# Windows Research Kernel Part 2 — Monitoring the function invocation

JULY 28, 2018

> This is the second part of the WRK series. For your convenience you can find other parts in the table of contents in Part 1 — Compiling and debugging

In this part we are going to monitor the invocation of `QuerySystemInformation` system function by using the debugger.
First, make sure that you can debug the kernel. Next, open file `base\ntos\ex\sysinfo.c`. You can see that the function starts in line 1390. We will add a static variable to count the invocations, so go to the line 1721 and add the following:

```
1 static int NumTimesCalled = 0
```

Next, just before `Status = STATUS_SUCCESS;` in line 1728 add this:

```
1 DbgPrint("WRK  %d: Entering NTQuerySystemInformation\n", ++NumTimesCalled);
```

Recompile the kernel, add new boot option to the boot.ini, restart the OS, attach the debugger and you should see:

```
1 WRK  1: Entering NTQuerySystemInformation
2 WRK  2: Entering NTQuerySystemInformation
```

This is just a sample of what you can do with the code. Next time, we are going to

implement the syscall.

POSTED IN CODING, DEBUGGING

WRK

‹ PREVIOUS
*Windows Research Kernel Part 1 — Compiling and debugging*

NEXT ›
*Windows Research Kernel Part 3 — Syscall*



Search … Search

## Recent Posts

State Machine Executor Part 6 — Forking

Non-atomic assignments in Python

State Machine Executor Part 5 — Streaming

State Machine Executor Part 4 — Timeouts, exceptions, suspending

State Machine Executor Part 3 — Actions and history

## Categories

Administration

Coding

Computer Science

Databases

Debugging

Math

Philosophy

## Archive

November 2025 (2)

October 2025 (5)

August 2025 (2)

July 2025 (1)

November 2024 (1)

September 2024 (2)

June 2024 (1)

May 2024 (4)

April 2024 (1)

March 2024 (3)

February 2024 (2)

December 2023 (2)

February 2023 (4)

January 2023 (4)

December 2022 (5)

November 2022 (4)

October 2022 (5)

September 2022 (4)

August 2022 (4)

July 2022 (5)

June 2022 (4)

May 2022 (4)

April 2022 (5)

March 2022 (4)

February 2022 (4)

January 2022 (5)

December 2021 (4)

November 2021 (4)

October 2021 (5)

September 2021 (4)

August 2021 (4)

July 2021 (5)

June 2021 (4)

May 2021 (5)

April 2021 (4)

March 2021 (4)

February 2021 (4)

January 2021 (5)

December 2020 (4)

November 2020 (4)

October 2020 (5)

September 2020 (4)

August 2020 (5)

July 2020 (4)

June 2020 (4)

May 2020 (5)

April 2020 (4)

March 2020 (4)

February 2020 (5)

January 2020 (4)

December 2019 (4)

November 2019 (5)

October 2019 (4)

September 2019 (4)

August 2019 (5)

July 2019 (4)

June 2019 (5)

May 2019 (4)

April 2019 (4)

March 2019 (5)

February 2019 (5)

January 2019 (4)

December 2018 (5)

November 2018 (4)

October 2018 (4)

September 2018 (5)

August 2018 (4)

July 2018 (4)

June 2018 (5)

May 2018 (4)

April 2018 (4)

March 2018 (5)

February 2018 (4)

January 2018 (4)

December 2017 (5)

November 2017 (4)

October 2017 (4)

September 2017 (5)

August 2017 (4)

July 2017 (5)

June 2017 (4)

May 2017 (4)

April 2017 (5)

March 2017 (4)

February 2017 (4)

January 2017 (4)

December 2016 (5)

November 2016 (4)

October 2016 (5)

September 2016 (4)

August 2016 (4)

July 2016 (5)

June 2016 (4)

May 2016 (4)

April 2016 (5)

March 2016 (4)

February 2016 (4)

January 2016 (5)

December 2015 (4)

November 2015 (4)

October 2015 (5)

September 2015 (4)

August 2015 (3)

Posts