752	80
41	2.233370	0.00000000	0	Read	244494040	8
42	2.251387	0.00000000	0	Read	244494832	8
43	2.667375	0.00000000	0	Read	232888666	64
44	3.064582	0.00000000	0	Read	19604824	16
45	3.074780	0.00000000	0	Read	9082048	16
46	3.081691	0.00000000	0	Read	203043464	56
47	3.083516	0.00000000	0	Read	195723293	24
48	3.083797	0.00000000	0	Read	194842034	32
49	3.281178	0.00000000	0	Write	10054008	8
50	3.281272	0.00000000	0	Write	130835608	48
51	3.281734	0.00000000	0	Write	3638528	8
52	3.282087	0.00000000	0	Write	154181656	8
53	3.282354	0.00000000	0	Write	6831848	16
54	3.282491	0.00000000	0	Write	6723848	48
55	3.283485	0.00000000	0	Write	98993456	16
56	3.283617	0.00000000	0	Write	188324304	8
57	3.283736	0.00000000	0	Write	188359864	8
58	3.283851	0.00000000	0	Write	206836984	8
59	3.283969	0.00000000	0	Write	206880624	16
60	3.284083	0.00000000	0	Write	206882024	8
61	3.284209	0.00000000	0	Write	206882616	16
62	3.284324	0.00000000	0	Write	6858760	8
63	3.284436	0.00000000	0	Write	6859696	8
64	3.284546	0.00000000	0	Write	6862304	8
65	3.284656	0.00000000	0	Write	6868144	8
66	3.284775	0.00000000	0	Write	6869432	8

Virtual memory map



Administrator: Command Prompt

```
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>vmmap

C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
```

VMMap License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

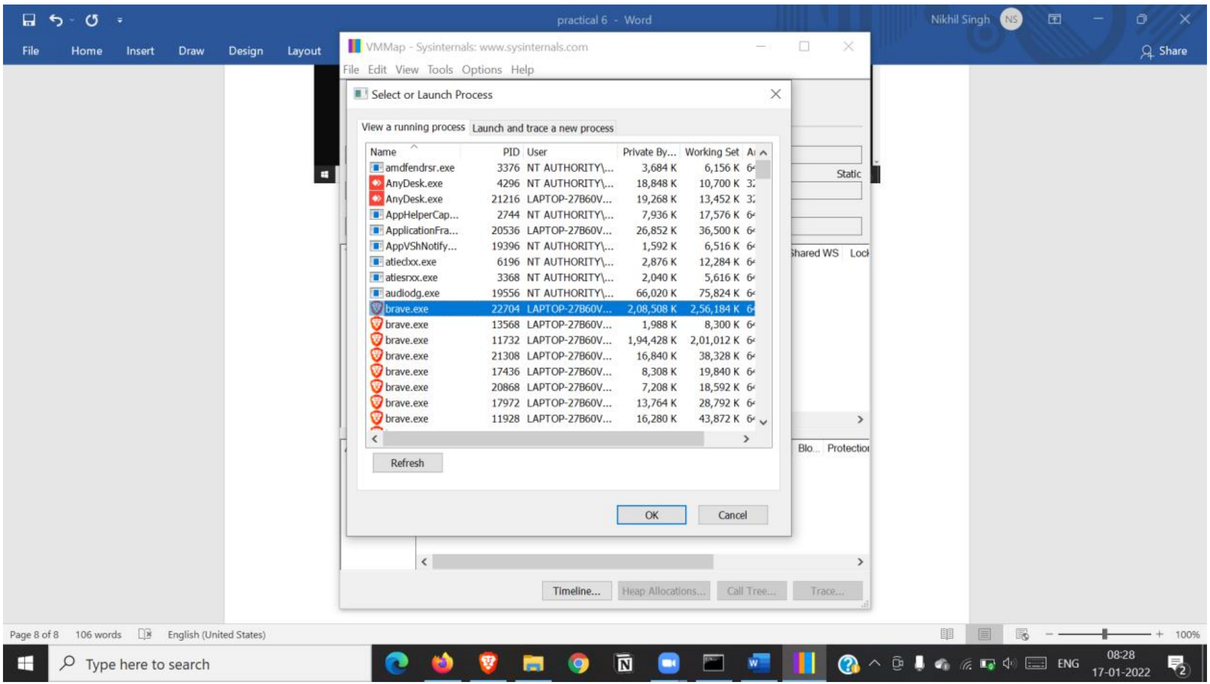
SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

- updates,
- supplements,
- Internet-based services, and

Practical 6

cf

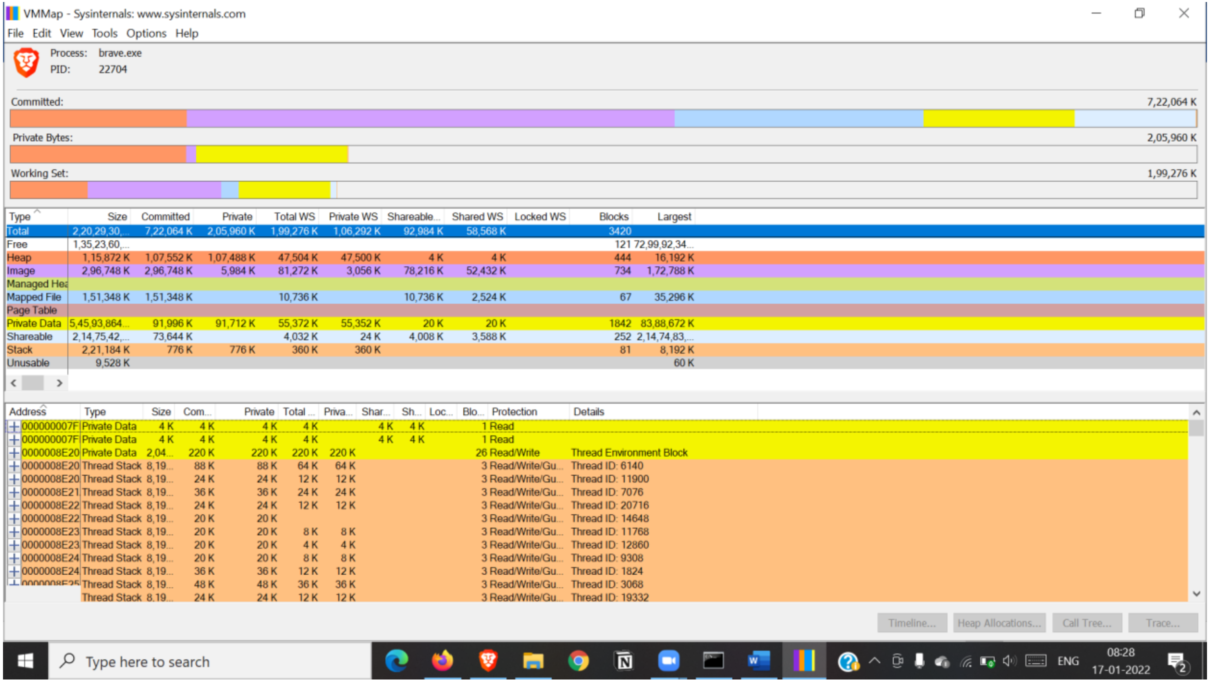


practical 6 - Word
Nikhil Singh
File
Home
Insert
Draw
Design
Layout
Share
VMMap - Sysinternals: www.sysinternals.com
File Edit View Tools Options Help
Page 8 of 8 106 words English (United States) 100%
Type here to search
ENG 08:28 17-01-2022

Select or Launch Process

View a running process | Launch and trace a new process

Name	PID	User	Private By...	Working Set	A
amdfendrsr.exe	3376	NT AUTHORITY\...	3,684 K	6,156 K	6
AnyDesk.exe	4296	NT AUTHORITY\...	18,848 K	10,700 K	3
AnyDesk.exe	21216	LAPTOP-27B60V...	19,268 K	13,452 K	3
AppHelperCap...	2744	NT AUTHORITY\...	7,936 K	17,576 K	6
ApplicationFra...	20536	LAPTOP-27B60V...	26,852 K	36,500 K	6
AppVShNotify...	19396	NT AUTHORITY\...	1,592 K	6,516 K	6
atieclxx.exe	6196	NT AUTHORITY\...	2,876 K	12,284 K	6
atiesrxx.exe	3368	NT AUTHORITY\...	2,040 K	5,616 K	6
audiodg.exe	19556	NT AUTHORITY\...	66,020 K	75,824 K	6
brave.exe	22704	LAPTOP-27B60V...	2,08,508 K	2,56,184 K	6
brave.exe	13568	LAPTOP-27B60V...	1,988 K	8,300 K	6
brave.exe	11732	LAPTOP-27B60V...	1,94,428 K	2,01,012 K	6
brave.exe	21308	LAPTOP-27B60V...	16,840 K	38,328 K	6
brave.exe	17436	LAPTOP-27B60V...	8,308 K	19,840 K	6
brave.exe	20868	LAPTOP-27B60V...	7,208 K	18,592 K	6
brave.exe	17972	LAPTOP-27B60V...	13,764 K	28,792 K	6
brave.exe	11928	LAPTOP-27B60V...	16,280 K	43,872 K	6



Process: brave.exe
PID: 22704

Committed: 7,22,064 K

Private Bytes: 2,05,960 K

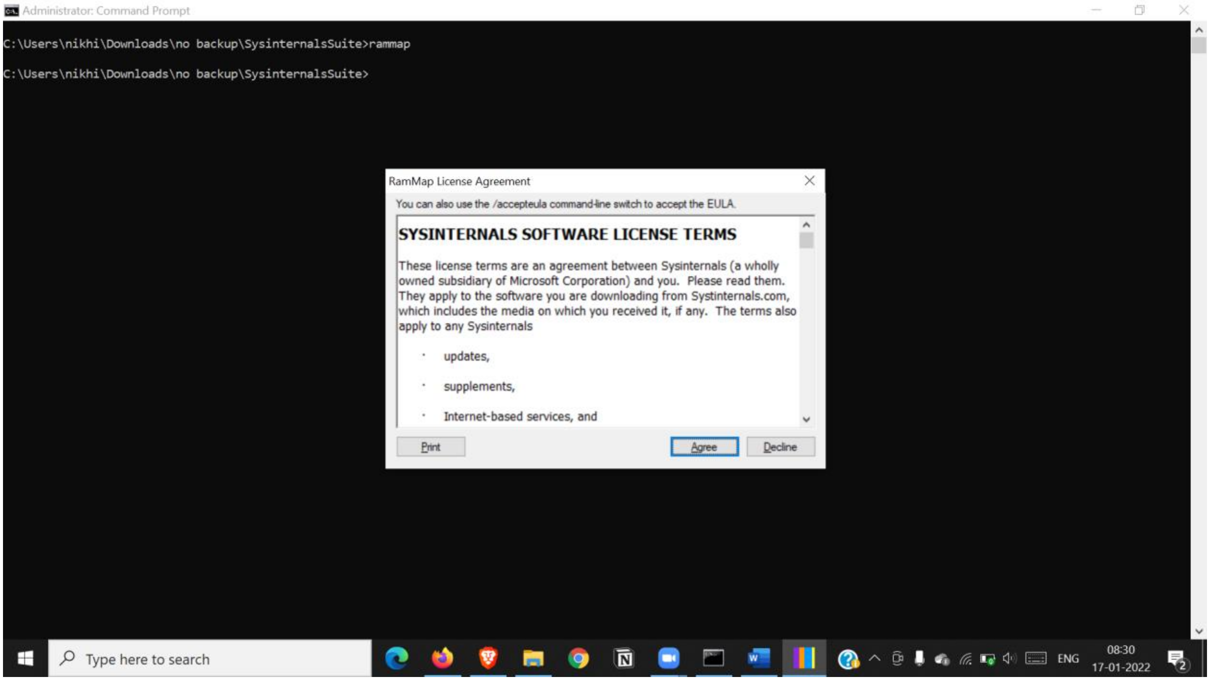
Working Set: 1,99,276 K

Type	Size	Committed	Private	Total WS	Private WS	Shareable...	Shared WS	Locked WS	Blocks	Largest
Total	2,20,29,30,...	7,22,064 K	2,05,960 K	1,99,276 K	1,06,292 K	92,984 K	58,568 K		3420	
Free	1,35,23,60,...								121	72,99,92,34...
Heap	1,15,872 K	1,07,552 K	1,07,488 K	47,504 K	47,500 K	4 K	4 K		444	16,192 K
Image	2,96,748 K	2,96,748 K	5,984 K	81,272 K	3,056 K	78,216 K	52,432 K		734	1,72,788 K
Managed Hea										
Mapped File	1,51,348 K	1,51,348 K		10,736 K		10,736 K	2,524 K		67	35,296 K
Page Table										
Private Data	5,45,93,864...	91,996 K	91,712 K	55,372 K	55,352 K	20 K	20 K		1842	83,88,672 K
Shareable	2,14,75,42,...	73,644 K		4,032 K	24 K	4,008 K	3,588 K		252	2,14,74,83,...
Stack	2,21,184 K	776 K	776 K	360 K	360 K				81	8,192 K
Unusable	9,528 K									60 K

Address	Type	Size	Com...	Private	Total ...	Priva...	Shar...	Sh...	Loc...	Blo...	Protection	Details
000000007F	Private Data	4 K	4 K	4 K	4 K		4 K	4 K		1	Read	
000000007F	Private Data	4 K	4 K	4 K	4 K		4 K	4 K		1	Read	
0000008E20	Private Data	2,04...	220 K	220 K	220 K	220 K				26	Read/Write	Thread Environment Block
0000008E20	Thread Stack	8,19...	88 K	88 K	64 K	64 K				3	Read/Write/Gu...	Thread ID: 6140
0000008E20	Thread Stack	8,19...	24 K	24 K	12 K	12 K				3	Read/Write/Gu...	Thread ID: 11900
0000008E21	Thread Stack	8,19...	36 K	36 K	24 K	24 K				3	Read/Write/Gu...	Thread ID: 7076
0000008E22	Thread Stack	8,19...	24 K	24 K	12 K	12 K				3	Read/Write/Gu...	Thread ID: 20716
0000008E22	Thread Stack	8,19...	20 K	20 K						3	Read/Write/Gu...	Thread ID: 14648
0000008E23	Thread Stack	8,19...	20 K	20 K	8 K	8 K				3	Read/Write/Gu...	Thread ID: 11768
0000008E23	Thread Stack	8,19...	20 K	20 K	4 K	4 K				3	Read/Write/Gu...	Thread ID: 12860
0000008E24	Thread Stack	8,19...	20 K	20 K	8 K	8 K				3	Read/Write/Gu...	Thread ID: 9308
0000008E24	Thread Stack	8,19...	36 K	36 K	12 K	12 K				3	Read/Write/Gu...	Thread ID: 1824
0000008E25	Thread Stack	8,19...	48 K	48 K	36 K	36 K				3	Read/Write/Gu...	Thread ID: 3068
	Thread Stack	8,19...	24 K	24 K	12 K	12 K				3	Read/Write/Gu...	Thread ID: 19332

Practical 6
cf

Rammap



```
C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>rammap

C:\Users\nikhi\Downloads\no backup\SysinternalsSuite>
```

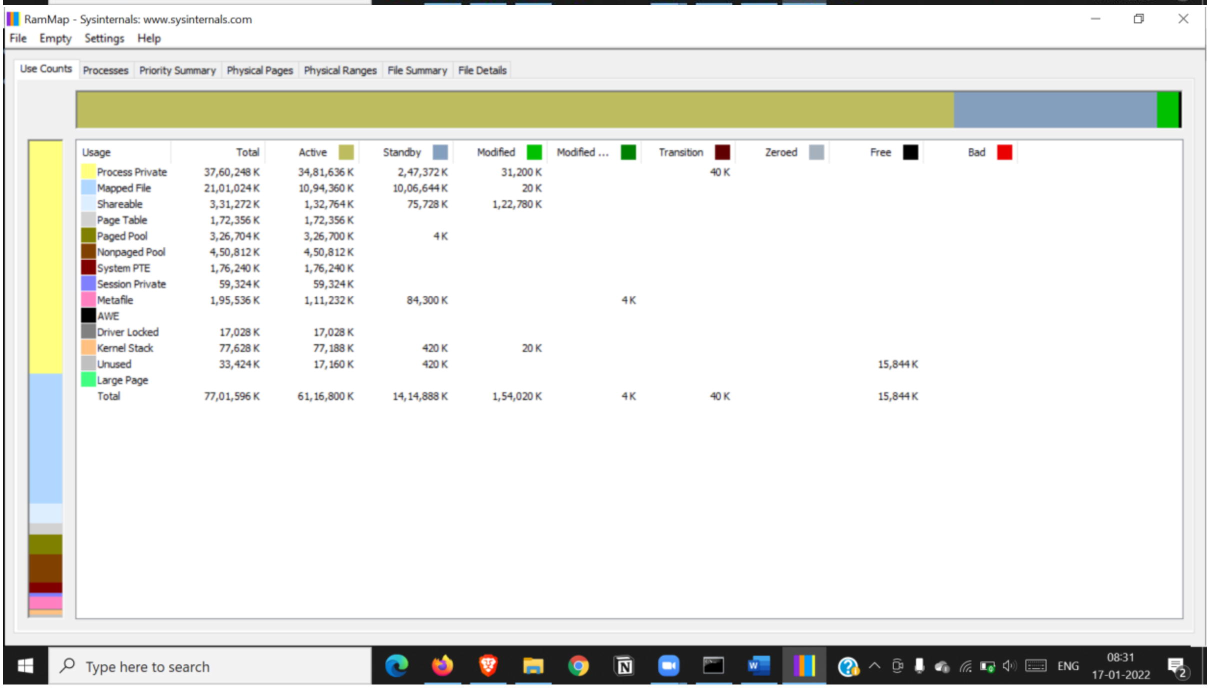
RamMap License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

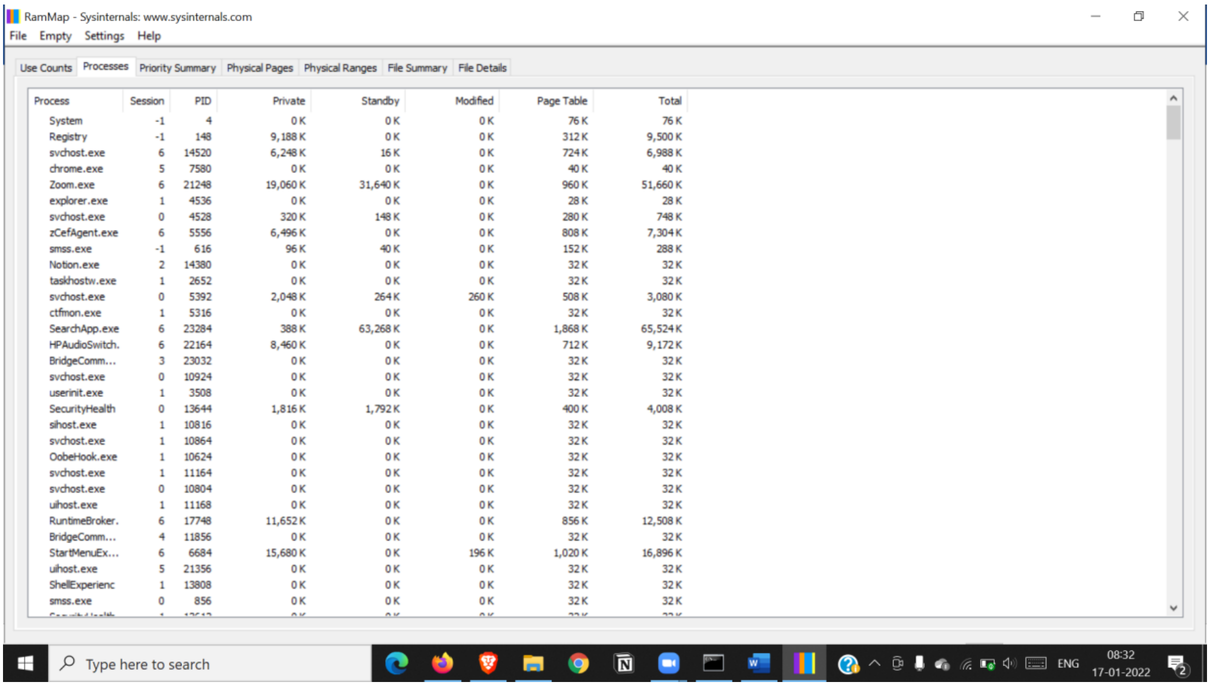
- updates,
- supplements,
- Internet-based services, and



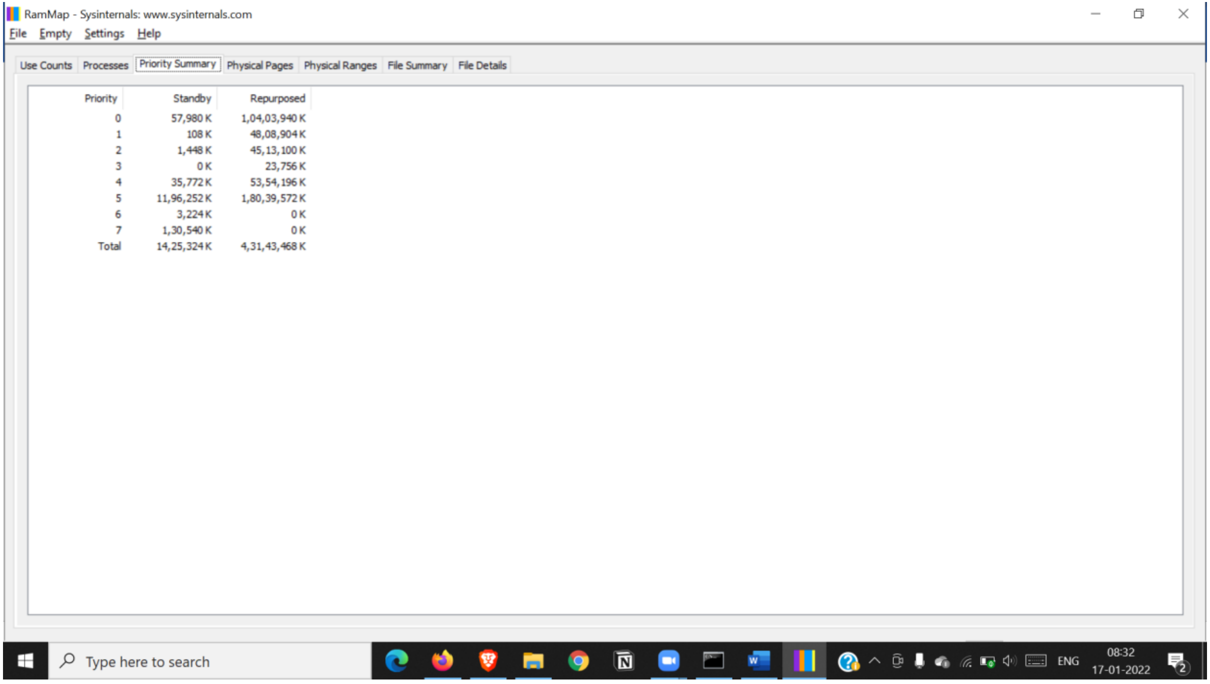
Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	37,60,248 K	34,81,636 K	2,47,372 K	31,200 K		40 K			
Mapped File	21,01,024 K	10,94,360 K	10,06,644 K	20 K					
Shareable	3,31,272 K	1,32,764 K	75,728 K	1,22,780 K					
Page Table	1,72,356 K	1,72,356 K							
Paged Pool	3,26,704 K	3,26,700 K	4 K						
Nonpaged Pool	4,50,812 K	4,50,812 K							
System PTE	1,76,240 K	1,76,240 K							
Session Private	59,324 K	59,324 K							
Metafile	1,95,536 K	1,11,232 K	84,300 K		4 K				
AWE									
Driver Locked	17,028 K	17,028 K							
Kernel Stack	77,628 K	77,188 K	420 K	20 K					
Unused	33,424 K	17,160 K	420 K					15,844 K	
Large Page									
Total	77,01,596 K	61,16,800 K	14,14,888 K	1,54,020 K	4 K	40 K		15,844 K	

Practical 6

cf

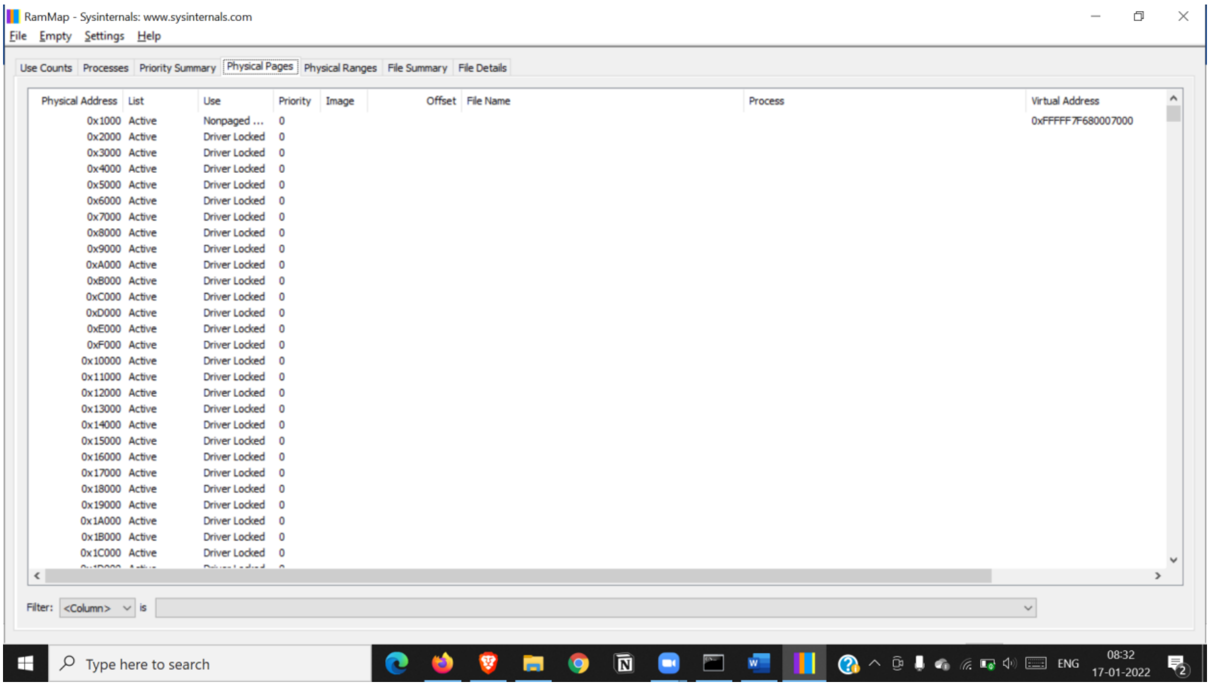


Process	Session	PID	Private	Standby	Modified	Page Table	Total
System	-1	4	0 K	0 K	0 K	76 K	76 K
Registry	-1	148	9,188 K	0 K	0 K	312 K	9,500 K
svchost.exe	6	14520	6,248 K	16 K	0 K	724 K	6,988 K
chrome.exe	5	7580	0 K	0 K	0 K	40 K	40 K
Zoom.exe	6	21248	19,060 K	31,640 K	0 K	960 K	51,660 K
explorer.exe	1	4536	0 K	0 K	0 K	28 K	28 K
svchost.exe	0	4528	320 K	148 K	0 K	280 K	748 K
zCefAgent.exe	6	5556	6,496 K	0 K	0 K	808 K	7,304 K
smss.exe	-1	616	96 K	40 K	0 K	152 K	288 K
Notion.exe	2	14380	0 K	0 K	0 K	32 K	32 K
taskhostw.exe	1	2652	0 K	0 K	0 K	32 K	32 K
svchost.exe	0	5392	2,048 K	264 K	260 K	508 K	3,080 K
ctfmon.exe	1	5316	0 K	0 K	0 K	32 K	32 K
SearchApp.exe	6	23284	388 K	63,268 K	0 K	1,868 K	65,524 K
HPAudioSwitch.	6	22164	8,460 K	0 K	0 K	712 K	9,172 K
BridgeComm...	3	23032	0 K	0 K	0 K	32 K	32 K
svchost.exe	0	10924	0 K	0 K	0 K	32 K	32 K
userinit.exe	1	3508	0 K	0 K	0 K	32 K	32 K
SecurityHealth	0	13644	1,816 K	1,792 K	0 K	400 K	4,008 K
sihost.exe	1	10816	0 K	0 K	0 K	32 K	32 K
svchost.exe	1	10864	0 K	0 K	0 K	32 K	32 K
OobeHook.exe	1	10624	0 K	0 K	0 K	32 K	32 K
svchost.exe	1	11164	0 K	0 K	0 K	32 K	32 K
svchost.exe	0	10804	0 K	0 K	0 K	32 K	32 K
uihost.exe	1	11168	0 K	0 K	0 K	32 K	32 K
RuntimeBroker.	6	17748	11,652 K	0 K	0 K	856 K	12,508 K
BridgeComm...	4	11856	0 K	0 K	0 K	32 K	32 K
StartMenuEx...	6	6684	15,680 K	0 K	196 K	1,020 K	16,896 K
uihost.exe	5	21356	0 K	0 K	0 K	32 K	32 K
ShellExperienc	1	13808	0 K	0 K	0 K	32 K	32 K
smss.exe	0	856	0 K	0 K	0 K	32 K	32 K

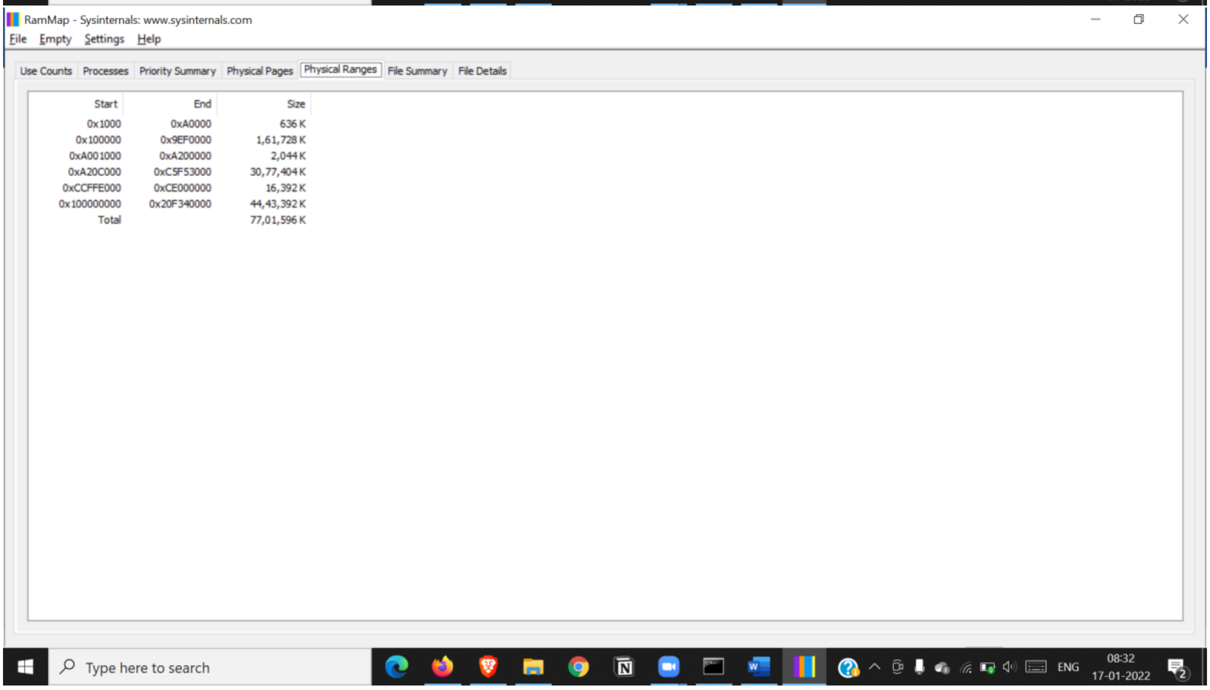


Priority	Standby	Repurposed
0	57,980 K	1,04,03,940 K
1	108 K	48,08,904 K
2	1,448 K	45,13,100 K
3	0 K	23,756 K
4	35,772 K	53,54,196 K
5	11,96,252 K	1,80,39,572 K
6	3,224 K	0 K
7	1,30,540 K	0 K
Total	14,25,324 K	4,31,43,468 K

Practical 6
cf


RamMap - Sysinternals: www.sysinternals.com
File Empty Settings Help
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details
Filter: <Column> is
Type here to search
ENG
08:32
17-01-2022

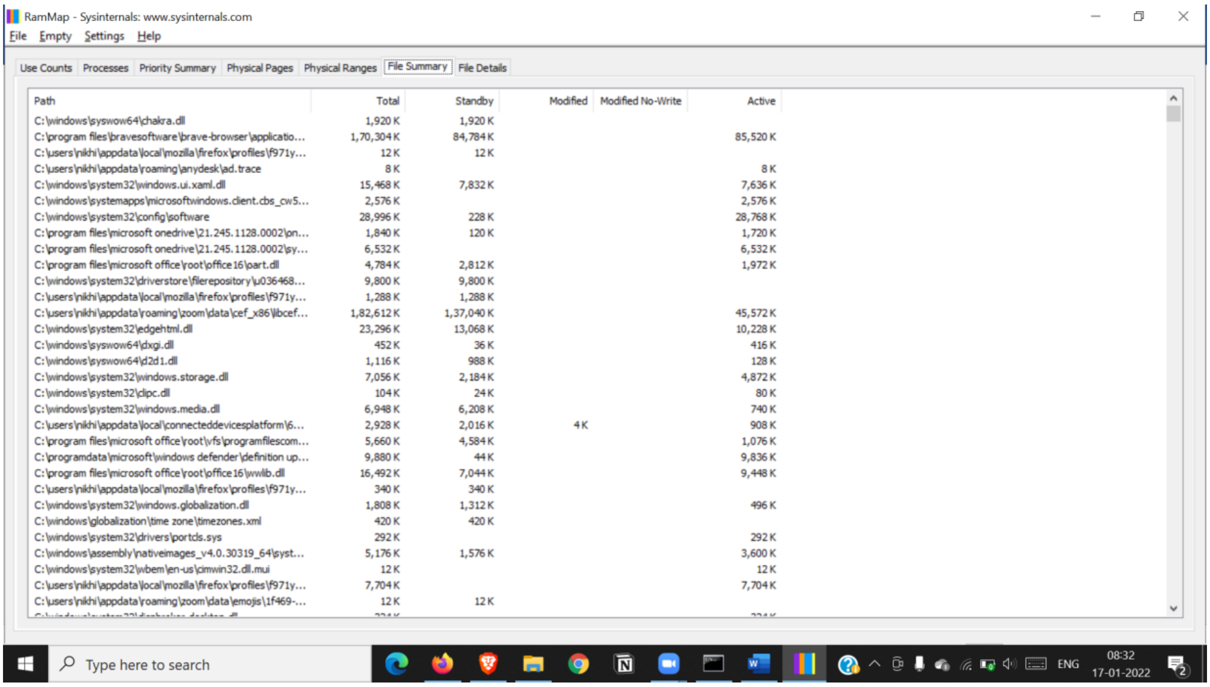
Physical Address	List	Use	Priority	Image	Offset	File Name	Process	Virtual Address
0x1000	Active	Nonpaged ...	0					0xFFFFF7F680007000
0x2000	Active	Driver Locked	0					
0x3000	Active	Driver Locked	0					
0x4000	Active	Driver Locked	0					
0x5000	Active	Driver Locked	0					
0x6000	Active	Driver Locked	0					
0x7000	Active	Driver Locked	0					
0x8000	Active	Driver Locked	0					
0x9000	Active	Driver Locked	0					
0xA000	Active	Driver Locked	0					
0xB000	Active	Driver Locked	0					
0xC000	Active	Driver Locked	0					
0xD000	Active	Driver Locked	0					
0xE000	Active	Driver Locked	0					
0xF000	Active	Driver Locked	0					
0x10000	Active	Driver Locked	0					
0x11000	Active	Driver Locked	0					
0x12000	Active	Driver Locked	0					
0x13000	Active	Driver Locked	0					
0x14000	Active	Driver Locked	0					
0x15000	Active	Driver Locked	0					
0x16000	Active	Driver Locked	0					
0x17000	Active	Driver Locked	0					
0x18000	Active	Driver Locked	0					
0x19000	Active	Driver Locked	0					
0x1A000	Active	Driver Locked	0					
0x1B000	Active	Driver Locked	0					
0x1C000	Active	Driver Locked	0					
0x1D000	Active	Driver Locked	0					


RamMap - Sysinternals: www.sysinternals.com
File Empty Settings Help
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details
Type here to search
ENG
08:32
17-01-2022

Start	End	Size
0x1000	0xA0000	636 K
0x100000	0x9EF0000	1,61,728 K
0xA001000	0xA200000	2,044 K
0xA20C000	0xC5F53000	30,77,404 K
0xCCFFE000	0xCE000000	16,392 K
0x100000000	0x20F340000	44,43,392 K
Total		77,01,596 K

Practical 6

cf

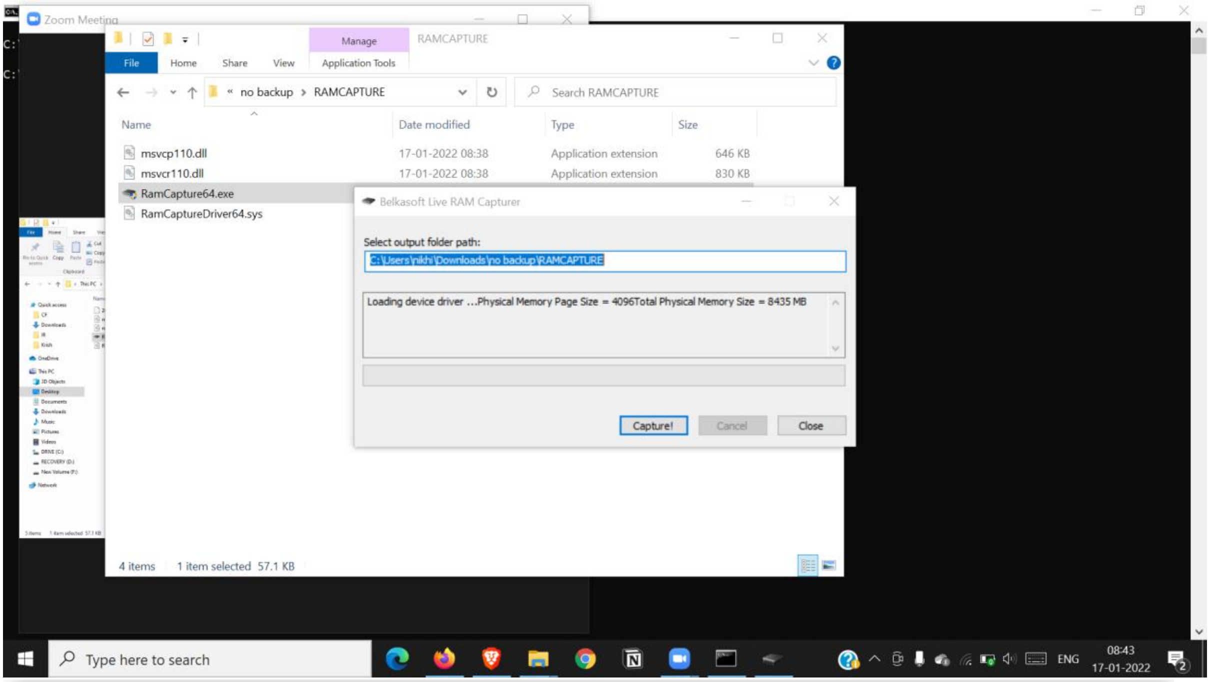


RamMap - Sysinternals: www.sysinternals.com
File Empty Settings Help
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details
Type here to search
ENG
08:32
17-01-2022

Path	Total	Standby	Modified	Modified No-Write	Active
C:\windows\syswow64\chakra.dll	1,920 K	1,920 K			
C:\program files\bravesoftware\brave-browser\applicatio...	1,70,304 K	84,784 K			85,520 K
C:\users\nikhi\appdata\local\mozilla\firefox\profiles\f971y...	12 K	12 K			
C:\users\nikhi\appdata\roaming\anydesk\ad.trace	8 K				8 K
C:\windows\system32\windows.ui.xaml.dll	15,468 K	7,832 K			7,636 K
C:\windows\systemapps\microsoftwindows.client.cbs_cw5...	2,576 K				2,576 K
C:\windows\system32\config\software	28,996 K	228 K			28,768 K
C:\program files\microsoft onedrive\21.245.1128.0002\on...	1,840 K	120 K			1,720 K
C:\program files\microsoft onedrive\21.245.1128.0002\sy...	6,532 K				6,532 K
C:\program files\microsoft office\root\office16\part.dll	4,784 K	2,812 K			1,972 K
C:\windows\system32\driverstore\filerepository\u036468...	9,800 K	9,800 K			
C:\users\nikhi\appdata\local\mozilla\firefox\profiles\f971y...	1,288 K	1,288 K			
C:\users\nikhi\appdata\roaming\zoom\data\cef_x86\libcef...	1,82,612 K	1,37,040 K			45,572 K
C:\windows\system32\edgehtml.dll	23,296 K	13,068 K			10,228 K
C:\windows\syswow64\dxgi.dll	452 K	36 K			416 K
C:\windows\syswow64\d2d1.dll	1,116 K	988 K			128 K
C:\windows\system32\windows.storage.dll	7,056 K	2,184 K			4,872 K
C:\windows\system32\clipc.dll	104 K	24 K			80 K
C:\windows\system32\windows.media.dll	6,948 K	6,208 K			740 K
C:\users\nikhi\appdata\local\connecteddevicesplatform\6...	2,928 K	2,016 K	4 K		908 K
C:\program files\microsoft office\root\vfs\programfilescom...	5,660 K	4,584 K			1,076 K
C:\programdata\microsoft\windows defender\definition up...	9,880 K	44 K			9,836 K
C:\program files\microsoft office\root\office16\wwlib.dll	16,492 K	7,044 K			9,448 K
C:\users\nikhi\appdata\local\mozilla\firefox\profiles\f971y...	340 K	340 K			
C:\windows\system32\windows.globalization.dll	1,808 K	1,312 K			496 K
C:\windows\globalization\time zone\timezones.xml	420 K	420 K			
C:\windows\system32\drivers\portcls.sys	292 K				292 K
C:\windows\assembly\nativeimages_v4.0.30319_64\syst...	5,176 K	1,576 K			3,600 K
C:\windows\system32\wbem\en-us\cimwin32.dll.mui	12 K				12 K
C:\users\nikhi\appdata\local\mozilla\firefox\profiles\f971y...	7,704 K				7,704 K
C:\users\nikhi\appdata\roaming\zoom\data\emojis\1f469-...	12 K	12 K			

Practical 6
cf

Ram capture



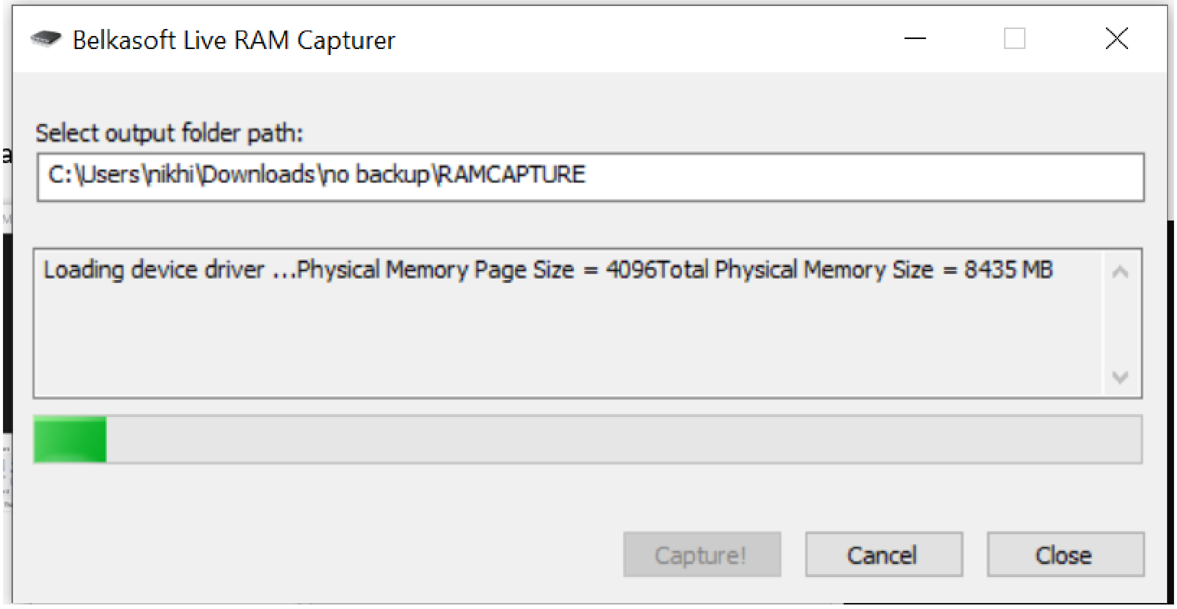
Name	Date modified	Type	Size
msvcp110.dll	17-01-2022 08:38	Application extension	646 KB
msvcr110.dll	17-01-2022 08:38	Application extension	830 KB
RamCapture64.exe			
RamCaptureDriver64.sys			

4 items 1 item selected 57.1 KB

Belkasoft Live RAM Capturer

Select output folder path: C:\Users\nikhi\Downloads\no backup\RAMCAPTURE

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 8435 MB
```

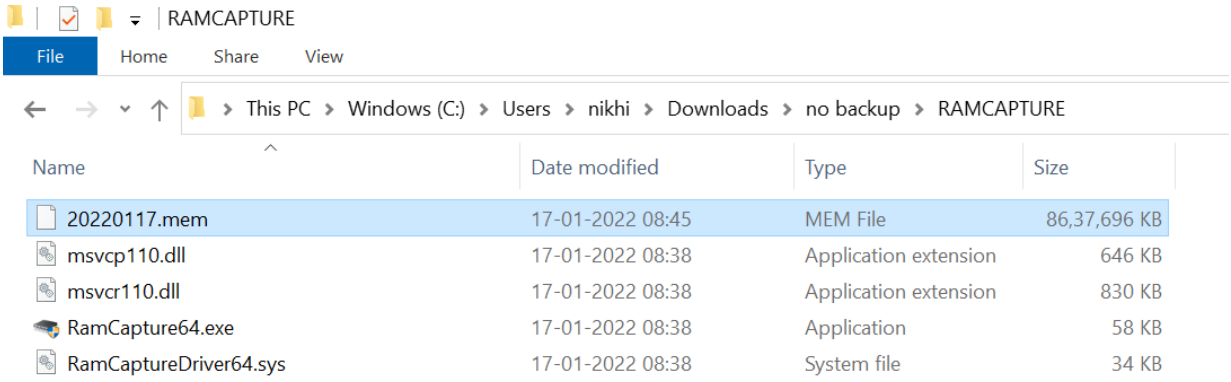


Belkasoft Live RAM Capturer

Select output folder path:

C:\Users\nikhi\Downloads\no backup\RAMCAPTURE

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 8435 MB
```



This PC › Windows (C:) › Users › nikhi › Downloads › no backup › RAMCAPTURE

Name	Date modified	Type	Size
20220117.mem	17-01-2022 08:45	MEM File	86,37,696 KB
msvcp110.dll	17-01-2022 08:38	Application extension	646 KB
msvcr110.dll	17-01-2022 08:38	Application extension	830 KB
RamCapture64.exe	17-01-2022 08:38	Application	58 KB
RamCaptureDriver64.sys	17-01-2022 08:38	System file	34 KB