FORENSICS: FIGURE ME OUT BY Monhal

EASY

Scenario:

Someone placed a suspicious file in the system.
The IT team has been working unsuccessfully for several hours to locate the file.
Help them find the file and discover what it does.

Objectuves:

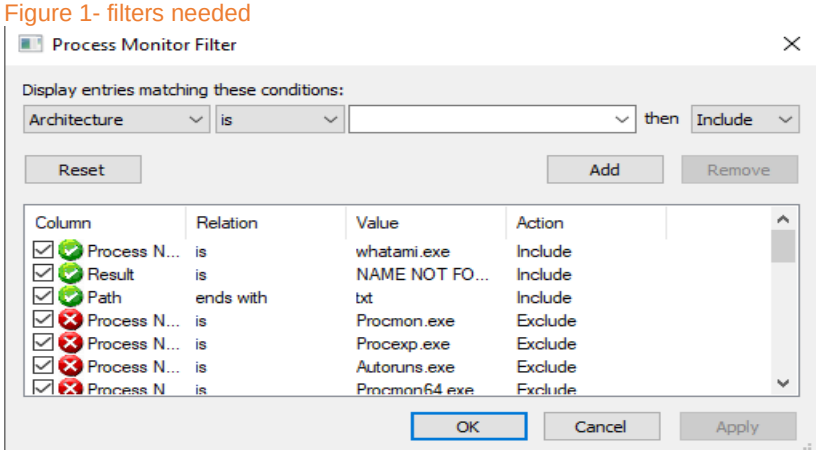
- Investigate the file.
- Find the flag.

Used tools:

Procmon64.exe (sysinternals)

First, downloading the attached file 'WhatAmI.exe".
then running procmon64.exe and deploying the filters:

Figure 1- filters needed

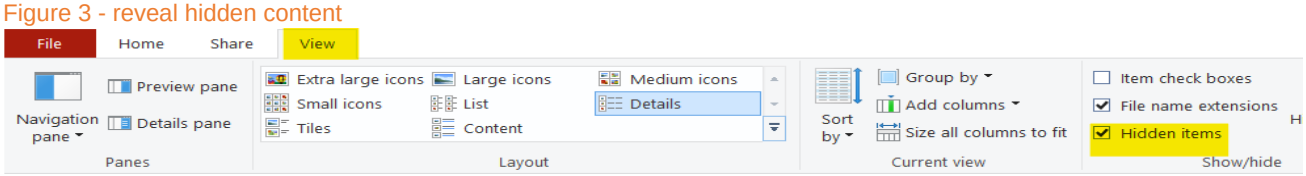


In the picture below it is possible to see that WhatAmI.exe create a file in C:\Users\[username]\App Data\Local\Temp\cracker.exe

Figure 2 - path to file

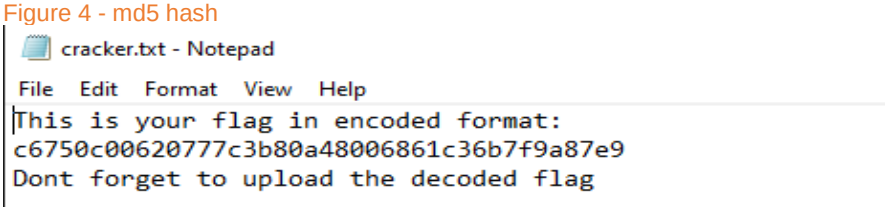
*Notice that App Data is hidden here is how to display it:

Figure 3 - reveal hidden content



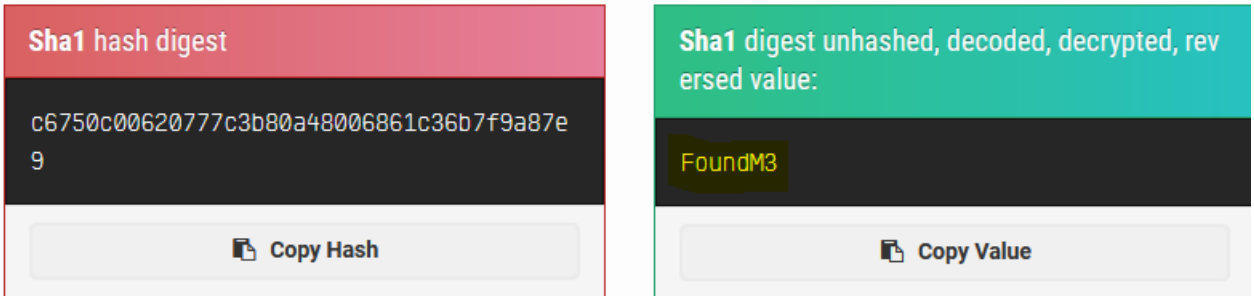
Navigating to the path, and searching for 'cracker.txt' will not help, because the file would be already deleted. So instead, a cracker.txt file need to be created in order to reveal its content.

Figure 4 - md5 hash



Last step is pasting the hash in google search and searching the decrypted format in the results:

Figure 5 - decrypting the hash



CHALLENGE PWNED!