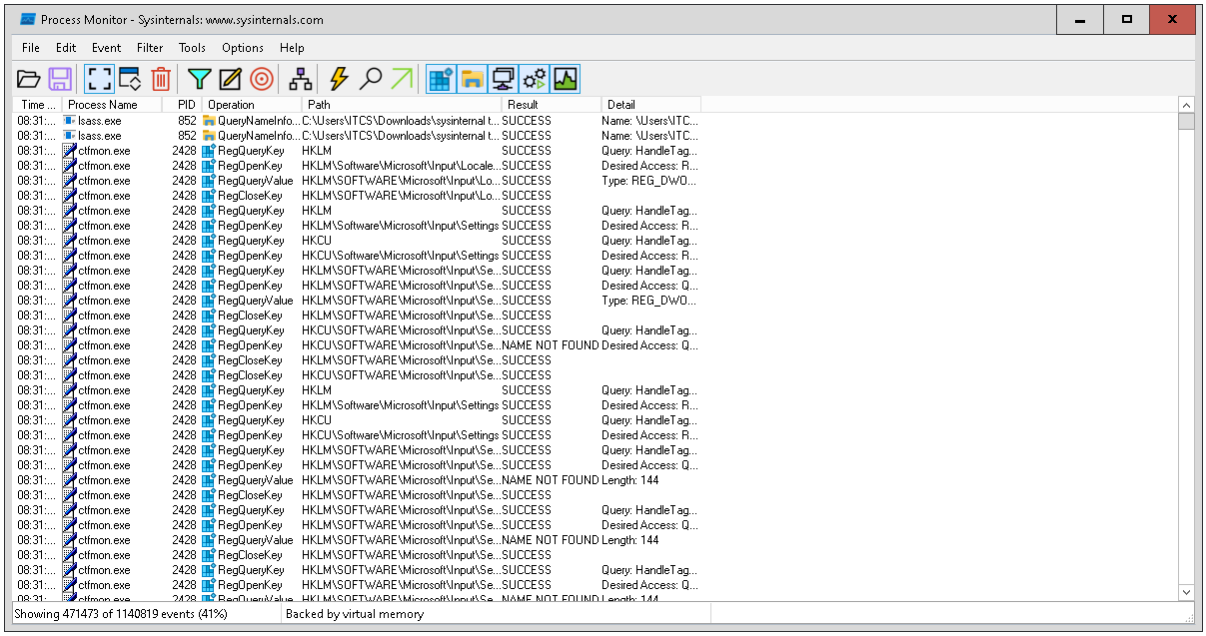
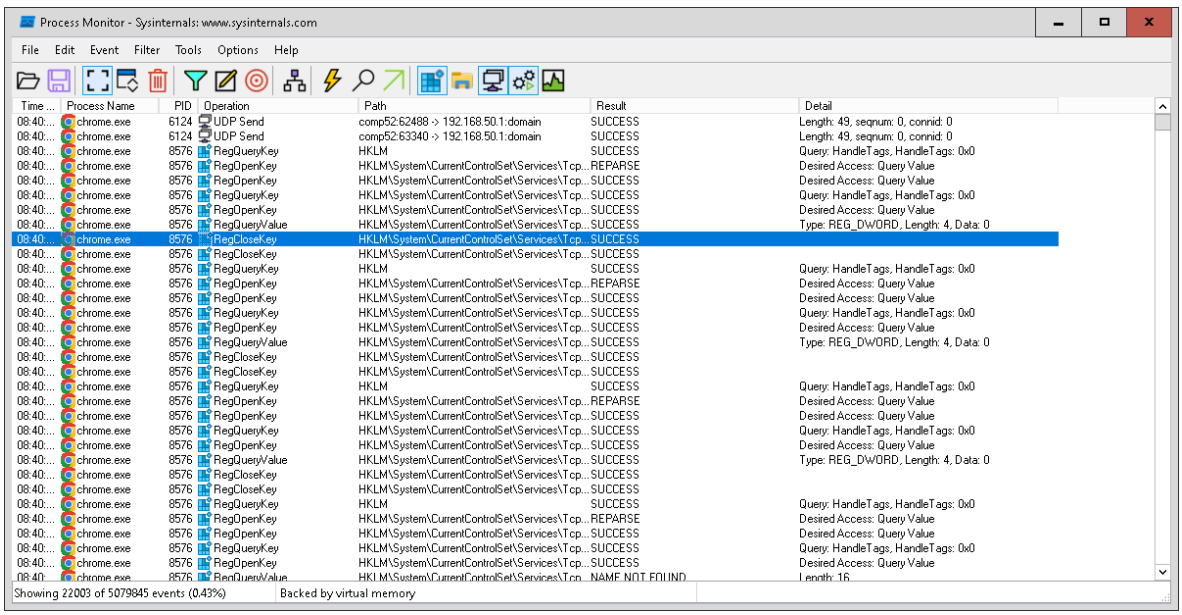
Part (a) - Using the Process Monitor:

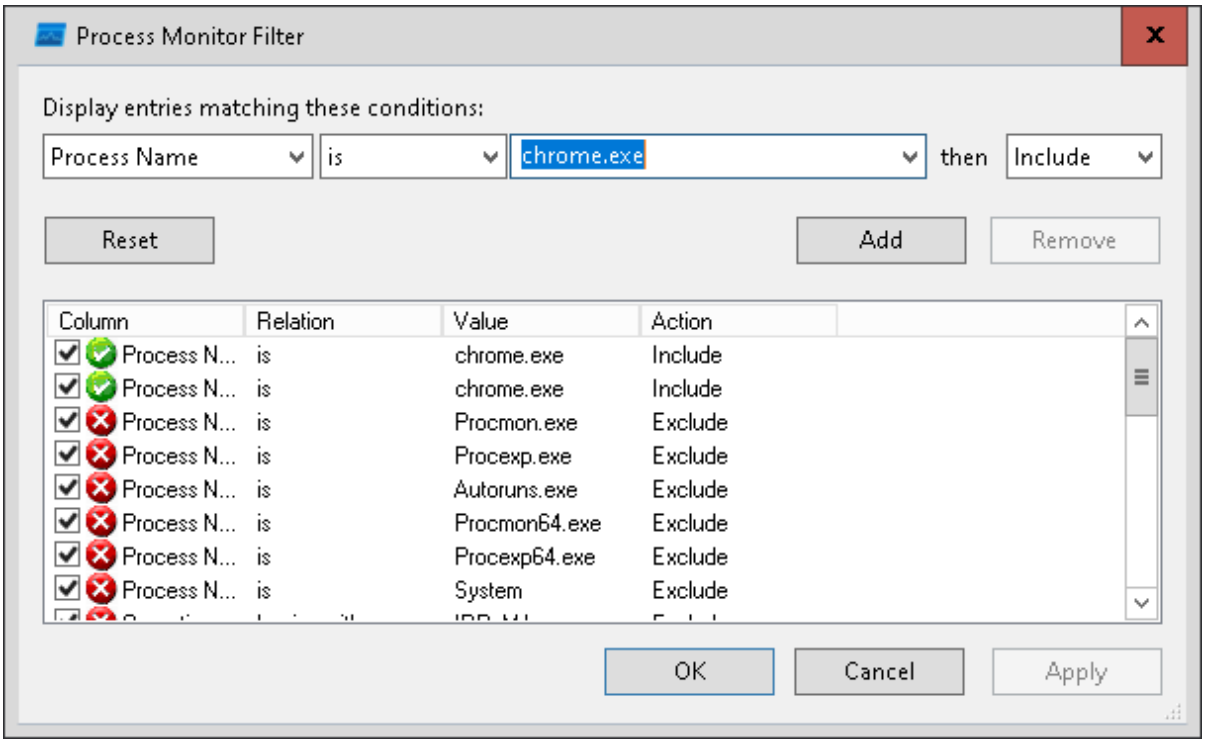
Step 1: Open Chrome browser and search any random thing. Run the Process Monitor as administrator. Click on “Start Capturing”.



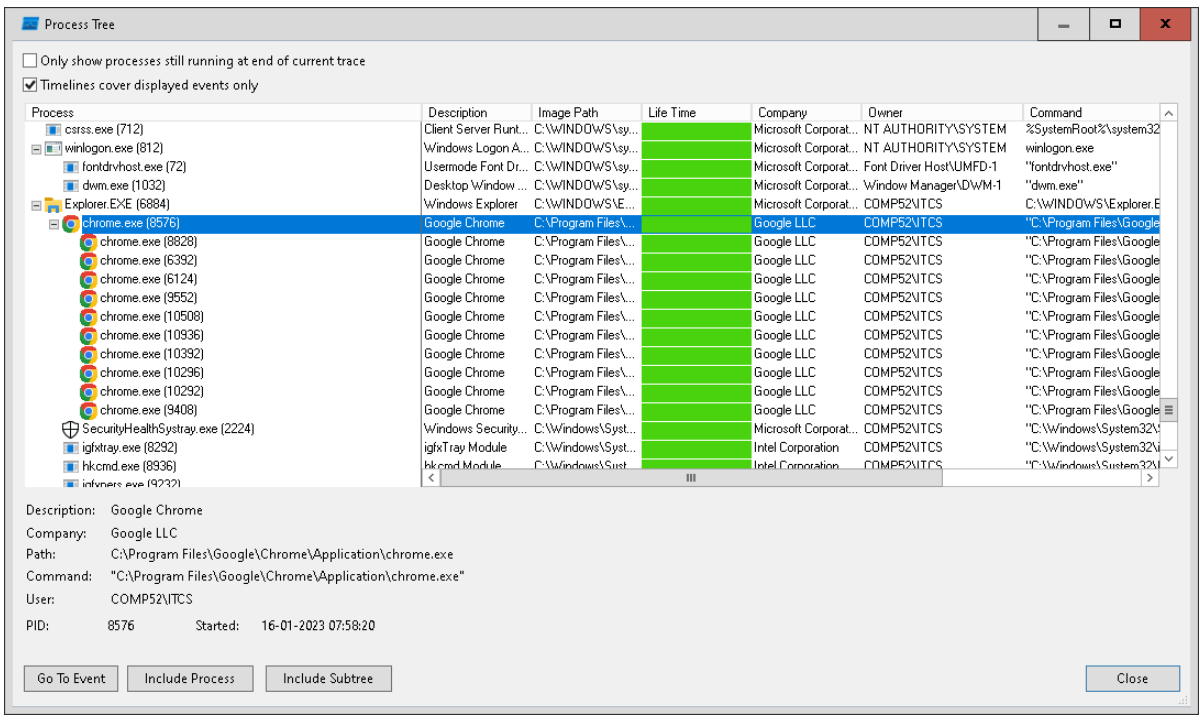
Step 2: Go to filter. Select “process name”, Select “is”, Select chrome.exe and click ok.



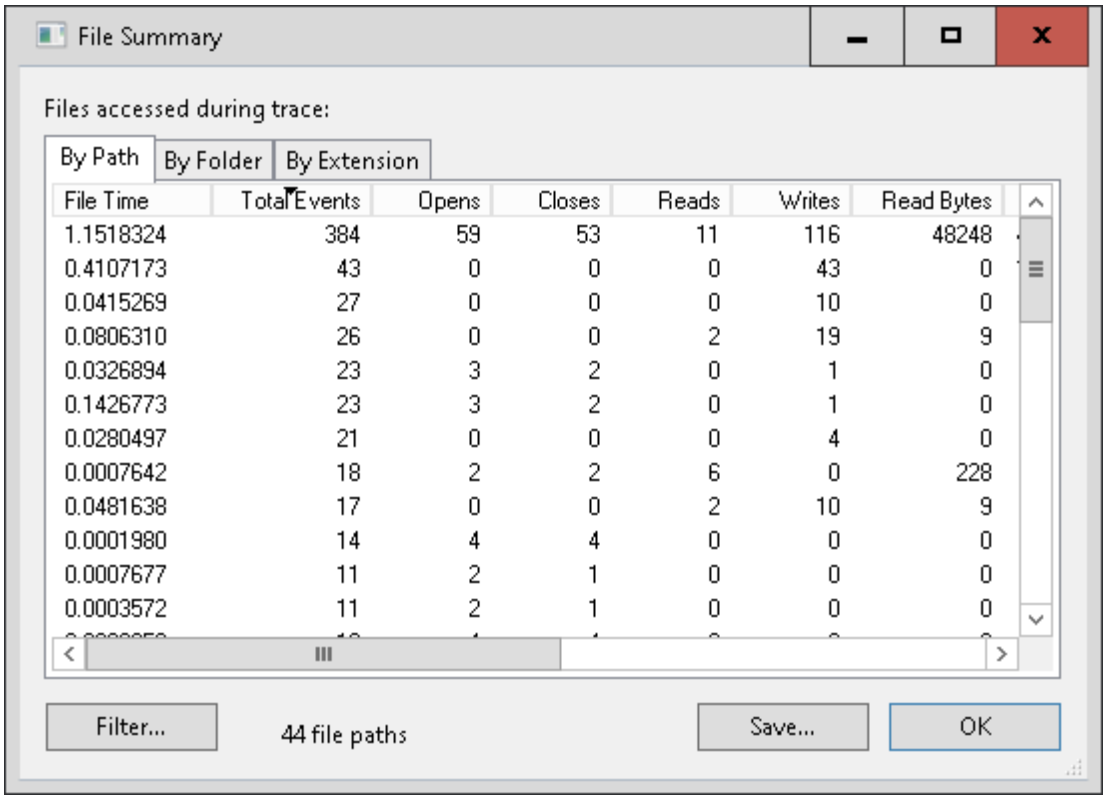
Step 3: The monitor will filter out only the Chrome.exe processes.



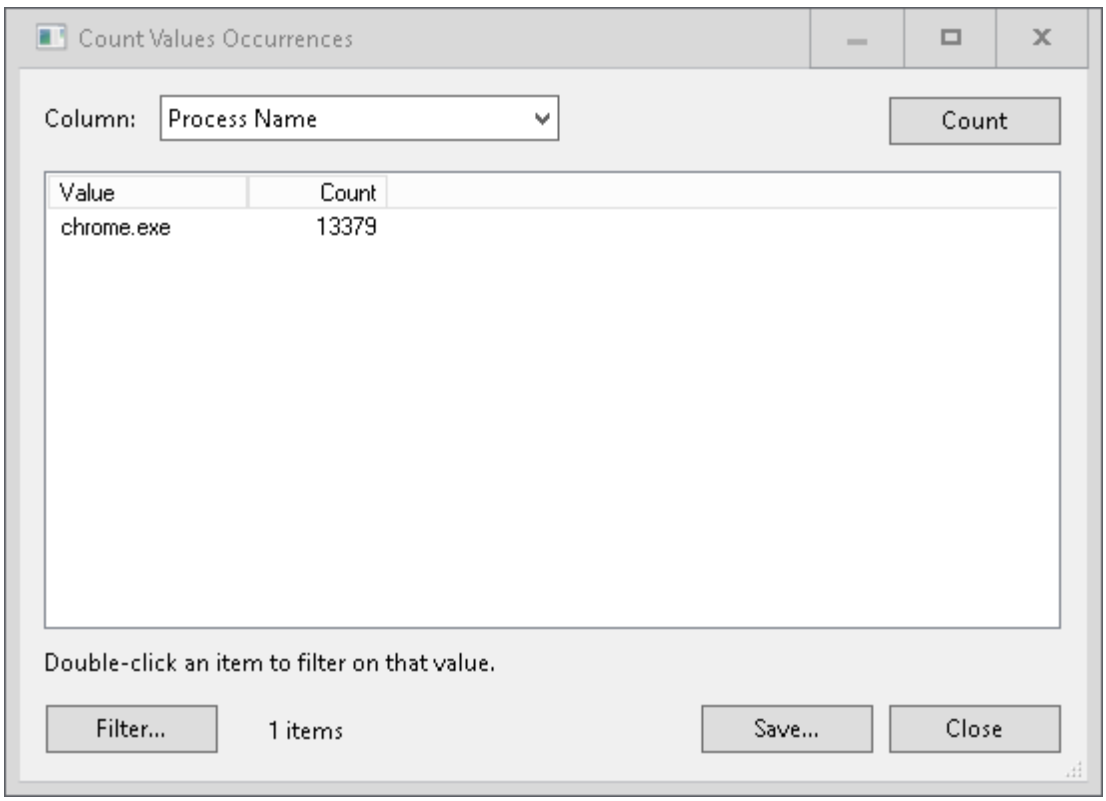
Step 4: Go to tools -> process tree. You can see the hierarchical structure of the processes.



Step 5: Go to File Summary. Here you can see the overall file summary. You can filter this summary to filter out a certain process. Here we filter out Chrome.exe process.



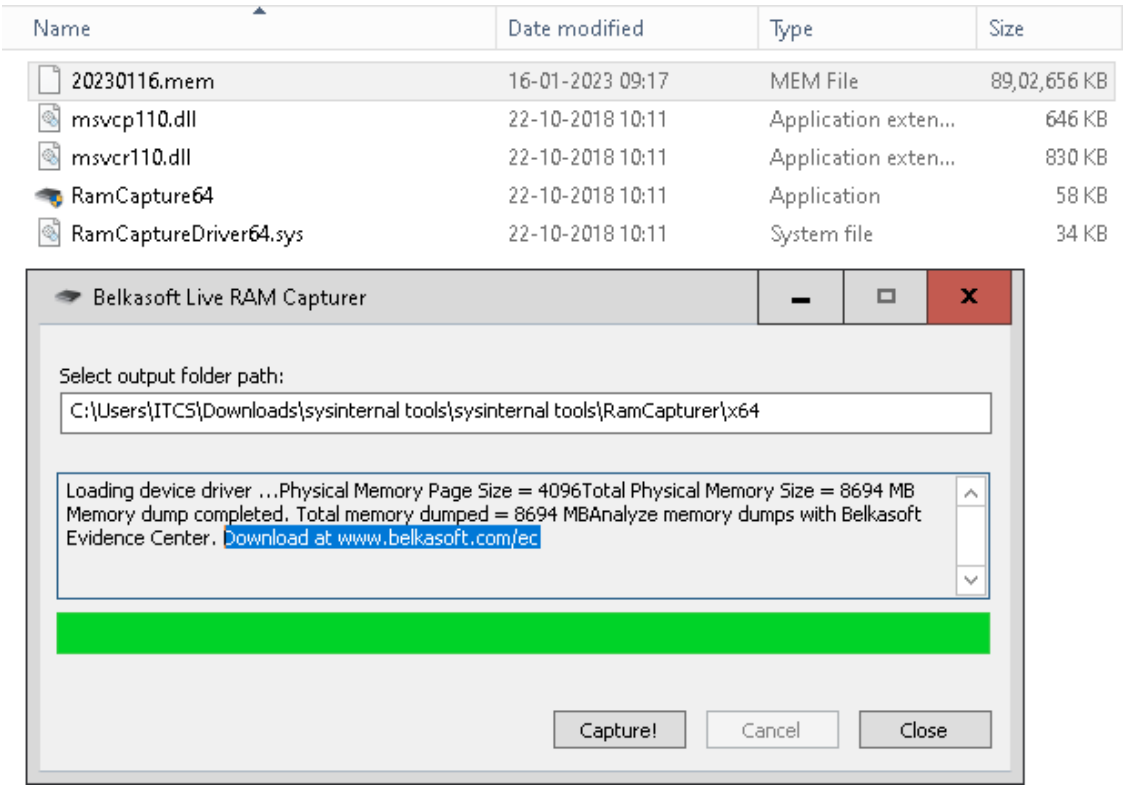
File Time	Total Events	Opens	Closes	Reads	Writes	Read Bytes
1.1518324	384	59	53	11	116	48248
0.4107173	43	0	0	0	43	0
0.0415269	27	0	0	0	10	0
0.0806310	26	0	0	2	19	9
0.0326894	23	3	2	0	1	0
0.1426773	23	3	2	0	1	0
0.0280497	21	0	0	0	4	0
0.0007642	18	2	2	6	0	228
0.0481638	17	0	0	2	10	9
0.0001980	14	4	4	0	0	0
0.0007677	11	2	1	0	0	0
0.0003572	11	2	1	0	0	0



Value	Count
chrome.exe	13379

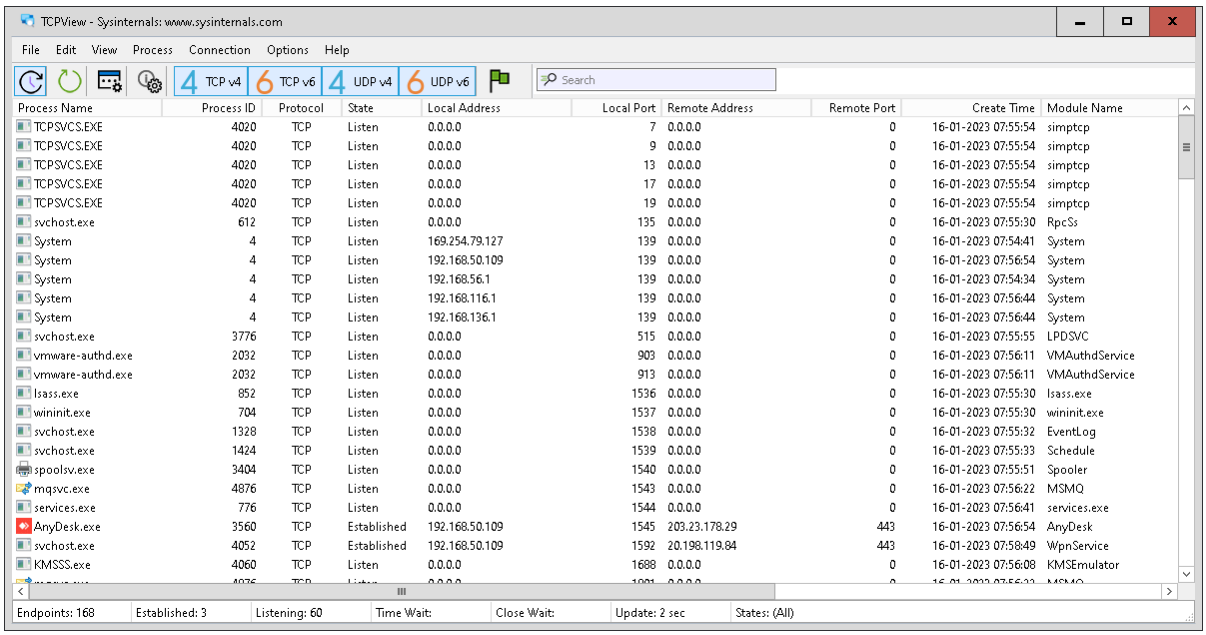
Part (b) – Using the RAM Capturer:

Step 1: Run the RAMCapturer program. Set your destination and Click Capture.



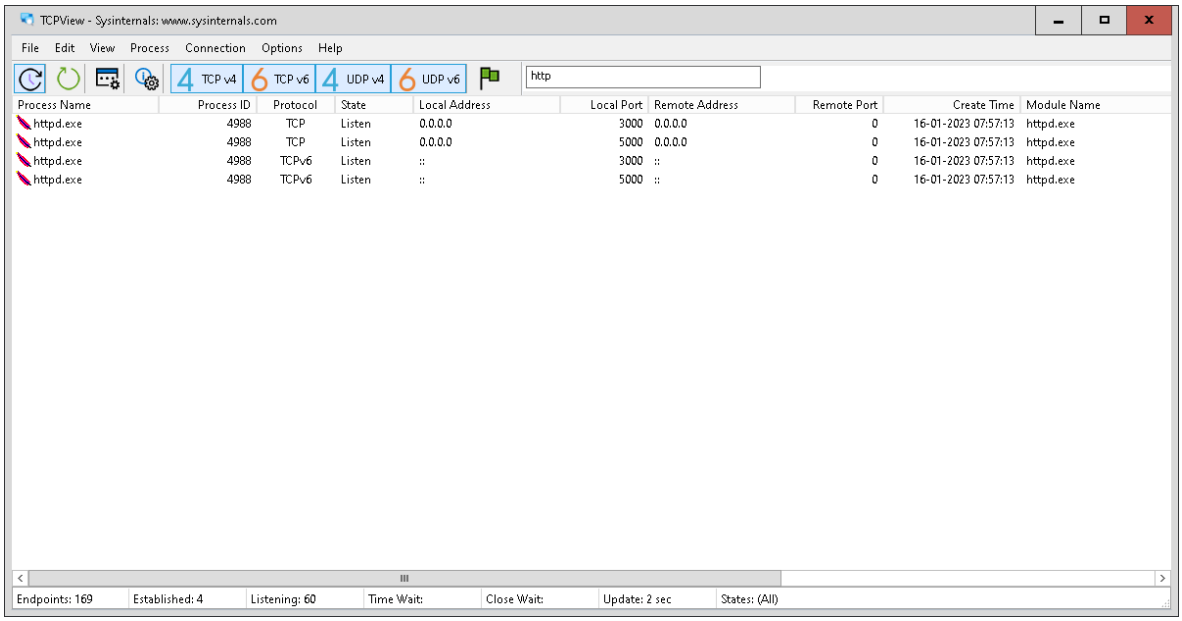
Part (c) – Using the TCP View:

Step 1: Run the TCPView program. Select the options TCPP v4,TCP v6, UPD v4, UDP v6.



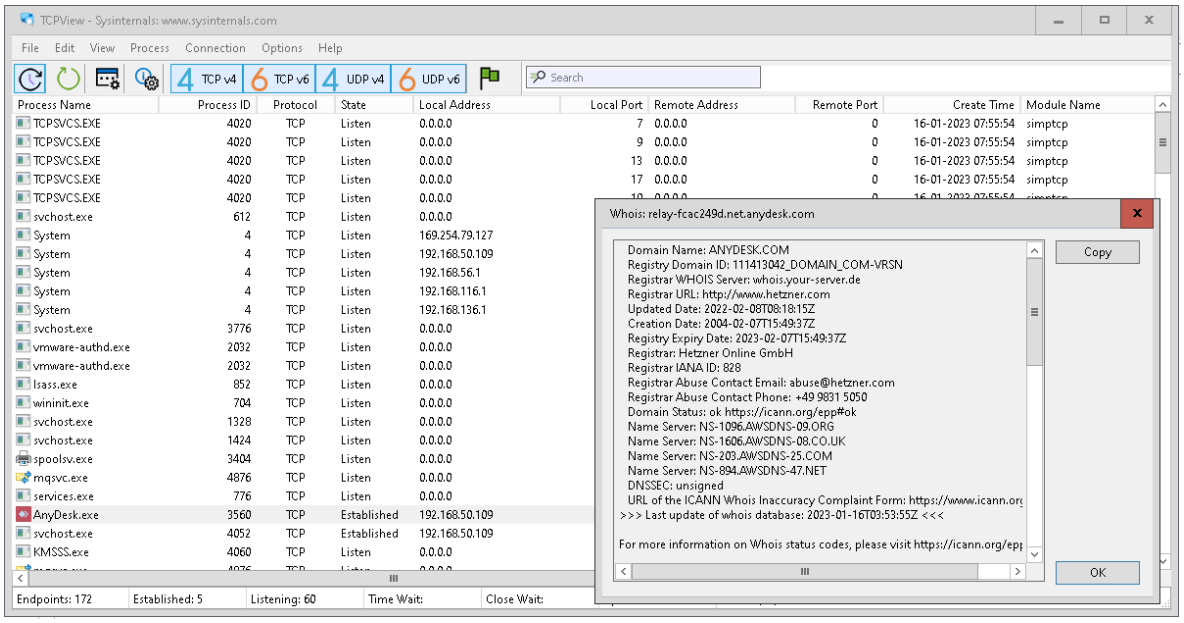
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
TCPSVCS.EXE	4020	TCP	Listen	0.0.0.0	7	0.0.0.0	0	16-01-2023 07:55:54	simptcp
TCPSVCS.EXE	4020	TCP	Listen	0.0.0.0	9	0.0.0.0	0	16-01-2023 07:55:54	simptcp
TCPSVCS.EXE	4020	TCP	Listen	0.0.0.0	13	0.0.0.0	0	16-01-2023 07:55:54	simptcp
TCPSVCS.EXE	4020	TCP	Listen	0.0.0.0	17	0.0.0.0	0	16-01-2023 07:55:54	simptcp
TCPSVCS.EXE	4020	TCP	Listen	0.0.0.0	19	0.0.0.0	0	16-01-2023 07:55:54	simptcp
svchost.exe	612	TCP	Listen	0.0.0.0	135	0.0.0.0	0	16-01-2023 07:55:30	RpcSs
System	4	TCP	Listen	169.254.79.127	139	0.0.0.0	0	16-01-2023 07:54:41	System
System	4	TCP	Listen	192.168.50.109	139	0.0.0.0	0	16-01-2023 07:56:54	System
System	4	TCP	Listen	192.168.56.1	139	0.0.0.0	0	16-01-2023 07:54:34	System
System	4	TCP	Listen	192.168.116.1	139	0.0.0.0	0	16-01-2023 07:56:44	System
System	4	TCP	Listen	192.168.136.1	139	0.0.0.0	0	16-01-2023 07:56:44	System
svchost.exe	3776	TCP	Listen	0.0.0.0	515	0.0.0.0	0	16-01-2023 07:55:55	LPDSVC
vmware-authd.exe	2032	TCP	Listen	0.0.0.0	903	0.0.0.0	0	16-01-2023 07:56:11	VMAuthdService
vmware-authd.exe	2032	TCP	Listen	0.0.0.0	913	0.0.0.0	0	16-01-2023 07:56:11	VMAuthdService
lsass.exe	852	TCP	Listen	0.0.0.0	1536	0.0.0.0	0	16-01-2023 07:55:30	lsass.exe
wininit.exe	704	TCP	Listen	0.0.0.0	1537	0.0.0.0	0	16-01-2023 07:55:30	wininit.exe
svchost.exe	1328	TCP	Listen	0.0.0.0	1538	0.0.0.0	0	16-01-2023 07:55:32	EventLog
svchost.exe	1424	TCP	Listen	0.0.0.0	1539	0.0.0.0	0	16-01-2023 07:55:33	Schedule
spoolsv.exe	3404	TCP	Listen	0.0.0.0	1540	0.0.0.0	0	16-01-2023 07:55:51	Spooler
mqsvc.exe	4876	TCP	Listen	0.0.0.0	1543	0.0.0.0	0	16-01-2023 07:56:22	MSMQ
services.exe	776	TCP	Listen	0.0.0.0	1544	0.0.0.0	0	16-01-2023 07:56:41	services.exe
AnyDesk.exe	3560	TCP	Established	192.168.50.109	1545	203.23.178.29	443	16-01-2023 07:56:54	AnyDesk
svchost.exe	4052	TCP	Established	192.168.50.109	1592	20.198.119.84	443	16-01-2023 07:58:49	WpnService
KMSSS.exe	4060	TCP	Listen	0.0.0.0	1688	0.0.0.0	0	16-01-2023 07:56:08	KMSEmulator

Step 2: In the Search bar, search “http”. Only the http processes will filter out.



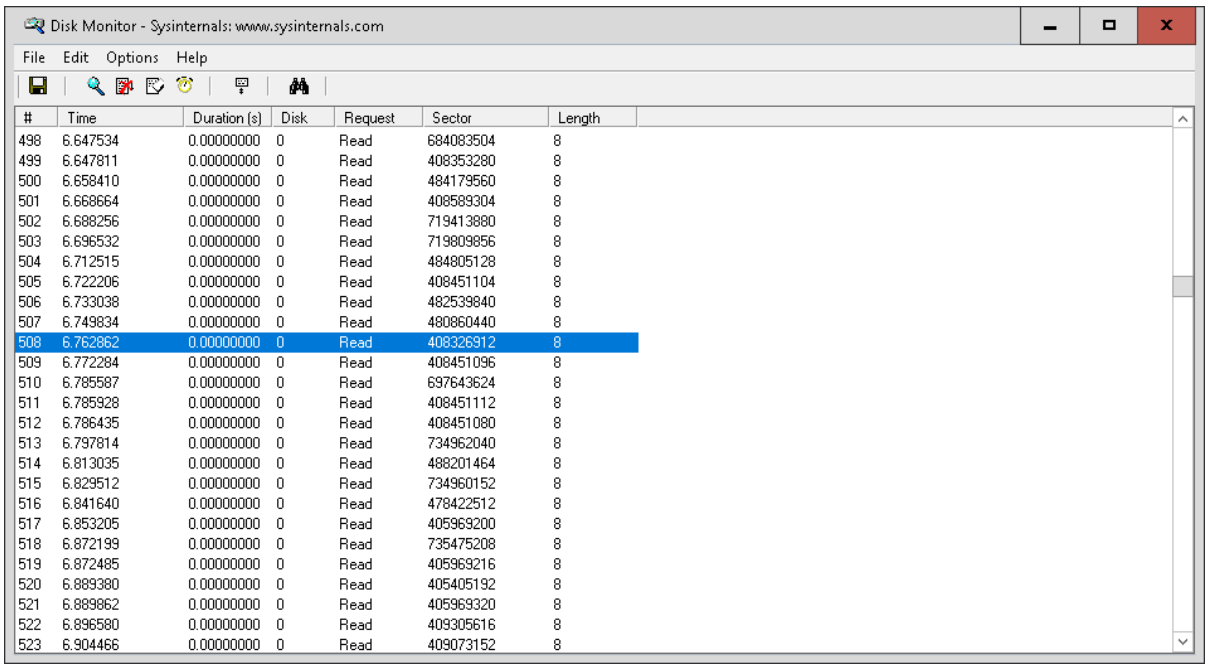
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
httpd.exe	4988	TCP	Listen	0.0.0.0	3000	0.0.0.0	0	16-01-2023 07:57:13	httpd.exe
httpd.exe	4988	TCP	Listen	0.0.0.0	5000	0.0.0.0	0	16-01-2023 07:57:13	httpd.exe
httpd.exe	4988	TCPv6	Listen	::	3000	::	0	16-01-2023 07:57:13	httpd.exe
httpd.exe	4988	TCPv6	Listen	::	5000	::	0	16-01-2023 07:57:13	httpd.exe

Step 3: Now select any process -> Right click -> whois. It will show the who.is information about that process.



Part (d) – Using Disk Monitor:

Step 1: Run the Disk Monitor as administrator. You can see all the disk processes.



#	Time	Duration (s)	Disk	Request	Sector	Length
498	6.647534	0.00000000	0	Read	684083504	8
499	6.647811	0.00000000	0	Read	408353280	8
500	6.658410	0.00000000	0	Read	484179560	8
501	6.668664	0.00000000	0	Read	408589304	8
502	6.688256	0.00000000	0	Read	719413880	8
503	6.696532	0.00000000	0	Read	719809856	8
504	6.712515	0.00000000	0	Read	484805128	8
505	6.722206	0.00000000	0	Read	408451104	8
506	6.733038	0.00000000	0	Read	482539840	8
507	6.749834	0.00000000	0	Read	480860440	8
508	6.762862	0.00000000	0	Read	408326912	8
509	6.772284	0.00000000	0	Read	408451096	8
510	6.785587	0.00000000	0	Read	697643624	8
511	6.785928	0.00000000	0	Read	408451112	8
512	6.786435	0.00000000	0	Read	408451080	8
513	6.797814	0.00000000	0	Read	734962040	8
514	6.813035	0.00000000	0	Read	488201464	8
515	6.829512	0.00000000	0	Read	734960152	8
516	6.841640	0.00000000	0	Read	478422512	8
517	6.853205	0.00000000	0	Read	405969200	8
518	6.872199	0.00000000	0	Read	735475208	8
519	6.872485	0.00000000	0	Read	405969216	8
520	6.889380	0.00000000	0	Read	405405192	8
521	6.889862	0.00000000	0	Read	405969320	8
522	6.896580	0.00000000	0	Read	409305616	8
523	6.904466	0.00000000	0	Read	409073152	8

Part (e) – Using VMMap:

Step 1: Run the VMMap Application as administrator. Select any application(here Anydesk). You can see all the process information about that application.