Expt. No.

Name : Piyush Pandurang Burate Class : TYCS Roll No.: 523

Title of Experiment : Using Sysinternals tools for network tracking and process monitoring

Date

Sub titles : Assignment/ Problem Solution, Flow chart/Algorithm, Problem Listing, Input Screen, Output Screen, Comments (If any)

Aim :- Using sysinternals tools for network tracking and process monitoring.

- Check sysinternals tools
- Monitor live process
- Capture RAM
- Capture TCP/UDP packets
- Monitor Harddisk
- Monitor virtual memory
- Monitor cache memory

Theory :-

① Diskmon :-

Diskmon is an application that logs and displays all hard disk activity on a windows system. You can also minimize diskmon to your system. They where it act as a disk read activity and a red can when there is disk write activity.

Installing Diskmon is an easy as unzipping it and typing ,"diskmon". The means and toolbox buttons can be used to disable event capturing control the scrolling of the listview and to save the list view contents to an ASCII Files.

To have Diskmon Function as a disk light in your system tray select the optional minimize

Remark

Signature

to tray menu item. start Diskmon with a "11" command line switch. To reactive the diskmon window double click on the diskmon in the tray create a shortcut in your program File startup Folder.

② Process Monitor :-

Process monitor is an advanced monitoring tool for windows that shown real time File system registry and process/thread activity. It combines the features of two legacy sysinternal utilities.

Process monitor include powerful monitoring and Filtering capabilities, includes

- More data captured for operation input and output parameters.
- Non distructive Filter allows you to set Filters without losing data.
- Configurable and modual columns for any event properly.

③ RAM capture :-

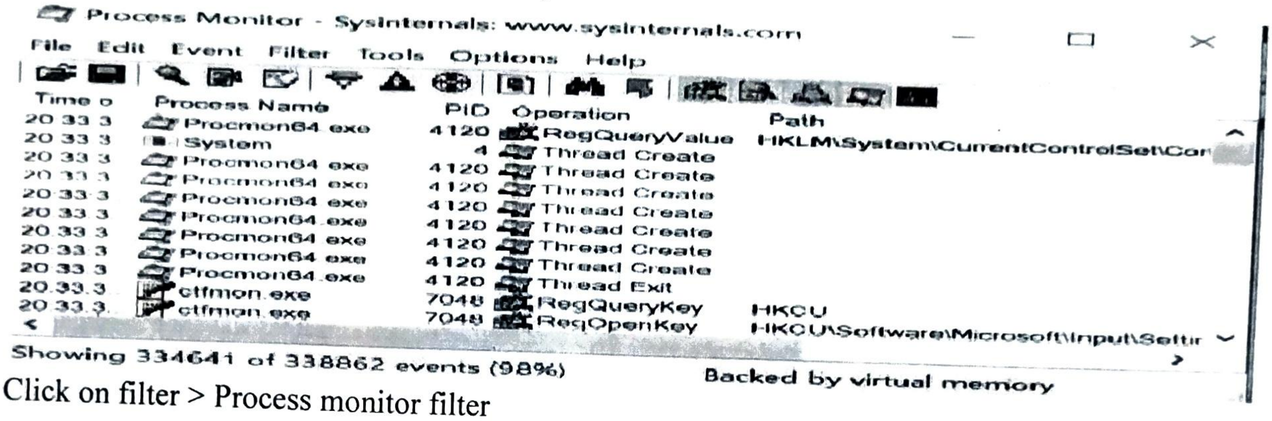
Digital Forensics experts understand the importance of remembering to perform a RAM capture on-sence so as to not leave valuable data in a computer memory dump enable Investigations and examiners to do a full memory analysis and access data including

- Browsing history
- Encryption keys
- Chat message
- Clipboard contents.

Practical 5: Using Sysinternals tools for Network Tracking and Process Monitoring:

Steps:

1) Check Sysinternals tools
2) Monitor Live Processes (Tool: ProcMon)

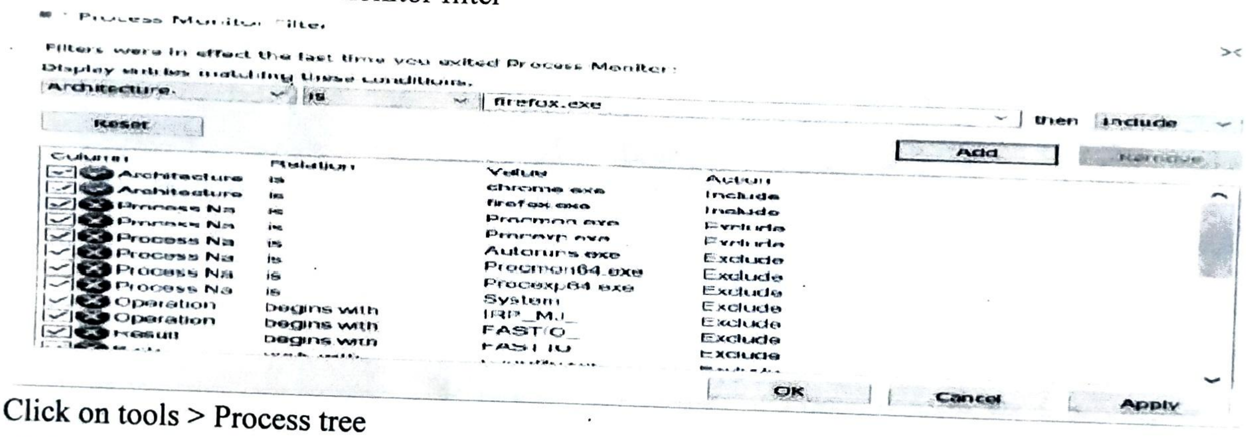


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time o	Process Name	PID	Operation	Path
20 33 3	Procmon64.exe	4120	RegQueryValue	HKLM\System\CurrentControlSet\Cor
20 33 3	System	4	Thread Create	
20 33 3	Procmon64.exe	4120	Thread Create	
20 33 3	Procmon64.exe	4120	Thread Create	
20 33 3	Procmon64.exe	4120	Thread Create	
20 33 3	Procmon64.exe	4120	Thread Create	
20 33 3	Procmon64.exe	4120	Thread Create	
20 33 3	Procmon64.exe	4120	Thread Create	
20 33 3	Procmon64.exe	4120	Thread Create	
20 33 3	ctfmon.exe	4120	Thread Exit	
20 33 3	ctfmon.exe	7048	RegQueryKey	HKCU
		7048	RegOpenKey	HKCU\Software\Microsoft\Input\Settir

Showing 334641 of 338862 events (98%) Backed by virtual memory

Click on filter > Process monitor filter

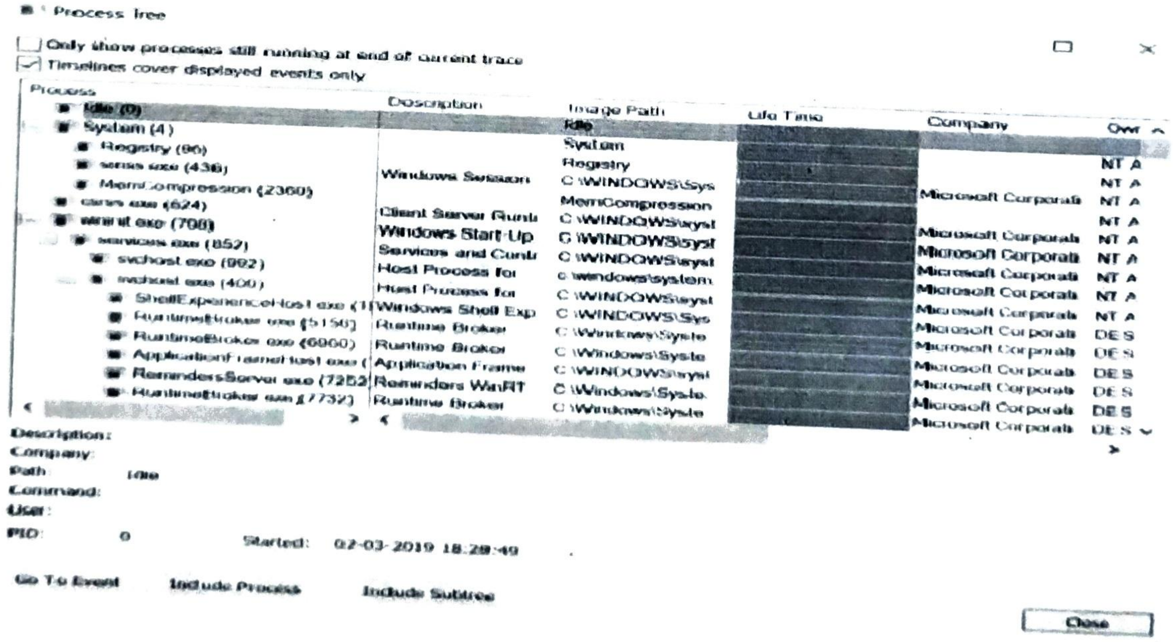


Filters were in effect the last time you exited Process Monitor:
Display entries matching these conditions:

Architecture. | is | firefox.exe | then Include

Column	Relation	Value	Action
☑ Architecture	is	chrome.exe	Include
☑ Architecture	is	firefox.exe	Include
☑ Process Na	is	Procmon.exe	Exclude
☑ Process Na	is	Procexp.exe	Exclude
☑ Process Na	is	Autoruns.exe	Exclude
☑ Process Na	is	Procmon64.exe	Exclude
☑ Process Na	is	Procexp64.exe	Exclude
☑ Process Na	is	System	Exclude
☑ Operation	begins with	IRP_MJ_	Exclude
☑ Operation	begins with	FAST IO_	Exclude
☑ Result	begins with	FAST IO	Exclude

Click on tools > Process tree

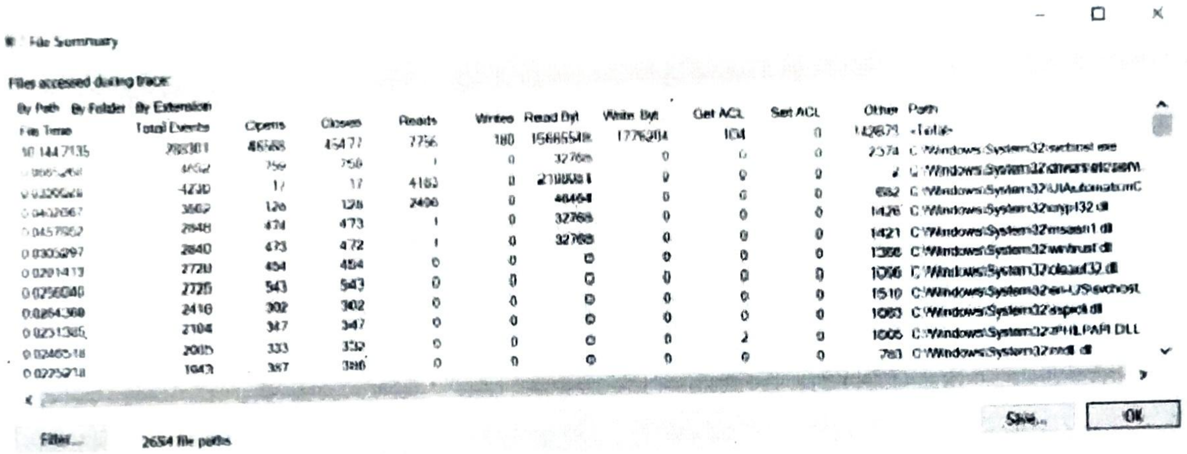


□ Only show processes still running at end of current trace
☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owr
Idle (0)		Idle			
System (4)		System			NT A
Registry (96)		Registry			NT A
smss.exe (436)	Windows Session	C:\WINDOWS\Sys			NT A
MemCompression (2360)		MemCompression		Microsoft Corporati	NT A
csrss.exe (624)	Client Server Runti	C:\WINDOWS\syst		Microsoft Corporati	NT A
wininit.exe (708)	Windows Start-Up	C:\WINDOWS\syst		Microsoft Corporati	NT A
services.exe (852)	Services and Contr	C:\WINDOWS\syst		Microsoft Corporati	NT A
svchost.exe (992)	Host Process for	c:\windows\system		Microsoft Corporati	NT A
svchost.exe (400)	Host Process for	C:\WINDOWS\syst		Microsoft Corporati	NT A
ShellExperienceHost.exe (1	Windows Shell Exp	C:\WINDOWS\Sys		Microsoft Corporati	DE S
RuntimeBroker.exe (5156)	Runtime Broker	C:\Windows\Syste		Microsoft Corporati	DE S
RuntimeBroker.exe (6960)	Runtime Broker	C:\Windows\Syste		Microsoft Corporati	DE S
ApplicationFrameHost.exe (	Application Frame	C:\WINDOWS\syst		Microsoft Corporati	DE S
RemindersServer.exe (7252	Reminders WinRT	C:\Windows\Syste		Microsoft Corporati	DE S
RuntimeBroker.exe (7732)	Runtime Broker	C:\Windows\Syste		Microsoft Corporati	DE S

Description:
Company:
Path: Idle
Command:
User:
PID: 0 Started: 02-03-2019 18:28:49

Click on filter > File summary



File Summary

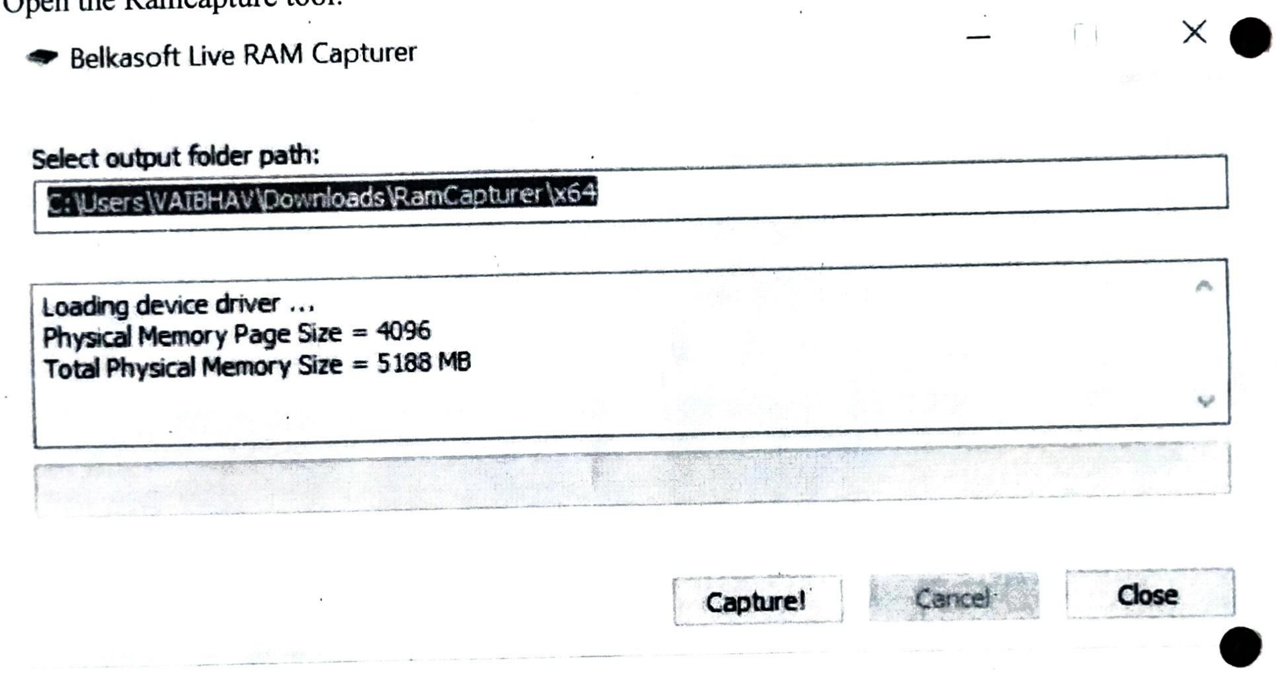
Files accessed during trace:

File Time	Total Events	Opens	Closes	Reads	Writes	Read Byt	Write Byt	Get ACL	Set ACL	Other	Path
10.1447135	788301	46588	45477	7756	180	156665418	1776204	104	0	142679	<Total>
[illegible]	4652	759	758	1	0	32768	0	0	0	2574	C:\Windows\System32\svchost.exe
0.03205628	4230	17	17	4163	0	2108881	0	0	0	2	C:\Windows\System32\drivers\etc\[illegible]
0.04020667	3662	126	128	2400	0	40464	0	0	0	682	C:\Windows\System32\UIAutomationC
0.0457952	2848	474	473	1	0	32768	0	0	0	1426	C:\Windows\System32\crypt32.dll
0.0305297	2840	473	472	1	0	32768	0	0	0	1421	C:\Windows\System32\msasn1.dll
0.0291413	2720	454	454	0	0	0	0	0	0	1366	C:\Windows\System32\wintrust.dll
0.0256040	2725	543	543	0	0	0	0	0	0	1066	C:\Windows\System32\oleaut32.dll
0.0264360	2416	302	302	0	0	0	0	0	0	1510	C:\Windows\System32\en-US\svchost
0.0251385	2104	347	347	0	0	0	0	0	0	1060	C:\Windows\System32\sspicli.dll
0.0246518	2005	333	332	0	0	0	0	2	0	1005	C:\Windows\System32\IPHLPAPI.DLL
0.0275218	1943	387	386	0	0	0	0	0	0	780	C:\Windows\System32\ntdll.dll

2654 file paths

3) Capture RAM (Tool: RAMCapture)

Open the Ramcapture tool.



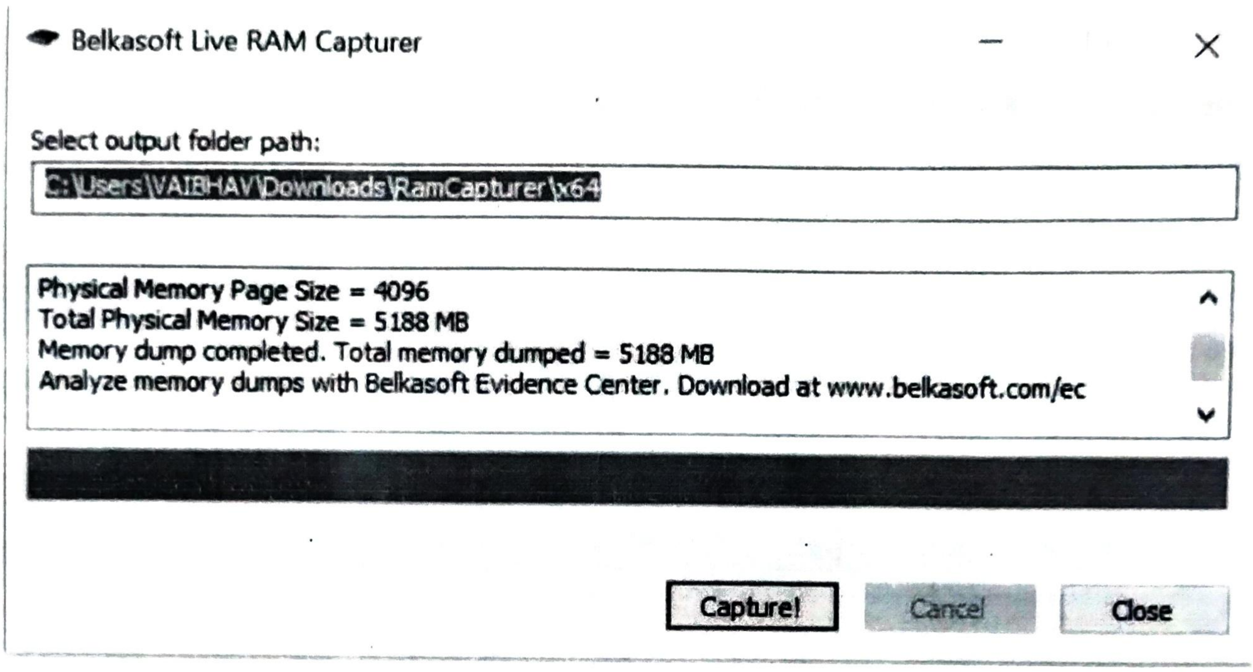
Belkasoft Live RAM Capturer

Select output folder path:

C:\Users\VAIBHAV\Downloads\RamCapturer\x64

```
Loading device driver ...
Physical Memory Page Size = 4096
Total Physical Memory Size = 5188 MB
```

Click on capture.



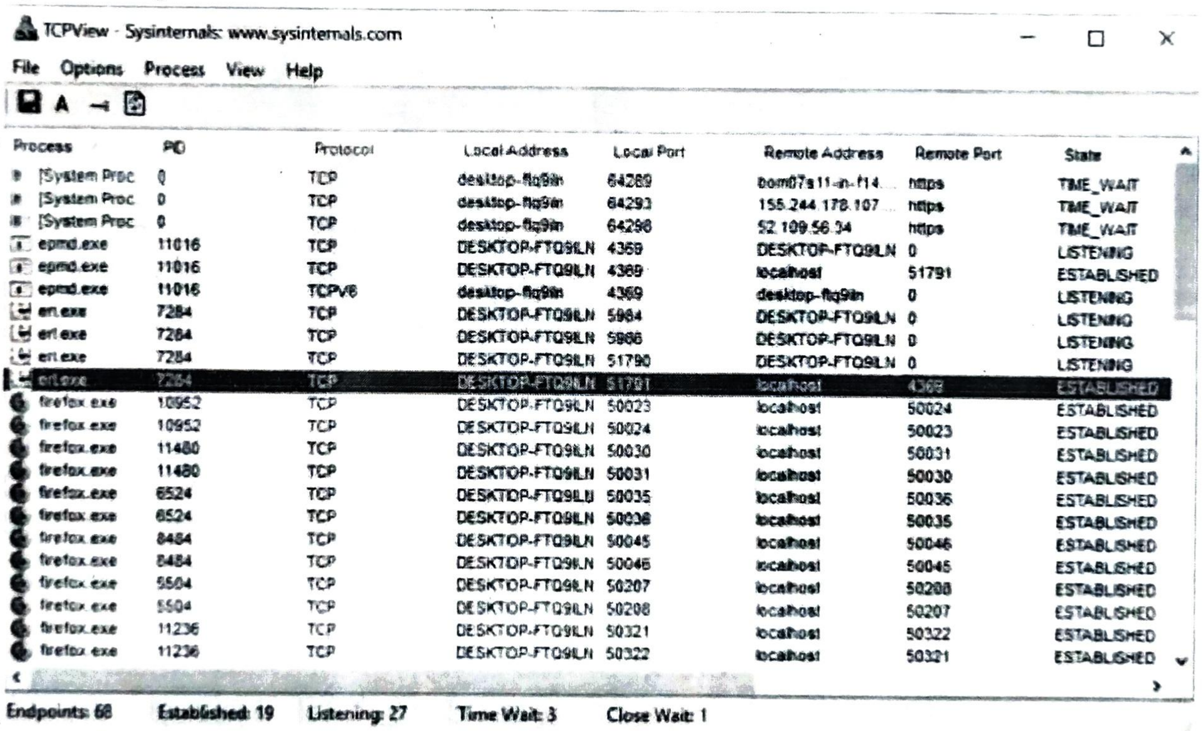
Select output folder path:

C:\Users\VAIBHAV\Downloads\RamCapturer\x64

```
Physical Memory Page Size = 4096
Total Physical Memory Size = 5188 MB
Memory dump completed. Total memory dumped = 5188 MB
Analyze memory dumps with Belkasoft Evidence Center. Download at www.belkasoft.com/ec
```

4) Capture TCP/UDP packets (Tool: TcpView)

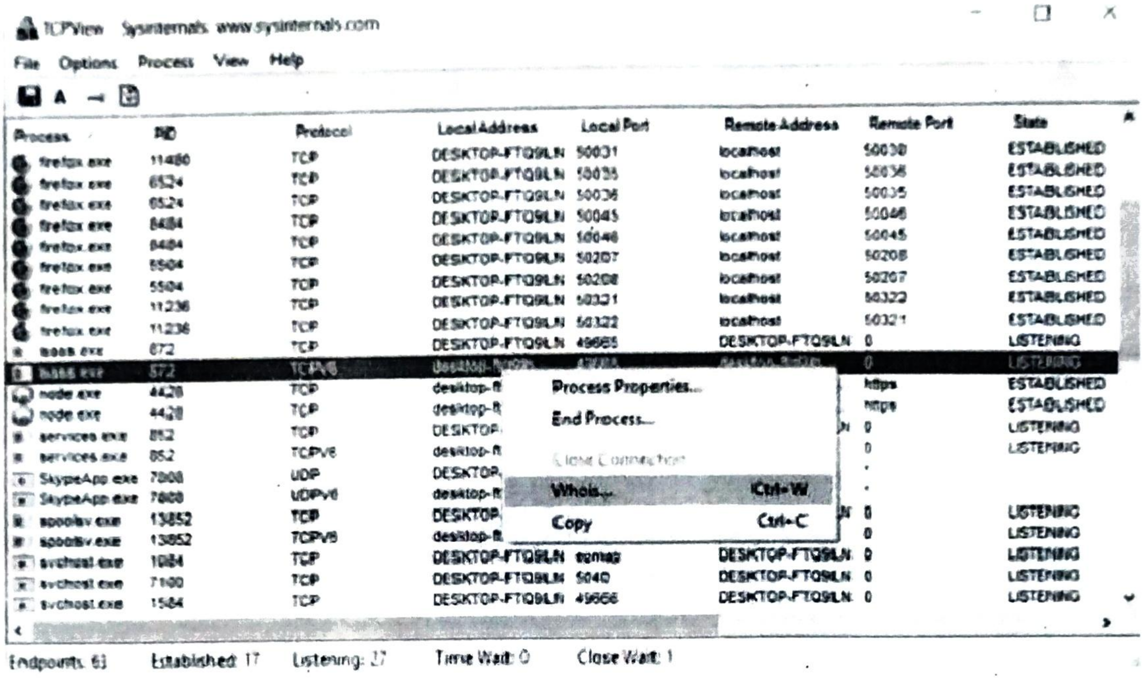
Open the Tcpview tool.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc	0	TCP	desktop-flq9in	64289	bom07s11-in-f14...	https	TIME_WAIT
[System Proc	0	TCP	desktop-flq9in	64293	155.244.178.107...	https	TIME_WAIT
[System Proc	0	TCP	desktop-flq9in	64298	52.109.56.34	https	TIME_WAIT
epmd.exe	11016	TCP	DESKTOP-FTQ9LN	4369	DESKTOP-FTQ9LN	0	LISTENING
epmd.exe	11016	TCP	DESKTOP-FTQ9LN	4369	localhost	51791	ESTABLISHED
epmd.exe	11016	TCPV6	desktop-flq9in	4369	desktop-flq9in	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9LN	5984	DESKTOP-FTQ9LN	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9LN	5986	DESKTOP-FTQ9LN	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9LN	51790	DESKTOP-FTQ9LN	0	LISTENING
erl.exe	7284	TCP	DESKTOP-FTQ9LN	51791	localhost	4369	ESTABLISHED
firefox.exe	10952	TCP	DESKTOP-FTQ9LN	50023	localhost	50024	ESTABLISHED
firefox.exe	10952	TCP	DESKTOP-FTQ9LN	50024	localhost	50023	ESTABLISHED
firefox.exe	11480	TCP	DESKTOP-FTQ9LN	50030	localhost	50031	ESTABLISHED
firefox.exe	11480	TCP	DESKTOP-FTQ9LN	50031	localhost	50030	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9LN	50035	localhost	50036	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9LN	50036	localhost	50035	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9LN	50045	localhost	50046	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9LN	50046	localhost	50045	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9LN	50207	localhost	50208	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9LN	50208	localhost	50207	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9LN	50321	localhost	50322	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9LN	50322	localhost	50321	ESTABLISHED

Endpoints: 68   Established: 19   Listening: 27   Time Wait: 3   Close Wait: 1

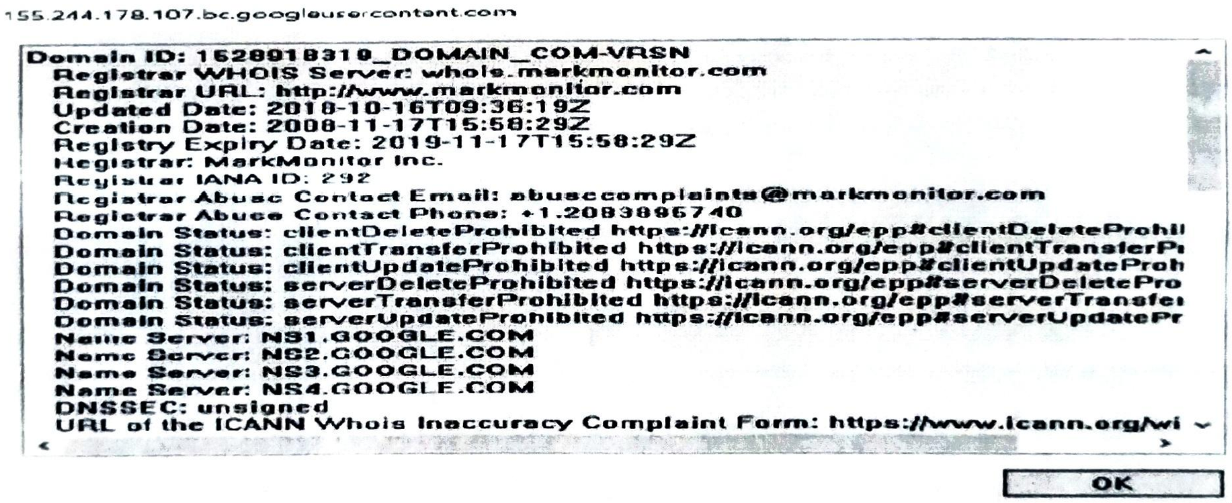
Right click on any packet > whois



TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
firefox.exe	11480	TCP	DESKTOP-FTQ9LN	50031	localhost	50030	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9LN	50035	localhost	50036	ESTABLISHED
firefox.exe	6524	TCP	DESKTOP-FTQ9LN	50036	localhost	50035	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9LN	50045	localhost	50046	ESTABLISHED
firefox.exe	8484	TCP	DESKTOP-FTQ9LN	50046	localhost	50045	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9LN	50207	localhost	50208	ESTABLISHED
firefox.exe	5504	TCP	DESKTOP-FTQ9LN	50208	localhost	50207	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9LN	50321	localhost	50322	ESTABLISHED
firefox.exe	11236	TCP	DESKTOP-FTQ9LN	50322	localhost	50321	ESTABLISHED
lsass.exe	672	TCP	DESKTOP-FTQ9LN	49665	DESKTOP-FTQ9LN	0	LISTENING
lsass.exe	672	TCPV6	desktop-ftq9ln	49665	desktop-ftq9ln	0	LISTENING
node.exe	4428	TCP	desktop-ft			https	ESTABLISHED
node.exe	4428	TCP	desktop-ft			https	ESTABLISHED
services.exe	852	TCP	DESKTOP-			0	LISTENING
services.exe	852	TCPV6	desktop-ft			0	LISTENING
SkypeApp.exe	7808	UDP	DESKTOP-			*	
SkypeApp.exe	7808	UDPV6	desktop-ft			*	
spoolsv.exe	13852	TCP	DESKTOP-			0	LISTENING
spoolsv.exe	13852	TCPV6	desktop-ft			0	LISTENING
svchost.exe	1084	TCP	DESKTOP-FTQ9LN	epmap	DESKTOP-FTQ9LN	0	LISTENING
svchost.exe	7100	TCP	DESKTOP-FTQ9LN	5040	DESKTOP-FTQ9LN	0	LISTENING
svchost.exe	1584	TCP	DESKTOP-FTQ9LN	49666	DESKTOP-FTQ9LN	0	LISTENING

Endpoints: 61 Established: 17 Listening: 27 Time Wait: 0 Close Wait: 1

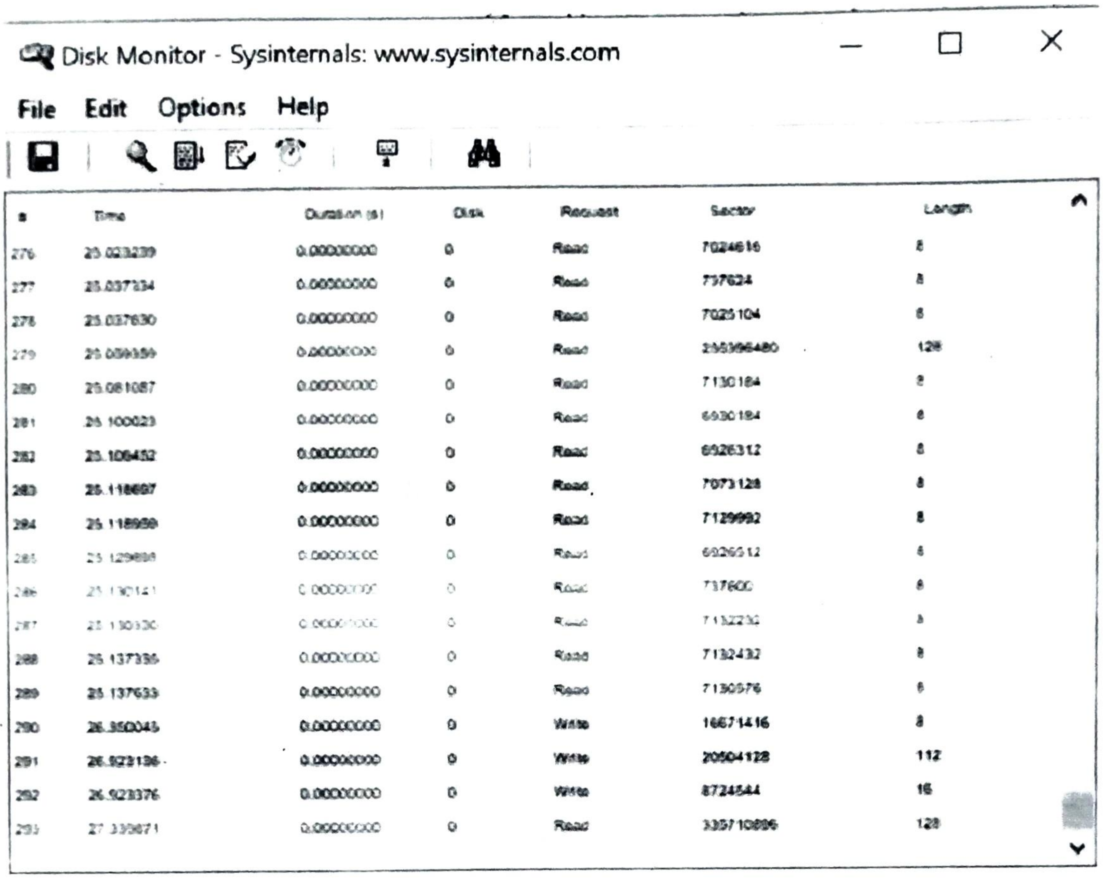


155.244.178.107.bc.googleusercontent.com

```
Domain ID: 1528918319_DOMAIN_COM-VRSN
  Registrar WHOIS Server: whois.markmonitor.com
  Registrar URL: http://www.markmonitor.com
  Updated Date: 2018-10-16T09:36:19Z
  Creation Date: 2008-11-17T15:58:29Z
  Registry Expiry Date: 2019-11-17T15:58:29Z
  Registrar: MarkMonitor Inc.
  Registrar IANA ID: 292
  Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
  Registrar Abuse Contact Phone: +1.2083896740
  Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhil
  Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferPr
  Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProh
  Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeletePro
  Domain Status: serverTransferProhibited https://icann.org/epp#serverTransfer
  Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdatePr
  Name Server: NS1.GOOGLE.COM
  Name Server: NS2.GOOGLE.COM
  Name Server: NS3.GOOGLE.COM
  Name Server: NS4.GOOGLE.COM
  DNSSEC: unsigned
  URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
```

5) Monitor Hard Disk (Tool: DiskMon)

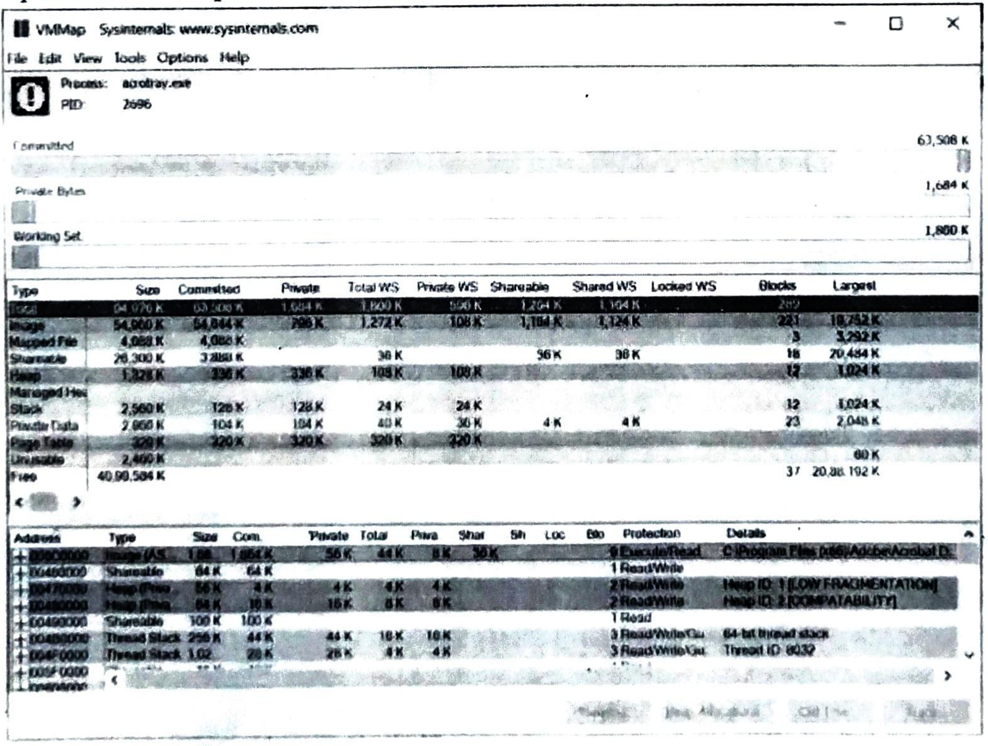
Open the Diskmon tool.



#	Time	Duration (s)	Disk	Request	Sector	Length
276	25.023239	0.00000000	0	Read	7024616	8
277	25.037334	0.00000000	0	Read	737624	8
278	25.037630	0.00000000	0	Read	7025104	8
279	25.059359	0.00000000	0	Read	255396480	128
280	25.081087	0.00000000	0	Read	7130184	8
281	25.100023	0.00000000	0	Read	6930184	8
282	25.106452	0.00000000	0	Read	6926312	8
283	25.118697	0.00000000	0	Read	7073128	8
284	25.118998	0.00000000	0	Read	7129992	8
285	25.129898	0.00000000	0	Read	6926512	8
286	25.130141	0.00000000	0	Read	737600	8
287	25.130330	0.00000000	0	Read	7132232	8
288	25.137336	0.00000000	0	Read	7132432	8
289	25.137633	0.00000000	0	Read	7130576	8
290	26.350045	0.00000000	0	Write	16671416	8
291	26.923136	0.00000000	0	Write	20504128	112
292	26.923376	0.00000000	0	Write	8724544	16
293	27.339871	0.00000000	0	Read	3357108896	128

6) Monitor Virtual Memory (Tool: VMMap)

Open the VMMap tool.



Process: acrotray.exe
PID: 2696

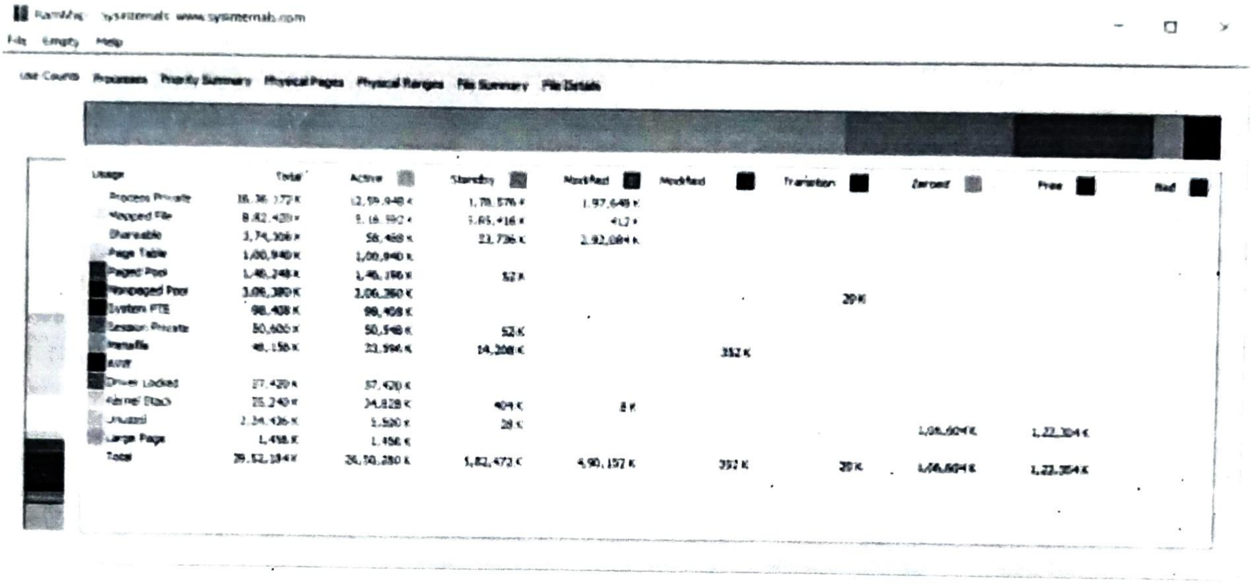
Committed 63,508 K
Private Bytes 1,684 K
Working Set 1,800 K

Type	Size	Committed	Private	Total WS	Private WS	Shareable	Shared WS	Locked WS	Blocks	Largest
Total	64,976 K	63,508 K	1,684 K	1,800 K	596 K	1,204 K	1,104 K		289	
Image	54,900 K	54,844 K	296 K	1,272 K	108 K	1,164 K	1,124 K		221	18,752 K
Mapped File	4,088 K	4,088 K							3	3,292 K
Shareable	26,300 K	3,888 K		36 K		36 K	36 K		18	20,484 K
Heap	1,328 K	336 K	336 K	108 K	108 K				12	1,024 K
Managed Hea										
Stack	2,560 K	128 K	128 K	24 K	24 K				12	1,024 K
Private Data	2,060 K	104 K	104 K	40 K	36 K	4 K	4 K		23	2,048 K
Page Table	320 K	320 K	320 K	320 K	320 K					
Unusable	2,460 K									60 K
Free	40,90,584 K								37	20,88,192 K

Address	Type	Size	Com.	Private	Total	Priva	Shar	Sh	Loc	Blo	Protection	Details
+ 00300000	Image (AS	1,88	1,864 K	56 K	44 K	8 K	36 K			9	Execute/Read	C:\Program Files (x86)\Adobe\Acrobat D
+ 00460000	Shareable	64 K	64 K							1	Read/Write	
+ 00470000	Heap (Priva	56 K	4 K	4 K	4 K	4 K				2	Read/Write	Heap ID: 1 [LOW FRAGMENTATION]
+ 00480000	Heap (Priva	64 K	16 K	16 K	8 K	8 K				2	Read/Write	Heap ID: 2 [COMPATABILITY]
+ 00490000	Shareable	100 K	100 K							1	Read	
+ 004B0000	Thread Stack	256 K	44 K	44 K	16 K	16 K				3	Read/Write/Gu	64-bit thread stack
+ 004F0000	Thread Stack	1,02	28 K	28 K	4 K	4 K				3	Read/Write/Gu	Thread ID: 8032
+ 005F0000												

7) Monitor Cache Memory (Tool: RAMMap)

Open the RAMMap tool.



RAMMap - Sysinternals: www.sysinternals.com
File Empty Help
Use Counts Processes Priority Summary Physical Pages Physical Ranges File Summary File Details

Usage	Total	Active	Standby	Modified	Modified	Transition	Zeroed	Free	Bad
Process Private	16,36,172 K	12,59,948 K	1,78,576 K	1,97,648 K					
Mapped File	8,82,420 K	5,16,592 K	3,65,416 K	412 K					
Shareable	3,74,308 K	58,488 K	23,736 K	2,92,084 K					
Page Table	1,00,940 K	1,00,940 K							
Paged Pool	1,46,248 K	1,46,196 K	52 K						
Nonpaged Pool	3,06,380 K	3,06,360 K				20 K			
System PTE	98,408 K	98,408 K							
Session Private	50,600 K	50,548 K	52 K						
Metafile	48,156 K	33,596 K	14,208 K		352 K				
AWE									
Driver Locked	37,420 K	37,420 K							
Kernel Stack	35,240 K	34,828 K	404 K	8 K					
Unused	2,34,436 K	5,500 K	28 K				1,06,604 K	1,22,304 K	
Large Page	1,456 K	1,456 K							
Total	39,52,184 K	26,50,280 K	5,82,472 K	4,90,152 K	352 K	20 K	1,06,604 K	1,22,304 K	