

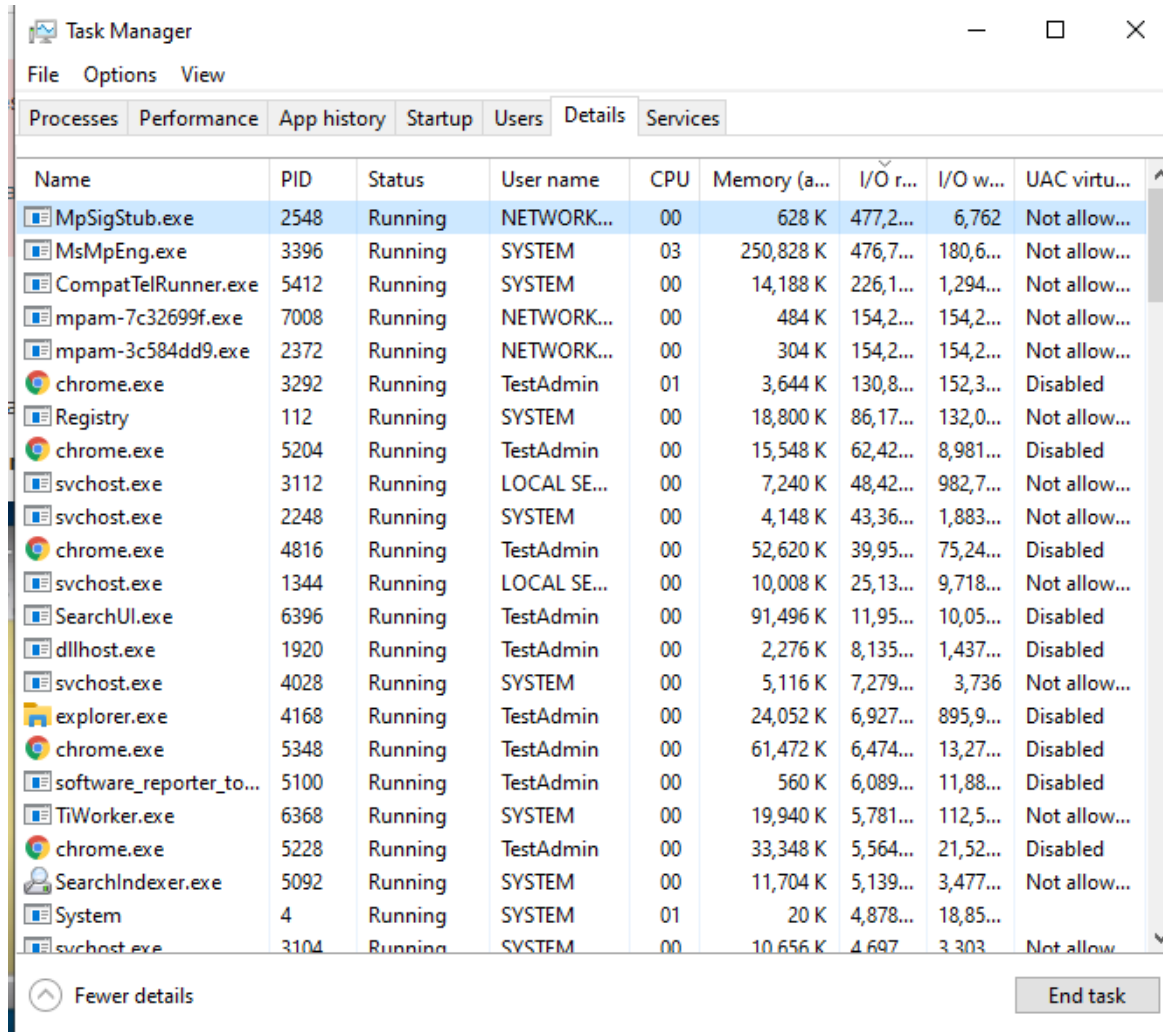
EP-Lab07-2021

Olaru Gabriel Iulian, 342C2



EX1:

The resource consumption is justified since MgSigStub.exe is a service for a malware detection tool from Windows. Probably it accesses memory lots more frequently since it scans for malware.



Task Manager

File Options View

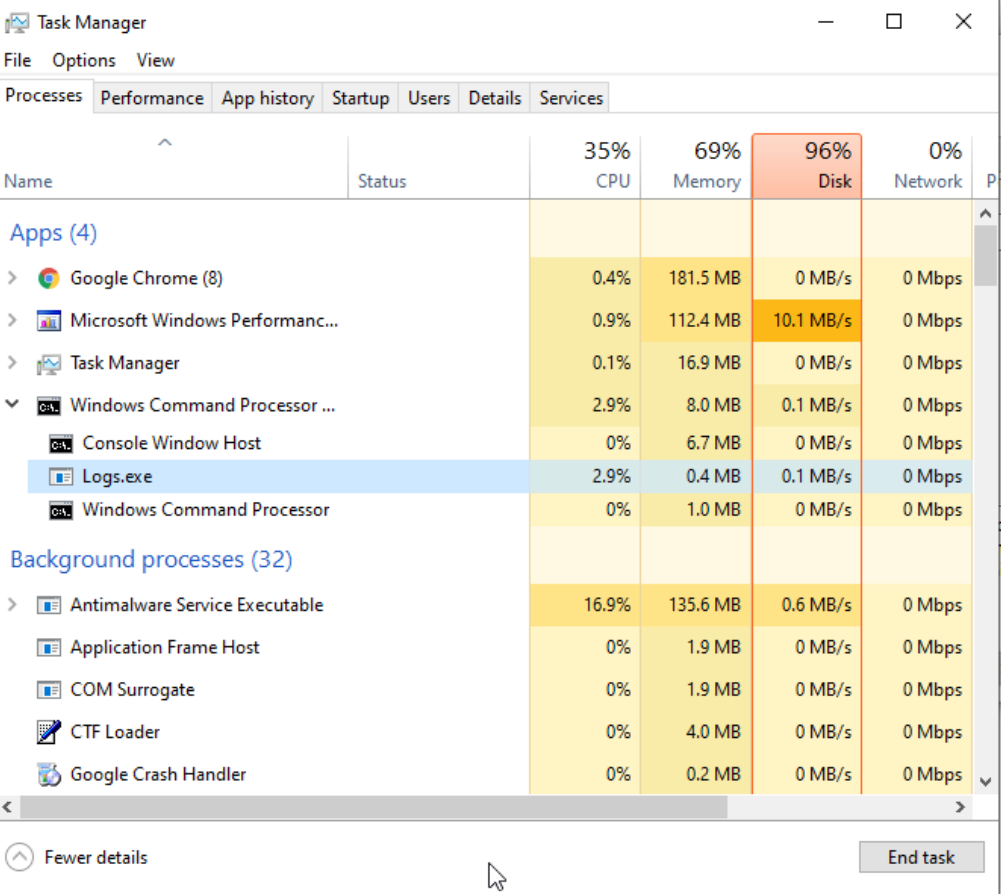
Processes Performance App history Startup Users Details Services

Name	PID	Status	User name	CPU	Memory (a...	I/O r...	I/O w...	UAC virtu...
MpSigStub.exe	2548	Running	NETWORK...	00	628 K	477,2...	6,762	Not allow...
MsMpEng.exe	3396	Running	SYSTEM	03	250,828 K	476,7...	180,6...	Not allow...
CompatTelRunner.exe	5412	Running	SYSTEM	00	14,188 K	226,1...	1,294...	Not allow...
mpam-7c32699f.exe	7008	Running	NETWORK...	00	484 K	154,2...	154,2...	Not allow...
mpam-3c584dd9.exe	2372	Running	NETWORK...	00	304 K	154,2...	154,2...	Not allow...
chrome.exe	3292	Running	TestAdmin	01	3,644 K	130,8...	152,3...	Disabled
Registry	112	Running	SYSTEM	00	18,800 K	86,17...	132,0...	Not allow...
chrome.exe	5204	Running	TestAdmin	00	15,548 K	62,42...	8,981...	Disabled
svchost.exe	3112	Running	LOCAL SE...	00	7,240 K	48,42...	982,7...	Not allow...
svchost.exe	2248	Running	SYSTEM	00	4,148 K	43,36...	1,883...	Not allow...
chrome.exe	4816	Running	TestAdmin	00	52,620 K	39,95...	75,24...	Disabled
svchost.exe	1344	Running	LOCAL SE...	00	10,008 K	25,13...	9,718...	Not allow...
SearchUI.exe	6396	Running	TestAdmin	00	91,496 K	11,95...	10,05...	Disabled
dllhost.exe	1920	Running	TestAdmin	00	2,276 K	8,135...	1,437...	Disabled
svchost.exe	4028	Running	SYSTEM	00	5,116 K	7,279...	3,736	Not allow...
explorer.exe	4168	Running	TestAdmin	00	24,052 K	6,927...	895,9...	Disabled
chrome.exe	5348	Running	TestAdmin	00	61,472 K	6,474...	13,27...	Disabled
software_reporter_to...	5100	Running	TestAdmin	00	560 K	6,089...	11,88...	Disabled
TiWorker.exe	6368	Running	SYSTEM	00	19,940 K	5,781...	112,5...	Not allow...
chrome.exe	5228	Running	TestAdmin	00	33,348 K	5,564...	21,52...	Disabled
SearchIndexer.exe	5092	Running	SYSTEM	00	11,704 K	5,139...	3,477...	Not allow...
System	4	Running	SYSTEM	01	20 K	4,878...	18,85...	
svchost.exe	3104	Running	SYSTEM	00	10,656 K	4,697	3,303	Not allow...

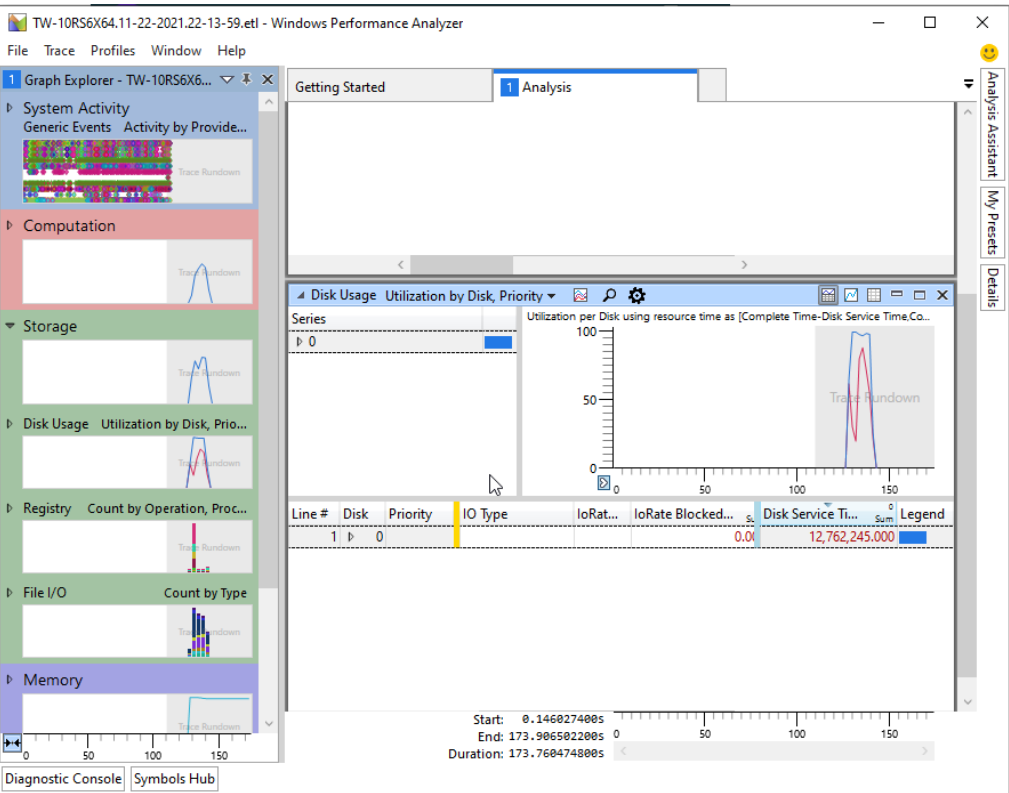
^ Fewer details End task

EX2

Task manager view:



WPA view:

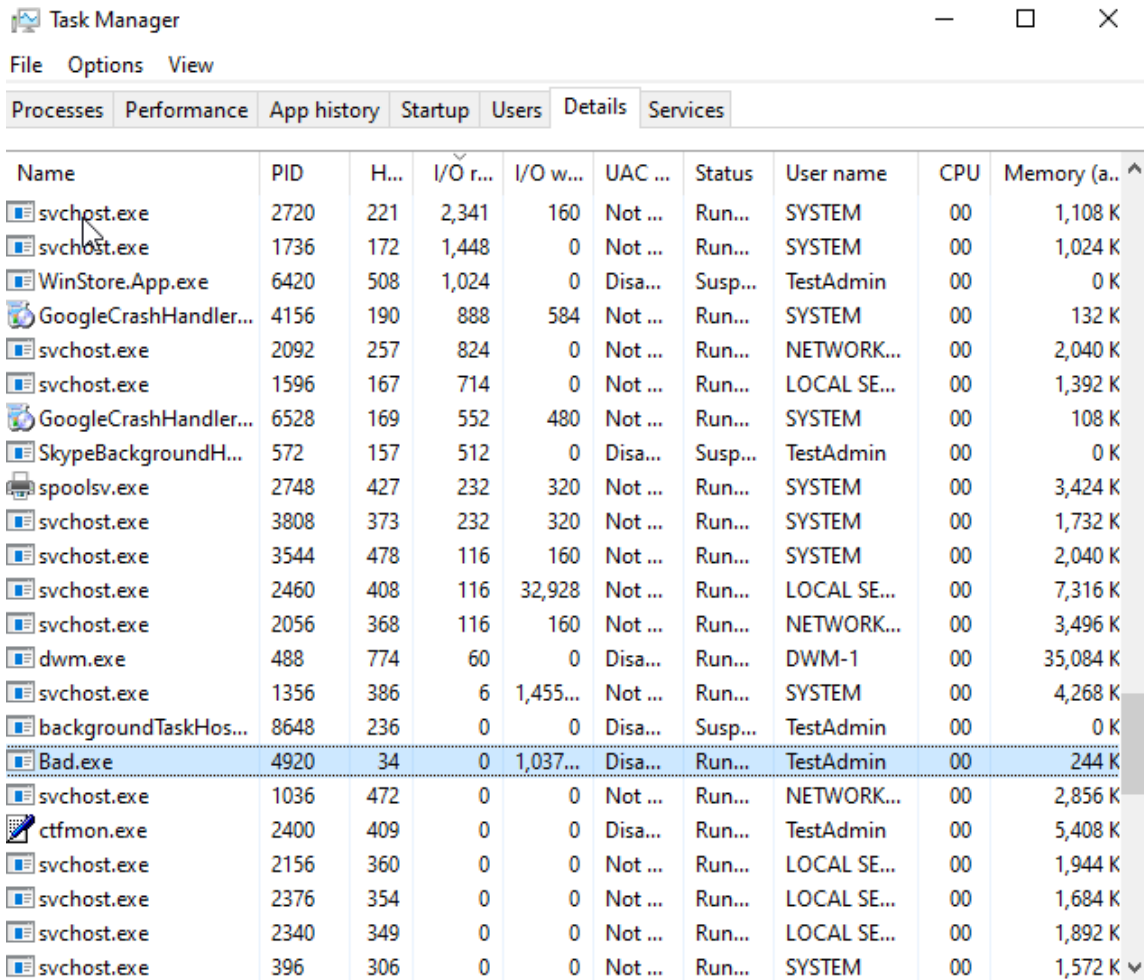


Log.exe vs GoodLog.exe

Process Monitor - C:\Users\TestAdmin\Desktop\ProcessMonitor\Logfile.PML							
File	Edit	Event	Filter	Tools	Options	Help	
Time ...	Process Name	PID	Operation	Path	Result	Detail	
8:49:4...	GoodLog.exe	5332	Process Start		SUCCESS	Parent	
8:49:4...	GoodLog.exe	5332	Thread Create		SUCCESS	Thread	
8:49:4...	GoodLog.exe	5332	Load Image	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Image	
8:49:4...	GoodLog.exe	5332	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length		
8:49:4...	GoodLog.exe	5332	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desire		
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Contr...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length		
8:49:4...	GoodLog.exe	5332	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		
8:49:4...	GoodLog.exe	5332	CreateFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image	
8:49:4...	GoodLog.exe	5332	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desire		
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desire		
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\Software\Policies\Microsoft\Win...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND Length		
8:49:4...	GoodLog.exe	5332	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS		
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND Desire		
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type:	
8:49:4...	GoodLog.exe	5332	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type:	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desire	
8:49:4...	GoodLog.exe	5332	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length		
8:49:4...	GoodLog.exe	5332	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS		
8:49:4...	GoodLog.exe	5332	QueryNameInfo	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Name:	
8:49:4...	GoodLog.exe	5332	CreateFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Desire	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	ReadFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	WriteFile	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Offset:	
8:49:4...	GoodLog.exe	5332	QueryStandard...	C:\Nab08tasks\Task-03\Task-A\Good...	SUCCESS	Allocat	

Task B:

```
C:\lab08-tasks\Task-03\Task-B>cd Good
C:\lab08-tasks\Task-03\Task-B\Good>Good.exe
C:\lab08-tasks\Task-03\Task-B\Good>cd ..
C:\lab08-tasks\Task-03\Task-B>cd Bad
C:\lab08-tasks\Task-03\Task-B\Bad>Bad.exe
```



Task Manager									
File Options View									
Processes Performance App history Startup Users Details Services									
Name	PID	H...	I/O r...	I/O w...	UAC ...	Status	User name	CPU	Memory (a.. ^
svchost.exe	2720	221	2,341	160	Not ...	Run...	SYSTEM	00	1,108 K
svchost.exe	1736	172	1,448	0	Not ...	Run...	SYSTEM	00	1,024 K
WinStore.App.exe	6420	508	1,024	0	Disa...	Susp...	TestAdmin	00	0 K
GoogleCrashHandler...	4156	190	888	584	Not ...	Run...	SYSTEM	00	132 K
svchost.exe	2092	257	824	0	Not ...	Run...	NETWORK...	00	2,040 K
svchost.exe	1596	167	714	0	Not ...	Run...	LOCAL SE...	00	1,392 K
GoogleCrashHandler...	6528	169	552	480	Not ...	Run...	SYSTEM	00	108 K
SkypeBackgroundH...	572	157	512	0	Disa...	Susp...	TestAdmin	00	0 K
spoolsv.exe	2748	427	232	320	Not ...	Run...	SYSTEM	00	3,424 K
svchost.exe	3808	373	232	320	Not ...	Run...	SYSTEM	00	1,732 K
svchost.exe	3544	478	116	160	Not ...	Run...	SYSTEM	00	2,040 K
svchost.exe	2460	408	116	32,928	Not ...	Run...	LOCAL SE...	00	7,316 K
svchost.exe	2056	368	116	160	Not ...	Run...	NETWORK...	00	3,496 K
dwm.exe	488	774	60	0	Disa...	Run...	DWM-1	00	35,084 K
svchost.exe	1356	386	6	1,455...	Not ...	Run...	SYSTEM	00	4,268 K
backgroundTaskHos...	8648	236	0	0	Disa...	Susp...	TestAdmin	00	0 K
Bad.exe	4920	34	0	1,037...	Disa...	Run...	TestAdmin	00	244 K
svchost.exe	1036	472	0	0	Not ...	Run...	NETWORK...	00	2,856 K
ctfmon.exe	2400	409	0	0	Disa...	Run...	TestAdmin	00	5,408 K
svchost.exe	2156	360	0	0	Not ...	Run...	LOCAL SE...	00	1,944 K
svchost.exe	2376	354	0	0	Not ...	Run...	LOCAL SE...	00	1,684 K
svchost.exe	2340	349	0	0	Not ...	Run...	LOCAL SE...	00	1,892 K
svchost.exe	396	306	0	0	Not ...	Run...	SYSTEM	00	1,572 K

From SS we can observe the large number of handles of the process (column after PID), proving that Bad.exe opens files without closing them, causing lag.

Looks like the process keeps creating files then opens them without closing them.

The screenshot displays the Process Monitor (ProcMon) application. The main window shows a list of events in the 'File System' category, filtered by 'Process Name' and 'PID'. The 'Process Name' column is set to 'HandleLeak.exe' and the 'PID' column is set to '3752'. The 'Operation' column is set to 'RegOpenKey'. The 'Path' column is set to 'HKLMSYSTEM\CurrentControlSet\Control\WPA\'. The 'Result' column is set to 'SUCCESS'. The 'Event' column is set to 'CreateFile'. The 'Process' column is set to 'C:\Windows\System32\kernel32.dll'. The 'Stack' column is set to 'C:\Windows\System32\kernel32.dll'. The 'Event' column is set to 'CreateFile'. The 'Process' column is set to 'C:\Windows\System32\kernel32.dll'. The 'Stack' column is set to 'C:\Windows\System32\kernel32.dll'.

The 'Event Properties' dialog box is open, showing the 'Event' tab. The 'Event' is 'CreateFile'. The 'Process' is 'C:\Windows\System32\kernel32.dll'. The 'Stack' is 'C:\Windows\System32\kernel32.dll'. The 'Date' is '11/23/2023 9:10:52.8973997 AM'. The 'Thread' is '6228'. The 'Class' is 'File System'. The 'Operation' is 'CreateFile'. The 'Result' is 'SUCCESS'. The 'Path' is 'C:\Windows\System32\kernel32.dll'. The 'Duration' is '0.0000525'. The 'Desired Access' is 'Execute/Traverse, Synchronize'. The 'Disposition' is 'Open'. The 'Options' are 'Directory, Synchronous IO Non-Alert'. The 'Attributes' are 'ShareMode'. The 'AllocationSize' is 'n/a'. The 'OpenResult' is 'Opened'.

Ex5:

Didn't manage to finish but did some work. Will attach source file.

Ex6:

Feedback Performance Evaluation

Your response has been recorded.

[Submit another response](#)