구글에서 무료로 제공하는 실행 중인 프로세스가 바이러스인지 검사하는 방법입니다.
대략 70여 개의 엔진으로 검사를 합니다.

1.
Sysinternals Suit

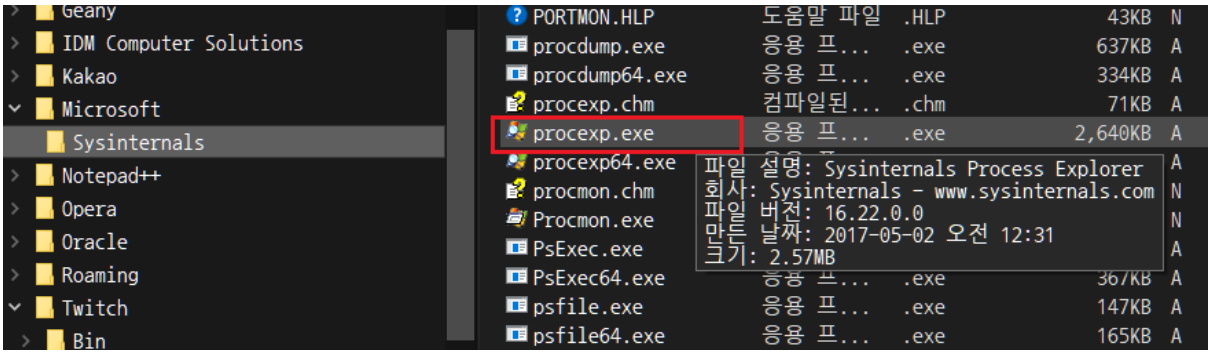
다운로드 가능한 홈페이지 : Sysinternals Suite

마이크로소프트 에서 제공하는 무료 시스템 유틸리티 모음으로 설치가 필요없이 바로 실행이 가능합니다.
모음집 전체를 다운받거나 필요한 것만 골라서 받은 후, 원하는 위치에서 압축 해제하면 됩니다.
여기서 필요한 것은 **Process Explorer** 입니다.

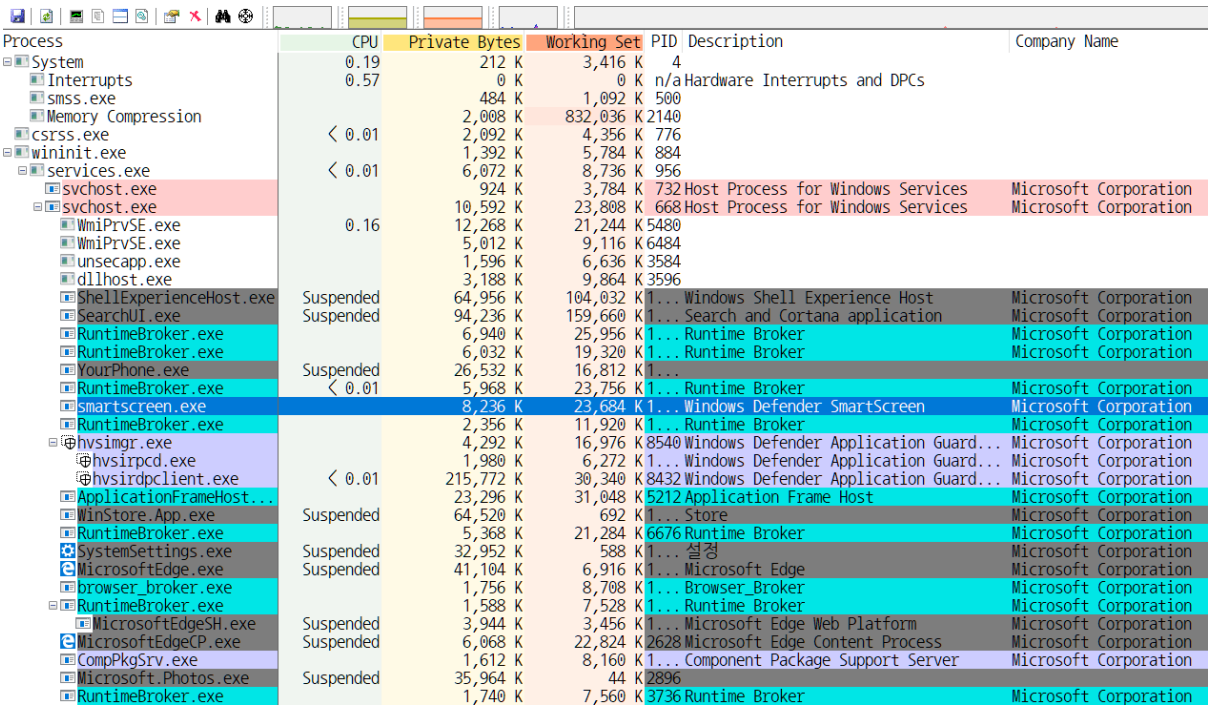
2.
Process Explorer

다운로드 가능한 홈페이지 : Process Explorer

윈도우의 기본 작업 관리자를 대체할 수 있는 강력한 프로세스 관리자 입니다.
프로세스 관리가 매우 중요하다면 대체해서 사용하는 것이 여러모로 더 좋습니다.



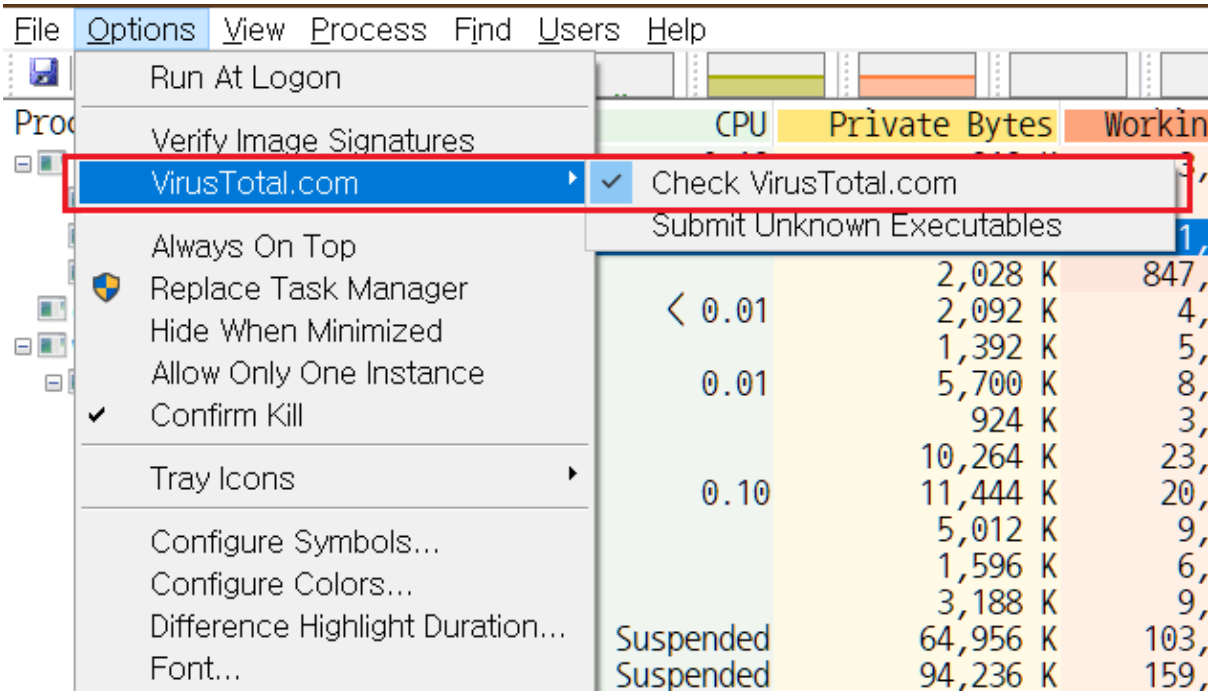
procexp.exe 를 실행합니다. 64비트 운영체제일 경우는 **procexp64.exe** 를 바로 실행해도 됩니다.
처음 실행하면 저작권에 동의할 것인지 물어 봅니다. 동의하면 이후부터는 무료로 사용할 수 있습니다.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System	0.19	212 K	3,416 K	4		
Interrupts	0.57	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		484 K	1,092 K	500		
Memory Compression		2,008 K	832,036 K	2140		
csrss.exe	< 0.01	2,092 K	4,356 K	776		
wininit.exe		1,392 K	5,784 K	884		
services.exe	< 0.01	6,072 K	8,736 K	956		
svchost.exe		924 K	3,784 K	732	Host Process for Windows Services	Microsoft Corporation
svchost.exe		10,592 K	23,808 K	668	Host Process for Windows Services	Microsoft Corporation
WmiPrvSE.exe	0.16	12,268 K	21,244 K	5480		
WmiPrvSE.exe		5,012 K	9,116 K	6484		
unsecapp.exe		1,596 K	6,636 K	3584		
dllhost.exe		3,188 K	9,864 K	3596		
ShellExperienceHost.exe	Suspended	64,956 K	104,032 K	1...	Windows Shell Experience Host	Microsoft Corporation
SearchUI.exe	Suspended	94,236 K	159,660 K	1...	Search and Cortana application	Microsoft Corporation
RuntimeBroker.exe		6,940 K	25,956 K	1...	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		6,032 K	19,320 K	1...	Runtime Broker	Microsoft Corporation
YourPhone.exe	Suspended	26,532 K	16,812 K	1...		
RuntimeBroker.exe	< 0.01	5,968 K	23,756 K	1...	Runtime Broker	Microsoft Corporation
smartscreen.exe		8,236 K	23,684 K	1...	Windows Defender SmartScreen	Microsoft Corporation
RuntimeBroker.exe		2,356 K	11,920 K	1...	Runtime Broker	Microsoft Corporation
hvsimgr.exe		4,292 K	16,976 K	8540	Windows Defender Application Guard...	Microsoft Corporation
hvsirpcd.exe		1,980 K	6,272 K	1...	Windows Defender Application Guard...	Microsoft Corporation
hvsirdpclient.exe	< 0.01	215,772 K	30,340 K	8432	Windows Defender Application Guard...	Microsoft Corporation
ApplicationFrameHost...		23,296 K	31,048 K	5212	Application Frame Host	Microsoft Corporation
WinStore.App.exe	Suspended	64,520 K	692 K	1...	Store	Microsoft Corporation
RuntimeBroker.exe		5,368 K	21,284 K	6676	Runtime Broker	Microsoft Corporation
SystemSettings.exe	Suspended	32,952 K	588 K	1...	설정	Microsoft Corporation
MicrosoftEdge.exe	Suspended	41,104 K	6,916 K	1...	Microsoft Edge	Microsoft Corporation
browser_broker.exe		1,756 K	8,708 K	1...	Browser_Broker	Microsoft Corporation
RuntimeBroker.exe		1,588 K	7,528 K	1...	Runtime Broker	Microsoft Corporation
MicrosoftEdgeSH.exe	Suspended	3,944 K	3,456 K	1...	Microsoft Edge Web Platform	Microsoft Corporation
MicrosoftEdgeCP.exe	Suspended	6,068 K	22,824 K	2628	Microsoft Edge Content Process	Microsoft Corporation
CompPkgSrv.exe		1,612 K	8,160 K	1...	Component Package Support Server	Microsoft Corporation
Microsoft.Photos.exe	Suspended	35,964 K	44 K	2896		
RuntimeBroker.exe		1,740 K	7,560 K	3736	Runtime Broker	Microsoft Corporation

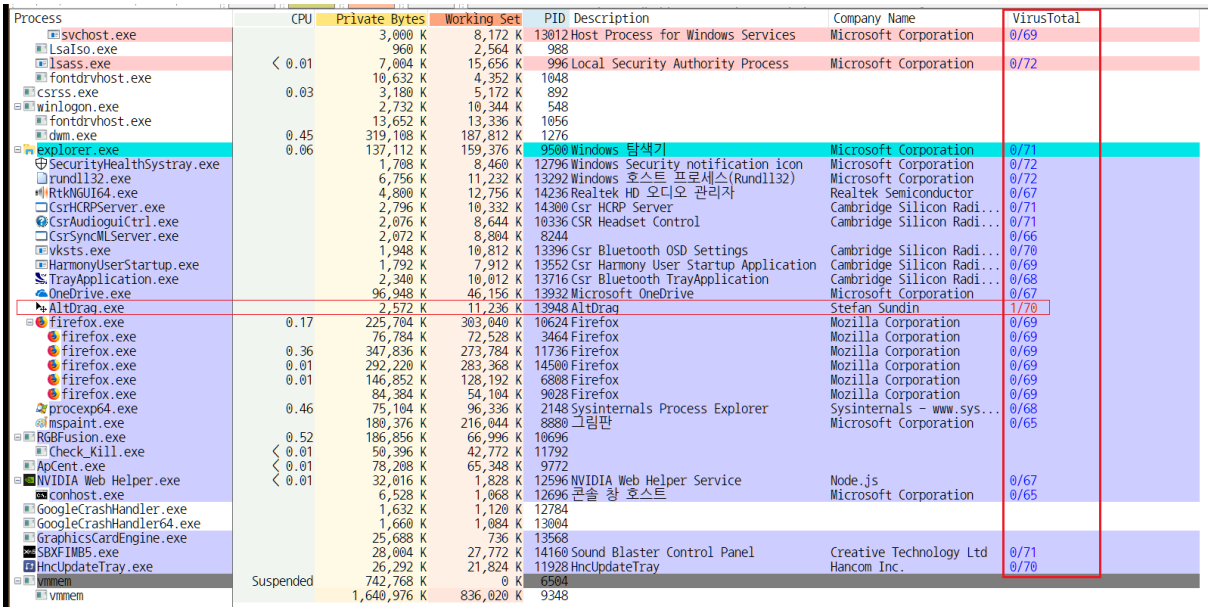
실행 중인 프로세스를 트리 형식으로 보여주므로 관리하기가 매우 편리합니다.
특별한 목적(?) 으로 숨겨진 프로세스까지 다 볼 수 있습니다.

3.
VirusTotal.com



Options → VirusTotal.com → Check VirusTotal.com 을 설정합니다.

4.
검사 결과



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
svchost.exe		3,000 K	8,172 K	13012	Host Process for Windows Services	Microsoft Corporation	0/69
LsaIso.exe		960 K	2,564 K	988			
lsass.exe	< 0.01	7,004 K	15,656 K	996	Local Security Authority Process	Microsoft Corporation	0/72
fontdrvhost.exe		10,632 K	4,352 K	1048			
csrss.exe	0.03	3,180 K	5,172 K	892			
winlogon.exe		2,732 K	10,344 K	548			
fontdrvhost.exe		13,652 K	13,336 K	1056			
dwm.exe	0.45	319,108 K	187,812 K	1276			
explorer.exe	0.06	137,112 K	159,376 K	9500	Windows 탐색기	Microsoft Corporation	0/71
SecurityHealthSystray.exe		1,708 K	8,460 K	12796	Windows Security notification icon	Microsoft Corporation	0/72
rundll32.exe		6,756 K	11,232 K	13292	Windows 호스트 프로세스(Rundll32)	Microsoft Corporation	0/72
RtkNGUI64.exe		4,800 K	12,756 K	14236	Realtek HD 오디오 관리자	Realtek Semiconductor	0/67
CsrHCRPServer.exe		2,796 K	10,332 K	14300	Csr HCRP Server	Cambridge Silicon Radi...	0/71
CsrAudioguiCtrl.exe		2,076 K	8,644 K	10336	CSR Headset Control	Cambridge Silicon Radi...	0/71
CsrSyncMLServer.exe		2,072 K	8,804 K	8244			0/66
vksts.exe		1,948 K	10,812 K	13396	Csr Bluetooth OSD Settings	Cambridge Silicon Radi...	0/70
HarmonyUserStartup.exe		1,792 K	7,912 K	13552	Csr Harmony User Startup Application	Cambridge Silicon Radi...	0/69
TrayApplication.exe		2,340 K	10,012 K	13716	Csr Bluetooth TrayApplication	Cambridge Silicon Radi...	0/68
OneDrive.exe		96,948 K	46,156 K	13932	Microsoft OneDrive	Microsoft Corporation	0/67
AltDrag.exe		2,572 K	11,236 K	13948	AltDrag	Stefan Sundin	1/70
firefox.exe	0.17	225,704 K	303,040 K	10624	Firefox	Mozilla Corporation	0/69
firefox.exe		76,784 K	72,528 K	3464	Firefox	Mozilla Corporation	0/69
firefox.exe	0.36	347,836 K	273,784 K	11736	Firefox	Mozilla Corporation	0/69
firefox.exe	0.01	292,220 K	283,368 K	14500	Firefox	Mozilla Corporation	0/69
firefox.exe	0.01	146,852 K	128,192 K	6808	Firefox	Mozilla Corporation	0/69
firefox.exe		84,384 K	54,104 K	9028	Firefox	Mozilla Corporation	0/69
procexp64.exe	0.46	75,104 K	96,336 K	2148	Sysinternals Process Explorer	Sysinternals - www.sys...	0/68
mspaint.exe		180,376 K	216,044 K	8880	그림판	Microsoft Corporation	0/65
RGBFusion.exe	0.52	186,856 K	66,996 K	10696			
Check_Kill.exe	< 0.01	50,396 K	42,772 K	11792			
ApCent.exe	< 0.01	78,208 K	65,348 K	9772			
NVIDIA Web Helper.exe	< 0.01	32,016 K	1,828 K	12596	NVIDIA Web Helper Service	Node.js	0/67
conhost.exe		6,528 K	1,068 K	12696	콘솔 창 호스트	Microsoft Corporation	0/65
GoogleCrashHandler.exe		1,632 K	1,120 K	12784			
GoogleCrashHandler64.exe		1,660 K	1,084 K	13004			
GraphicsCardEngine.exe		25,688 K	736 K	13568			
SBXFIMB5.exe		28,004 K	27,772 K	14160	Sound Blaster Control Panel	Creative Technology Ltd	0/71
HncUpdateTray.exe		26,292 K	21,824 K	11928	HncUpdateTray	Hancom Inc.	0/70
vmmem	Suspended	742,768 K	0 K	6504			
vmmem		1,640,976 K	836,020 K	9348			

실행 중인 프로세스의 바이러스 검사 결과가 실시간으로 표시 됩니다
표시 형식은 "바이러스로 검사한 엔진의 수 / 바이러스를 검사하는 검색 엔진의 수" 입니다.

위의 예에서 **"AltDrag.exe"** 가 **"1/70"** 으로 바이러스로 검사한 엔진이 **1**개라고 표시가 되었는데, 이것은 오진입니다.
바이러스로 진단하는 엔진의 수가 **1-5** 정도면 오진일 가능성이 매우 크며, 실제로 오진인 경우가 많습니다.
그러나, 그 이상의 수가 바이러스로 진단하면 일단 의심해야 합니다.

윈도우에서 기본으로 제공하는 **Windows Defender** 와 병행하면 웬만한 유료 바이러스 백신보다 더 좋은 효과를 볼 수도 있습니다.
.