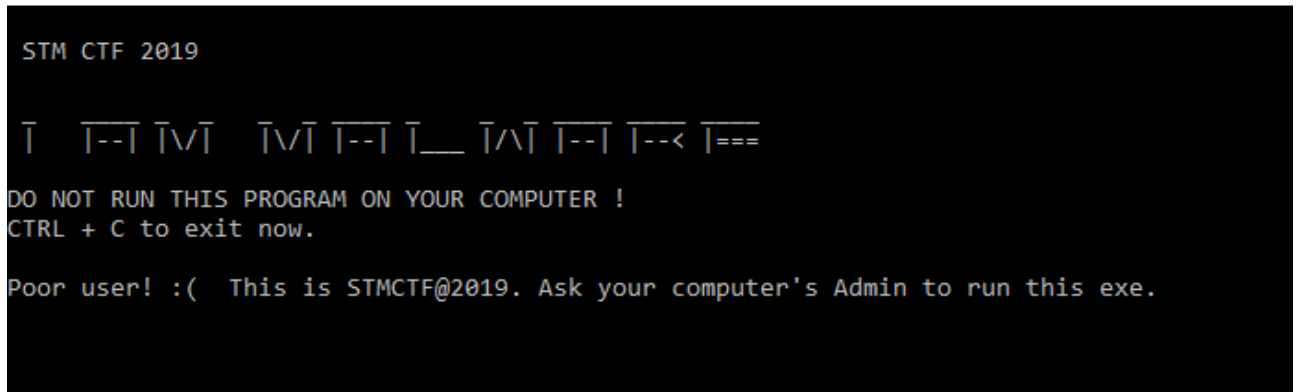
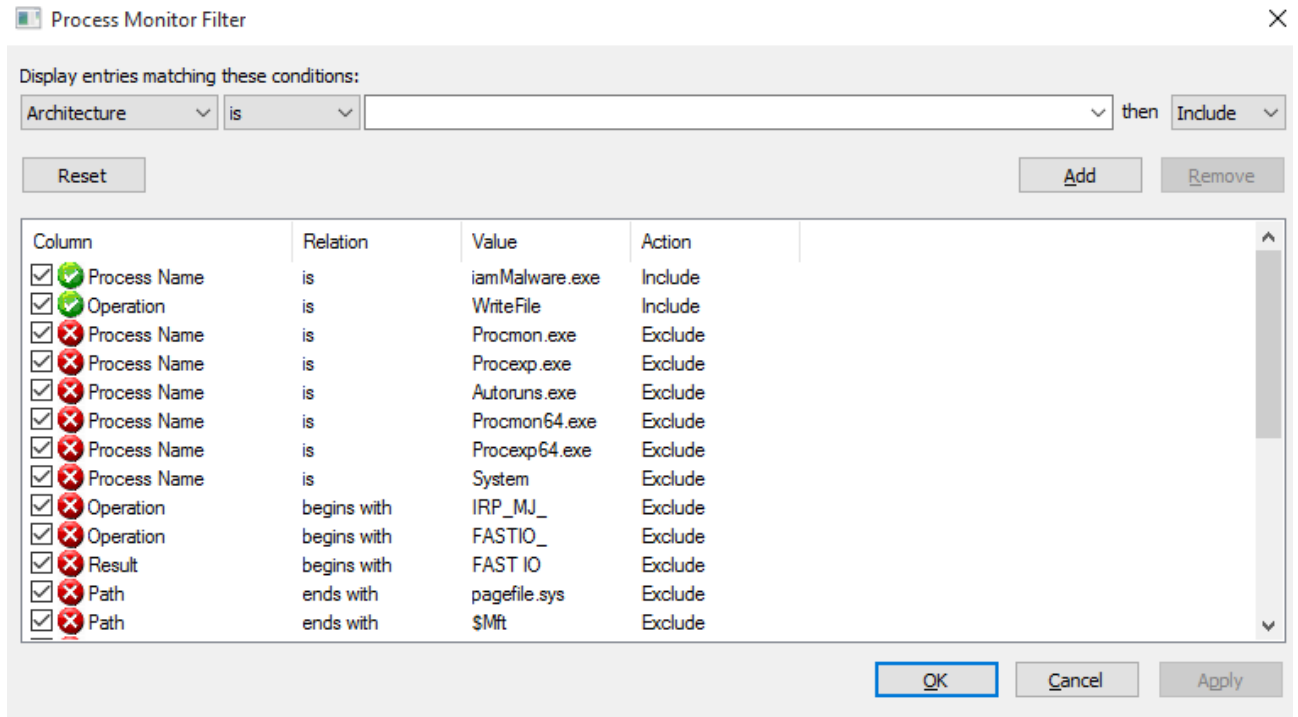


Reverse kategorisinde bulunan iamMalware isimli dosyayı indirip çalıştırdığımızda admin yetkileriyle çalıştırılmamızı istiyordu.

C:\Users\{etn}\Desktop\iammalware.exe




Sorunun metninde flag'i bilgisayara bıraktığı yazıyordu. Bundan dolayı procmonda gerekli ayarları yapıp dosyayı izlemeye başladım. İlk görselde procmonda kullandığım filtre ikinci görselde ise procmon çıktısını göreceksiniz.



Time ...	Process Name	PID	Operation	Path	Result	Detail
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\AutoWorkplace.exe.config	SUCCESS	Offset: 391, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\NOISE.DAT	SUCCESS	Offset: 743, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\DefaultQuestions.json	SUCCESS	Offset: 860, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\enowman.ini	SUCCESS	Offset: 1,402, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\cirof.rat	SUCCESS	Offset: 1,990, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\icrav03.rat	SUCCESS	Offset: 8,800, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\OEMDefaultAssociations.xml	SUCCESS	Offset: 15,464, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\DESKTOP-CVJNS7_reli_HistoryPrediction.bin	SUCCESS	Offset: 16,148, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\DESKTOP-M7F1N66_Administrator_HistoryPrediction.bin	SUCCESS	Offset: 16,150, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\DESKTOP-CVJNS7_defaultuser0_HistoryPrediction.bin	SUCCESS	Offset: 16,150, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\gsmorp.dll	SUCCESS	Offset: 19,010, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\cuzzapi.dll	SUCCESS	Offset: 23,306, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\neucom.dll	SUCCESS	Offset: 23,610, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\msvcp140_codecvt_ids.dll	SUCCESS	Offset: 27,626, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\microsoft.windows.softwarelogo.showdesktop.exe	SUCCESS	Offset: 29,802, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\msvcp140_1.dll	SUCCESS	Offset: 27,626, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\perf009.dat	SUCCESS	Offset: 1, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\gwbcn.dll	SUCCESS	Offset: 1, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf100cht.dll	SUCCESS	Offset: 36,178, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf100chs.dll	SUCCESS	Offset: 36,178, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\license.ttf	SUCCESS	Offset: 36,745, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf100kor.dll	SUCCESS	Offset: 43,346, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf100jpn.dll	SUCCESS	Offset: 43,858, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\vicruntime140_1.dll	SUCCESS	Offset: 44,010, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf110cht.dll	SUCCESS	Offset: 46,161, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf110chs.dll	SUCCESS	Offset: 46,161, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf120cht.dll	SUCCESS	Offset: 46,249, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf120chs.dll	SUCCESS	Offset: 46,249, Length: 1, Priority: Normal
18:13:...	iam\Malware.exe	3488	WriteFile	C:\Windows\System32\mf140cht.dll	SUCCESS	Offset: 47,385, Length: 1, Priority: Normal

Görselde de görüldüğü gibi yazdığı dosyaların en sonuna tek bir karakter yazılmış. Karakterlere teker teker baktığımızda flag'i görebilirdik Aşağıda sadece ilk dosyanınki var

 AutoWorkplace.exe.config

```

3 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text
D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 <?xml version="1
F 3E 0D 0A 3C 63 6F 6E 66 69 67 75 72 .0"?>..<configur
F 6E 3E 0D 0A 20 20 0D 0A 20 20 3C 73 ation>.. .. <s
5 6D 2E 64 69 61 67 6E 6F 73 74 69 63 ystem.diagnostic
A 20 20 20 20 3C 21 2D 2D 0D 0A 20 20 s>.. <!--..
4 72 61 63 65 20 61 75 74 6F 66 6C 75 <trace autoflu
2 74 72 75 65 22 20 69 6E 64 65 6E 74 sh="true" indent
5 3D 22 34 22 3E 0D 0A 20 20 20 20 20 size="4">..
C 69 73 74 65 6E 65 72 73 3E 0D 0A 20 <listeners>..
0 20 20 20 20 20 20 20 3C 61 64 64 20 6E <add n
D 22 41 75 74 6F 57 6F 72 6B 70 6C 61 ame="AutoWorkpla
0 74 79 70 65 3D 22 53 79 73 74 65 6D ce" type="System
1 67 6E 6F 73 74 69 63 73 2E 54 65 78 .Diagnostics.Tex
9 74 65 72 54 72 61 63 65 4C 69 73 74 tWriterTraceList
2 22 20 20 69 6E 69 74 69 61 6C 69 7A ener" initializ
4 61 3D 22 61 75 74 6F 57 6F 72 6B 70 eData="autoWorkp
5 2E 6C 6F 67 22 20 74 72 61 63 65 4F lace.log" traceO
5 74 4F 70 74 69 6F 6E 73 3D 22 44 61 utputOptions="Da
9 6D 65 22 20 2F 3E 0D 0A 20 20 20 20 teTime" />..
C 2F 6C 69 73 74 65 6E 65 72 73 3E 0D </listeners>.
0 20 3C 2F 74 72 61 63 65 3E 0D 0A 20 . </trace>..
D 2D 3E 0D 0A 20 20 3C 2F 73 79 73 74 -->.. </syst
4 69 61 67 6E 6F 73 74 69 63 73 3E 0D em.diagnostics>.
C 2F 63 6F 6E 66 69 67 75 72 61 74 69 ...</configurati
D 0A 53 on>..S|

```