NAME : SATHYAPRAKASH SAHOO **CLASS** : BSC. TY. CS

ROLL NO : CS- 4124 **DIV** : 2 **BATCH** : C

SUBJECT : CYBER FORENSICS - PRACTICAL

PRACTICAL NO. 6

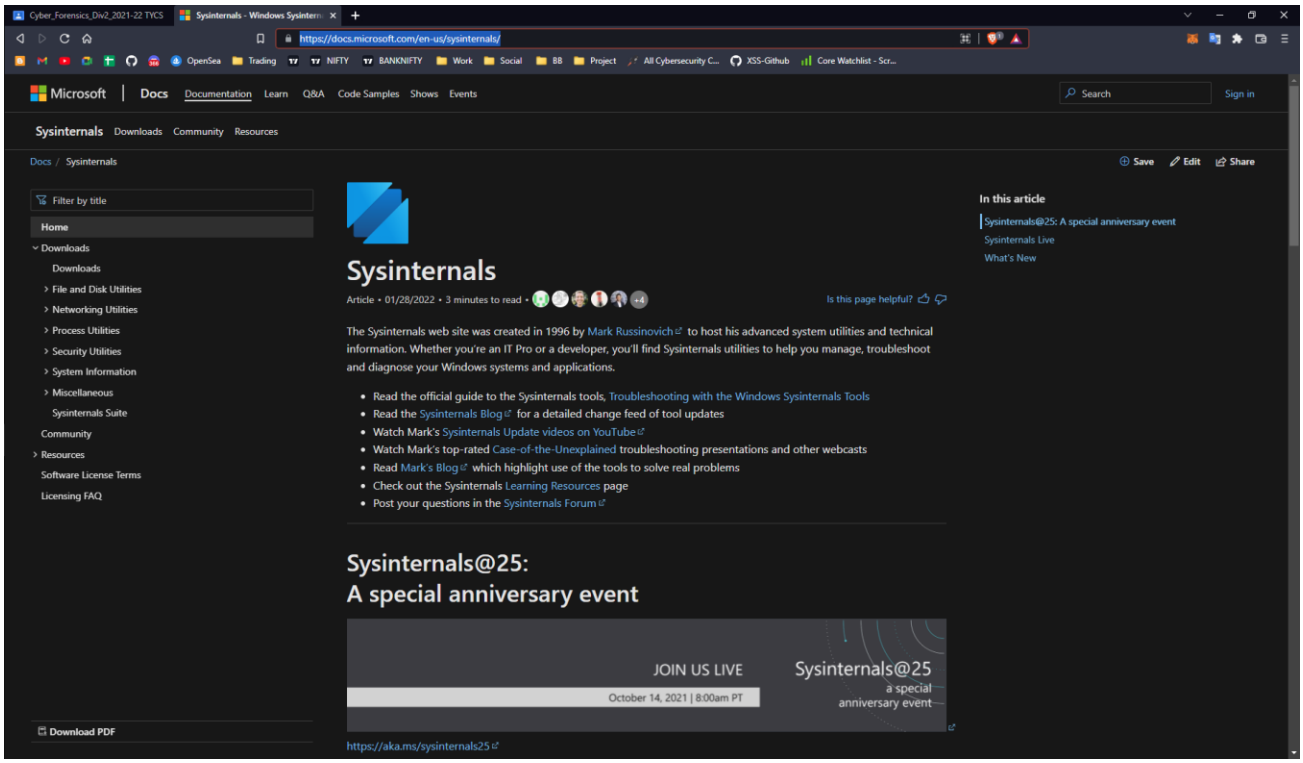
AIM : Using Sysinternals tools for Network Tracking and Process Monitoring

1. Check Sysinternals tools
2. Monitor Live Processes
3. Capture RAM
4. Capture TCP/UDP packets
5. Monitor Hard Disk
6. Monitor Virtual Memory
7. Monitor Cache Memory

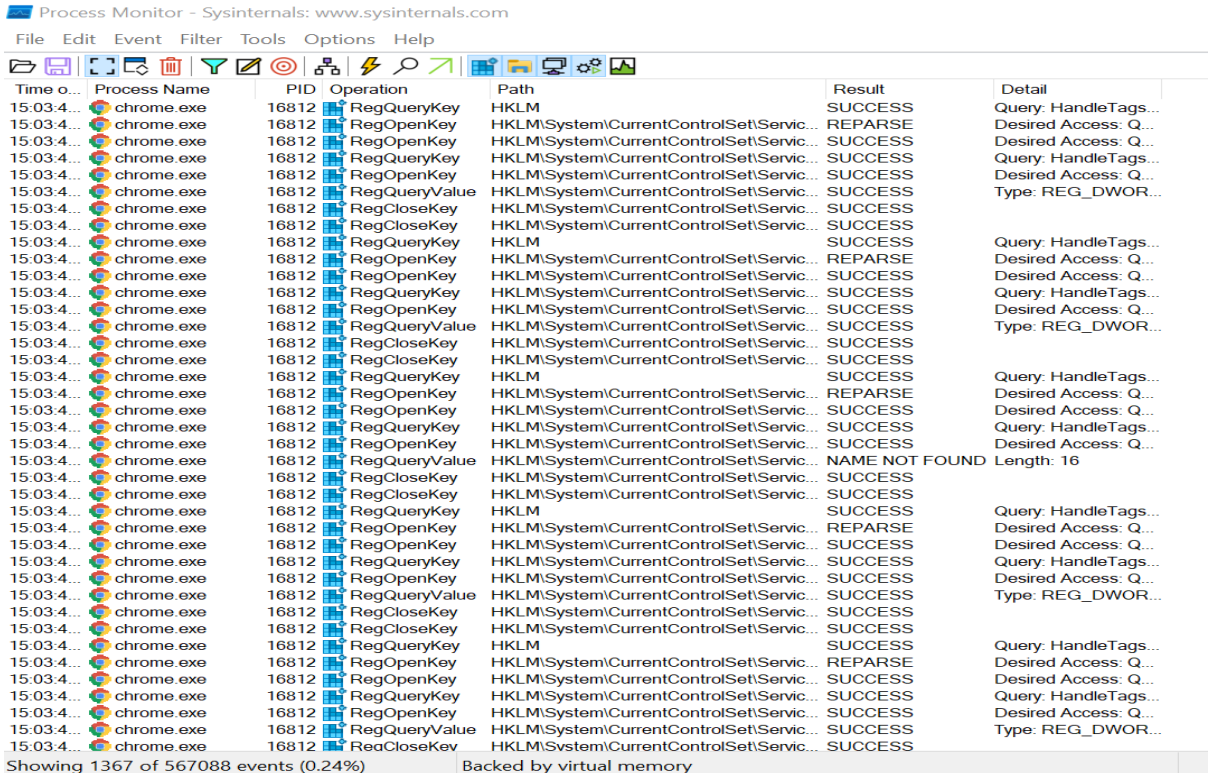
STEPS : follow the below steps –

1. Check Sysinternals tools

Visit https://docs.microsoft.com/en-us/sysinternals/ and download all the given tools as per requirement

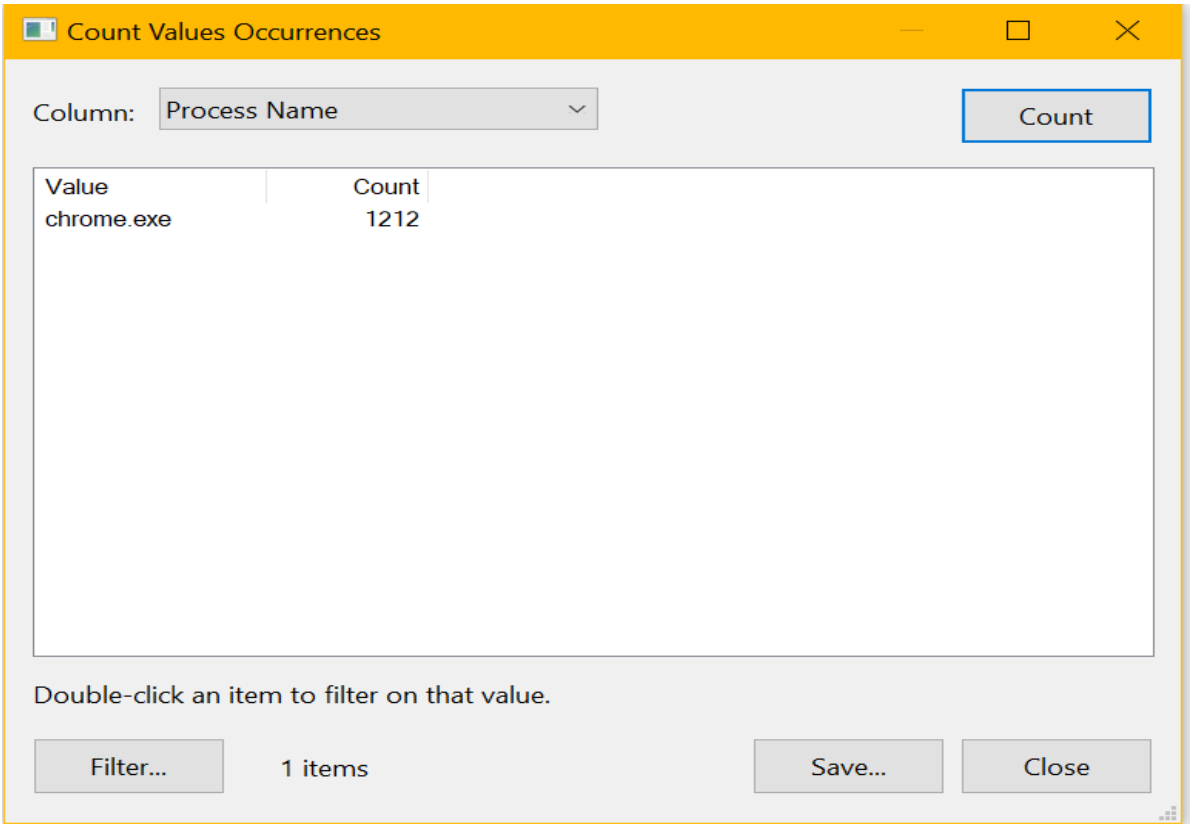


2. Monitor Live Process



Time o...	Process Name	PID	Operation	Path	Result	Detail
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	REPARSE	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryValue	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Type: REG_DWOR...
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	REPARSE	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryValue	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Type: REG_DWOR...
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	REPARSE	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryValue	HKLM\System\CurrentControlSet\Servic...	NAME NOT FOUND	Length: 16
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	REPARSE	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryValue	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Type: REG_DWOR...
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	REPARSE	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Query: HandleTags...
15:03:4...	chrome.exe	16812	RegOpenKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Desired Access: Q...
15:03:4...	chrome.exe	16812	RegQueryValue	HKLM\System\CurrentControlSet\Servic...	SUCCESS	Type: REG_DWOR...
15:03:4...	chrome.exe	16812	RegCloseKey	HKLM\System\CurrentControlSet\Servic...	SUCCESS	

Showing 1367 of 567088 events (0.24%)   Backed by virtual memory



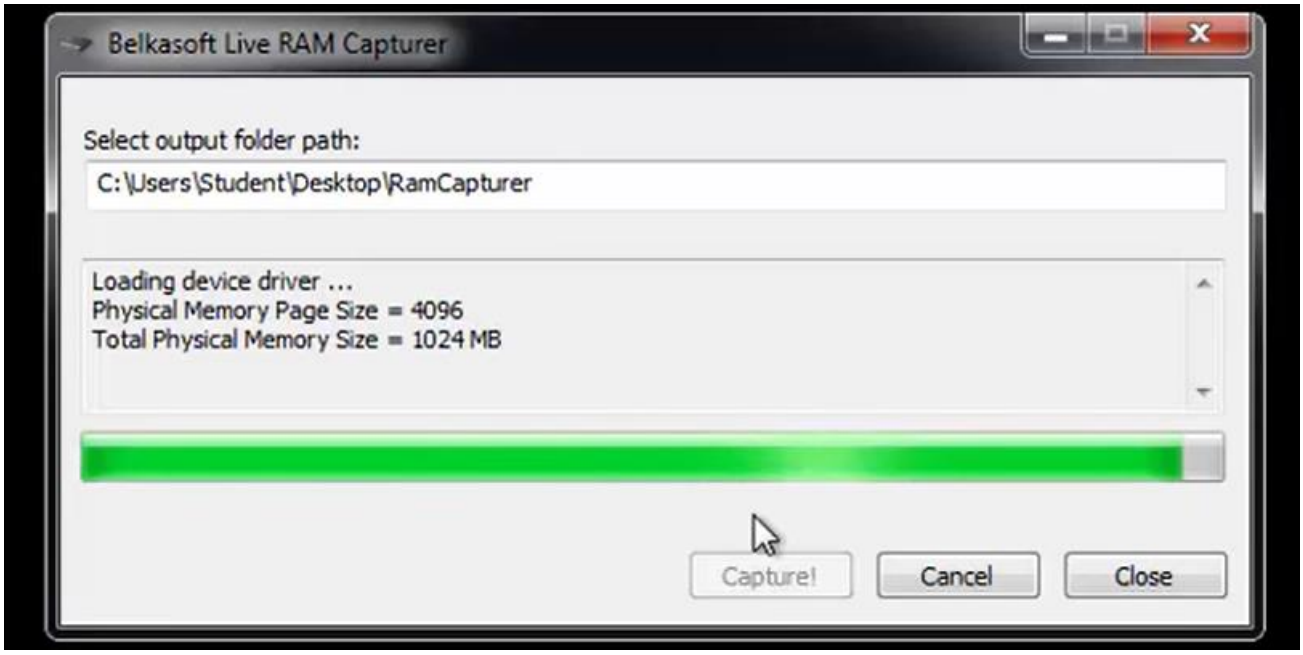
Column: Process Name

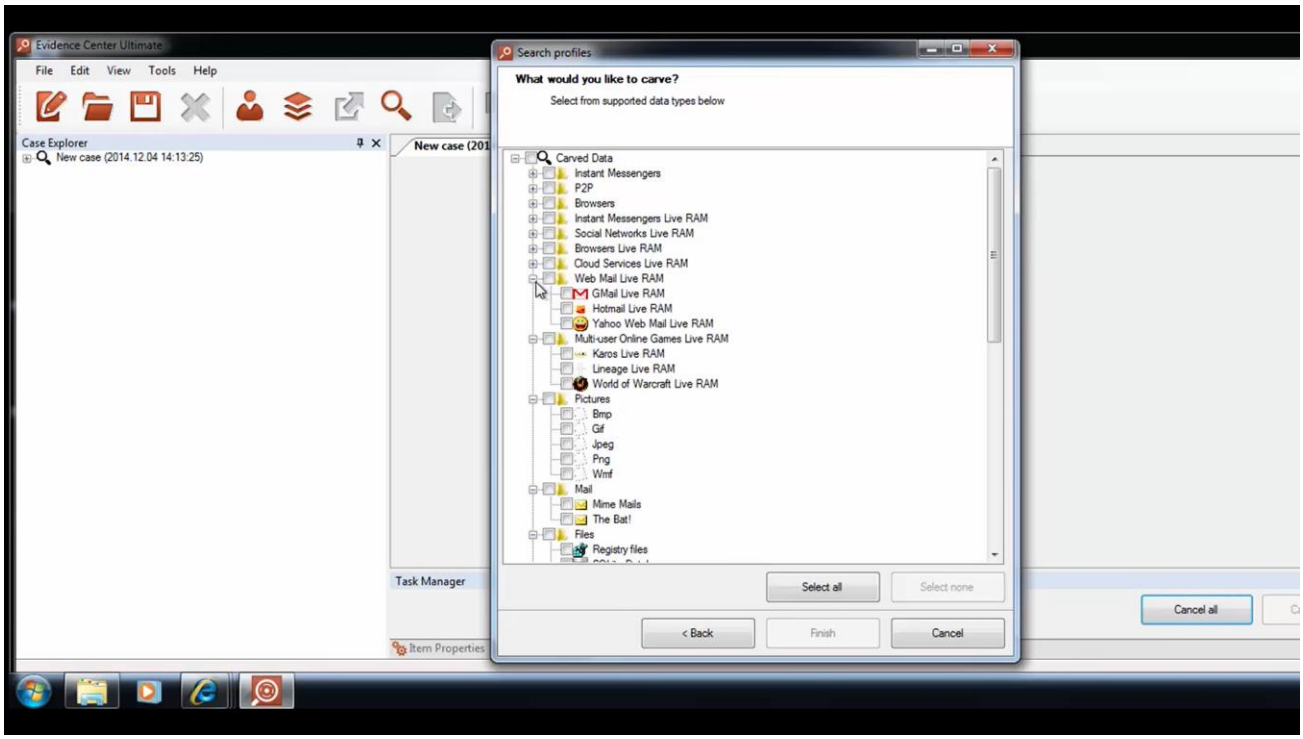
Value	Count
chrome.exe	1212

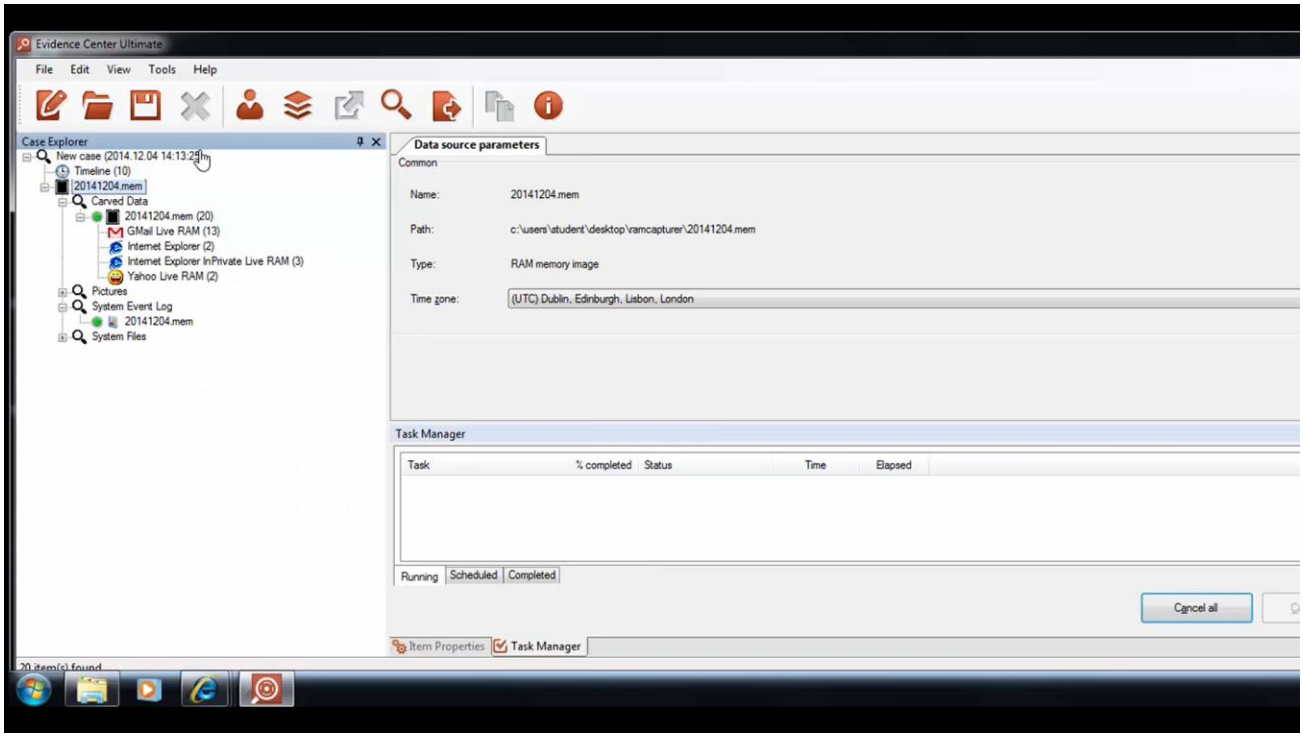
Double-click an item to filter on that value.

1 items

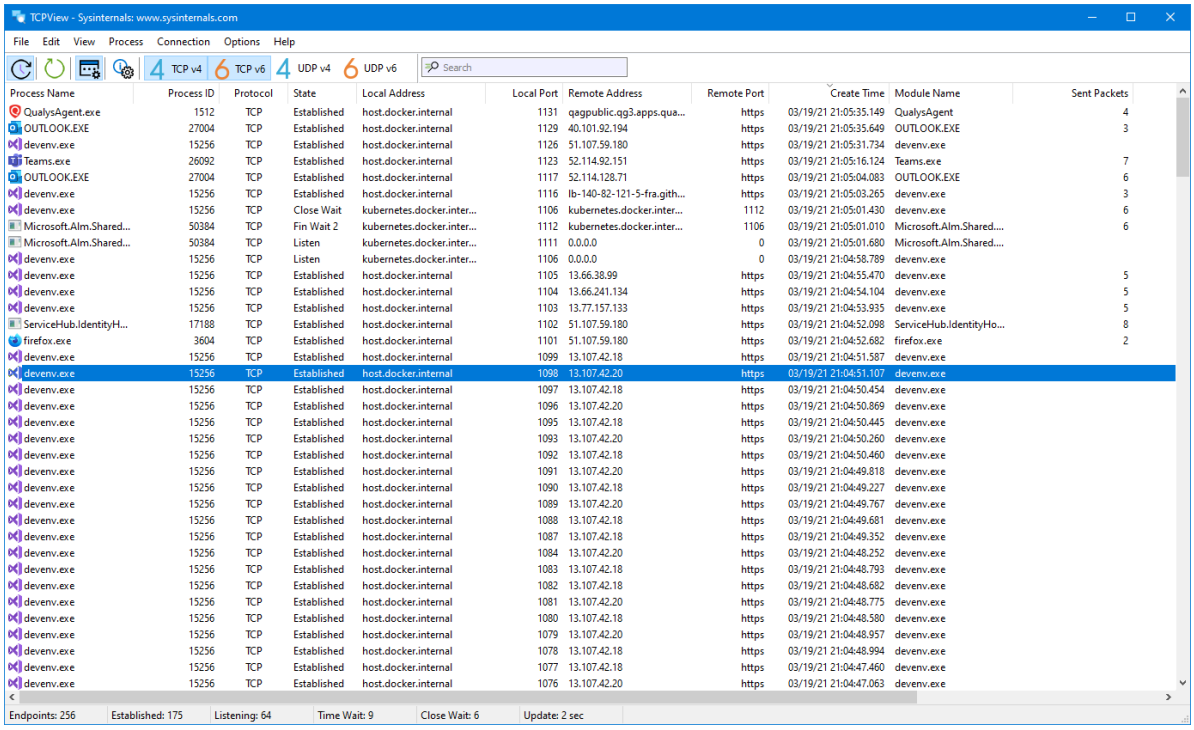
3. Capture Ram



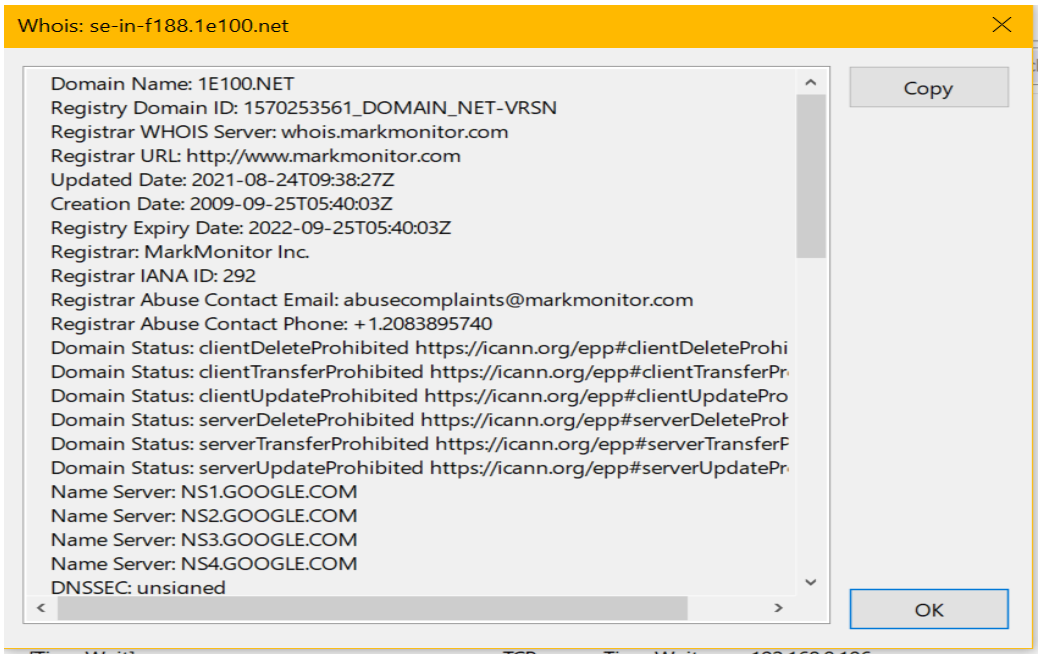




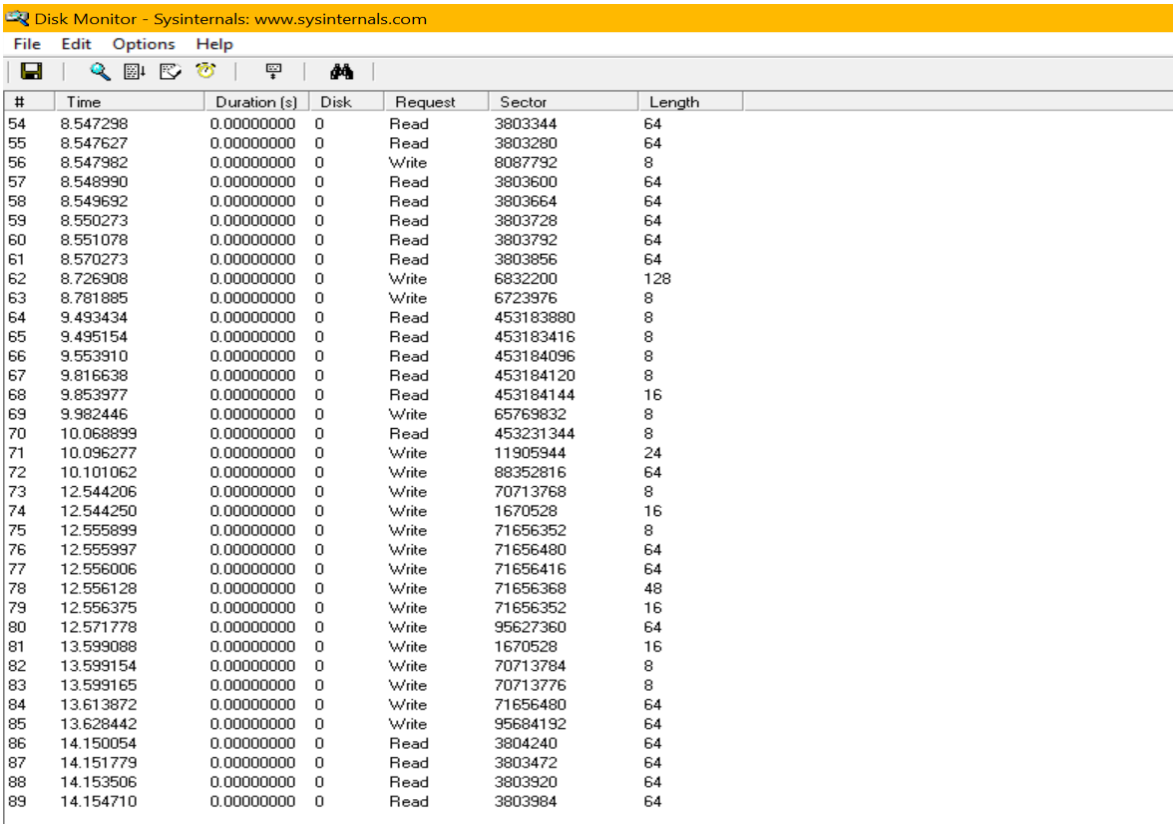
4. Capture TCP/UDP packets



Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
QualysAgent.exe	1512	TCP	Established	host.docker.internal	1131	qagpublic.qg3.apps.qua...	https	03/19/21 21:05:35.149	QualysAgent	4
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1129	40.101.92.194	https	03/19/21 21:05:35.649	OUTLOOK.EXE	3
devenv.exe	15256	TCP	Established	host.docker.internal	1126	51.107.59.180	https	03/19/21 21:05:31.734	devenv.exe	
Teams.exe	26092	TCP	Established	host.docker.internal	1123	52.114.92.151	https	03/19/21 21:05:16.124	Teams.exe	7
OUTLOOK.EXE	27004	TCP	Established	host.docker.internal	1117	52.114.128.71	https	03/19/21 21:05:04.083	OUTLOOK.EXE	6
devenv.exe	15256	TCP	Established	host.docker.internal	1116	lb-140-82-121-5-fra.gith...	https	03/19/21 21:05:03.265	devenv.exe	3
devenv.exe	15256	TCP	Close Wait	kubernetes.docker.inter...	1106	kubernetes.docker.inter...	1112	03/19/21 21:05:01.430	devenv.exe	6
Microsoft.Alm.Shared...	50384	TCP	Fin Wait 2	kubernetes.docker.inter...	1112	kubernetes.docker.inter...	1106	03/19/21 21:05:01.010	Microsoft.Alm.Shared....	6
Microsoft.Alm.Shared...	50384	TCP	Listen	kubernetes.docker.inter...	1111	0.0.0.0	0	03/19/21 21:05:01.680	Microsoft.Alm.Shared....	
devenv.exe	15256	TCP	Listen	kubernetes.docker.inter...	1106	0.0.0.0	0	03/19/21 21:04:58.789	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1105	13.66.38.99	https	03/19/21 21:04:55.470	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1104	13.66.241.134	https	03/19/21 21:04:54.104	devenv.exe	5
devenv.exe	15256	TCP	Established	host.docker.internal	1103	13.77.157.133	https	03/19/21 21:04:53.935	devenv.exe	5
ServiceHub.IdentityH...	17188	TCP	Established	host.docker.internal	1102	51.107.59.180	https	03/19/21 21:04:52.098	ServiceHub.IdentityHo...	8
firefox.exe	3604	TCP	Established	host.docker.internal	1101	51.107.59.180	https	03/19/21 21:04:52.682	firefox.exe	2
devenv.exe	15256	TCP	Established	host.docker.internal	1099	13.107.42.18	https	03/19/21 21:04:51.587	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1098	13.107.42.20	https	03/19/21 21:04:51.107	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1097	13.107.42.18	https	03/19/21 21:04:50.454	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1096	13.107.42.20	https	03/19/21 21:04:50.869	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1095	13.107.42.18	https	03/19/21 21:04:50.445	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1093	13.107.42.20	https	03/19/21 21:04:50.260	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1092	13.107.42.18	https	03/19/21 21:04:50.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1091	13.107.42.20	https	03/19/21 21:04:49.818	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1090	13.107.42.18	https	03/19/21 21:04:49.227	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1089	13.107.42.20	https	03/19/21 21:04:49.767	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1088	13.107.42.18	https	03/19/21 21:04:49.681	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1087	13.107.42.18	https	03/19/21 21:04:49.352	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1084	13.107.42.20	https	03/19/21 21:04:48.252	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1083	13.107.42.18	https	03/19/21 21:04:48.793	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1082	13.107.42.18	https	03/19/21 21:04:48.682	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1081	13.107.42.20	https	03/19/21 21:04:48.775	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1080	13.107.42.18	https	03/19/21 21:04:48.580	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1079	13.107.42.20	https	03/19/21 21:04:48.957	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1078	13.107.42.18	https	03/19/21 21:04:48.994	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1077	13.107.42.18	https	03/19/21 21:04:47.460	devenv.exe	
devenv.exe	15256	TCP	Established	host.docker.internal	1076	13.107.42.20	https	03/19/21 21:04:47.063	devenv.exe	

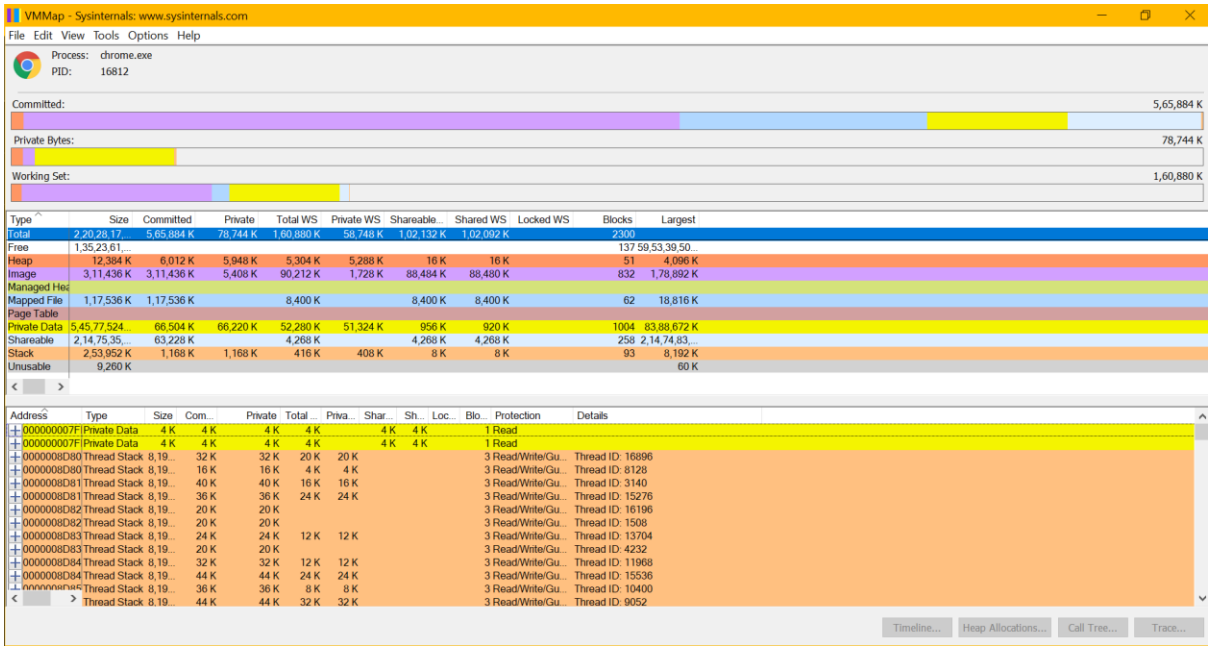


5. Monitor hard disk



#	Time	Duration (s)	Disk	Request	Sector	Length
54	8.547298	0.00000000	0	Read	3803344	64
55	8.547627	0.00000000	0	Read	3803280	64
56	8.547982	0.00000000	0	Write	8087792	8
57	8.548990	0.00000000	0	Read	3803600	64
58	8.549692	0.00000000	0	Read	3803664	64
59	8.550273	0.00000000	0	Read	3803728	64
60	8.551078	0.00000000	0	Read	3803792	64
61	8.570273	0.00000000	0	Read	3803856	64
62	8.726908	0.00000000	0	Write	6832200	128
63	8.781885	0.00000000	0	Write	6723976	8
64	9.493434	0.00000000	0	Read	453183880	8
65	9.495154	0.00000000	0	Read	453183416	8
66	9.553910	0.00000000	0	Read	453184096	8
67	9.816638	0.00000000	0	Read	453184120	8
68	9.853977	0.00000000	0	Read	453184144	16
69	9.982446	0.00000000	0	Write	65769832	8
70	10.068899	0.00000000	0	Read	453231344	8
71	10.096277	0.00000000	0	Write	11905944	24
72	10.101062	0.00000000	0	Write	88352816	64
73	12.544206	0.00000000	0	Write	70713768	8
74	12.544250	0.00000000	0	Write	1670528	16
75	12.555899	0.00000000	0	Write	71656352	8
76	12.555997	0.00000000	0	Write	71656480	64
77	12.556006	0.00000000	0	Write	71656416	64
78	12.556128	0.00000000	0	Write	71656368	48
79	12.556375	0.00000000	0	Write	71656352	16
80	12.571778	0.00000000	0	Write	95627360	64
81	13.599088	0.00000000	0	Write	1670528	16
82	13.599154	0.00000000	0	Write	70713784	8
83	13.599165	0.00000000	0	Write	70713776	8
84	13.613872	0.00000000	0	Write	71656480	64
85	13.628442	0.00000000	0	Write	95684192	64
86	14.150054	0.00000000	0	Read	3804240	64
87	14.151779	0.00000000	0	Read	3803472	64
88	14.153506	0.00000000	0	Read	3803920	64
89	14.154710	0.00000000	0	Read	3803984	64

6. Monitor virtual memory



7. Monitor cache memory