Microsoft released Sysmon 10 with DNS query logging feature

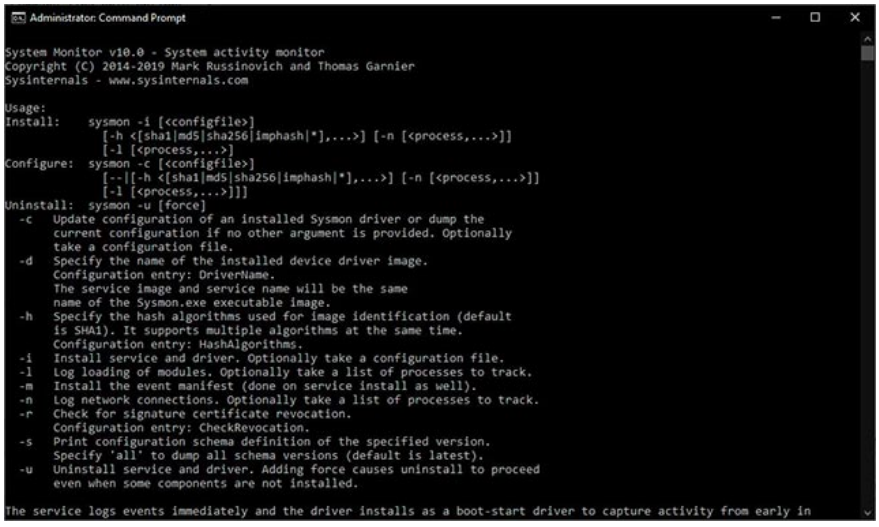
Microsoft has released the Sysmon 10 tool today and comes with the long-awaited DNS query (DNS Query Logging) feature.

Microsoft has released the Sysmon 10 tool today and comes with the long-awaited DNS query (DNS Query Logging) feature. Accordingly, this feature will allow Sysmon users to log DNS queries performed on the monitored computer, and this will also include query execution.

If you don't already know, Sysmon (aka) System Monitor is a Sysiternals tool that allows users to monitor certain activities on the computer and write information about those activities to the Windows Event Viewer.

1. It is possible to download official ISO files for Windows 10 20H1

To download Sysmon 10 to your computer, you can visit the Sysiternal website or download it from *https: //live.sysi INTERNals.com/sysmon.exe* . After the software has been successfully downloaded, you need to run it in the advanced comand prompt (comand prompt with administrative rights), because this tool requires administrator privileges to be able to launch.



Sysmon 10.0

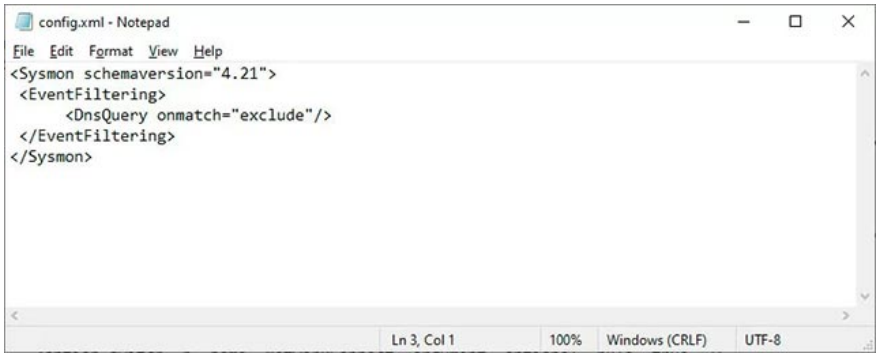
1. Apple's new iCloud Windows 10 application is now available in MS Store

If running simply without any arguments, the program will display its usage information and for more details, you can visit Sysmon's Sysiternals website.

By default, Sysmon will monitor basic information such as creating processes and modifying file times. However, you can also configure this tool to monitor other events such as loading drivers, creating files, Registry events, and more.

There is a notable new point in Sysmon 10.0, which is that Microsoft has added the ability to monitor DNS queries and executable files that execute queries. This feature will need to be enabled via the configuration file with the DNSQuery directive.

An example of a very basic configuration file that allows DNS query logging is shown below. This configuration file can be installed with **sysmon.exe -i config.xml** in case sysmon is not installed, or **sysmon.exe -c config.xml** , in case sysmon is already running.

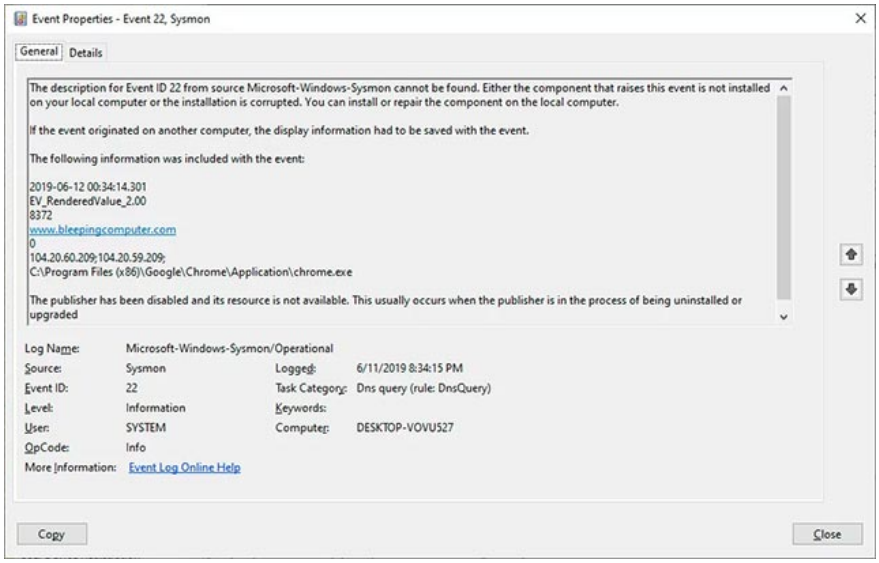


Enable DNSQuery logging feature

1. The input experience in Windows 10 20H1 update will be significantly better, and this is the reason

When Sysmon is started with the above configuration file, it will start logging DNS query events (DNS Query) into the **Applications and Services Logs / Microsoft / Windows / Sysmon / Operational section in Event Viewer.**

Below you can see an example of Chrome querying DNS for the *www.bleepingcomputer.com* address when we visit this site.



Example of DNS query logging

1. Search and activate hidden features in Windows 10 with Mach2 tool

The example above is just a small sketch of the overall picture of what System Monitor can do. If you want to learn how to use this software, I really recommend reading the documentation on the Sysiternals page.

In case you only want to access and use the Sysmon configuration file available to detect malicious traffic and threats, you can use SwiftOnSecurity's Sysmon configuration file on GitHub.

You finished reading the article "**Microsoft released Sysmon 10 with DNS query logging feature**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com