Seeing Behind The Scenes

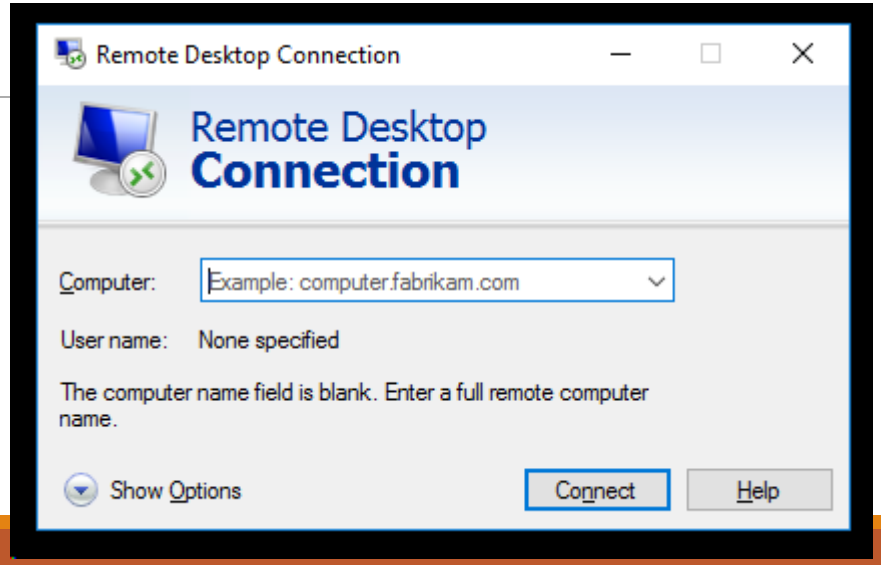
CONTACT@ADAMFURMANEK.PL

HTTP://BLOG.ADAMFURMANEK.PL

FURMANEKADAM

Audio is lagging behind in *mstsc.exe*.

FIX IT PLEASE



Audio and Video

We don’t have access to the ***mstsc.exe*** source code.

We are on our own (nobody’s going to help us).

We can use only publicly available materials.

We know nothing about ***mstsc.exe***:

- What programming language it’s written in
- How it downloads, stores, and plays audio and video
- Why it’s getting out of sync

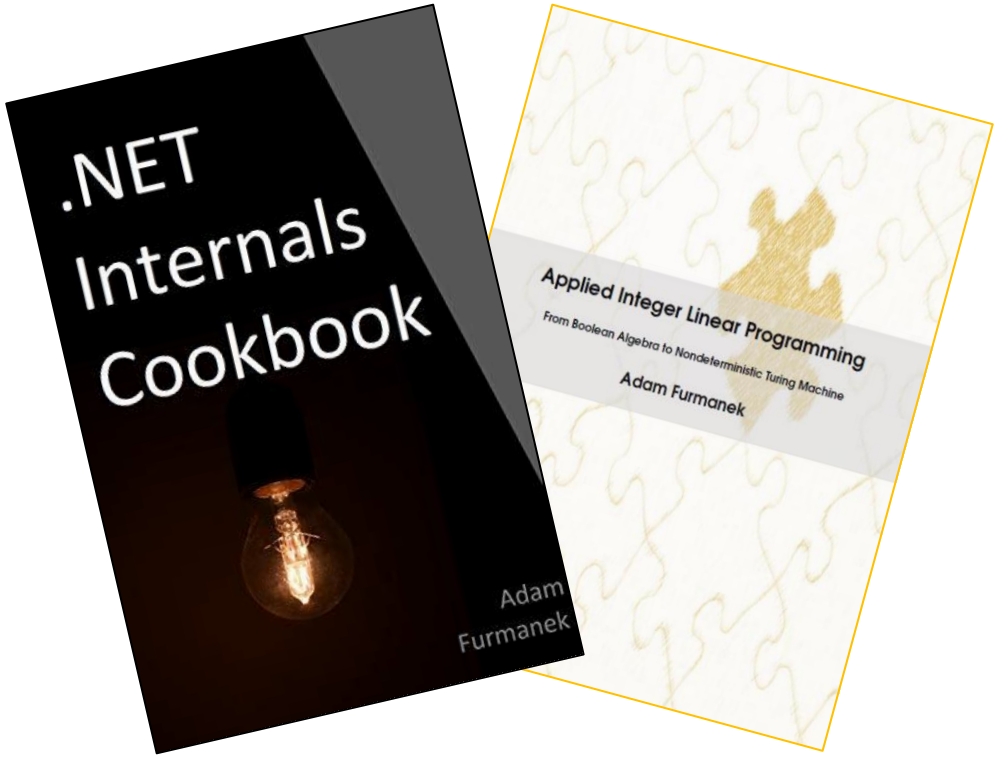
About me

Software Engineer, Blogger, Book Writer, Public Speaker.
Author of ***Applied Integer Linear Programming*** and ***.NET Internals Cookbook***.

http://blog.adamfurmanek.pl

contact@adamfurmanek.pl

furmanekadam



Random IT Utensils

IT, operating systems, maths, and more.

Agenda

Debugging is not hard. But it's not easy either

Patterns: MMCSS, threads, locks, memory, IPC, network, and others

Tools: Debugging, Profiling, Tracing, Memory, Network, Metrics

Debugging demos

Everyone knows that debugging is twice as hard as writing a program in the first place.

So if you're as clever as you can be when you write it, how will you ever debug it?

BRIAN KERNIGHAN
THE ELEMENTS OF PROGRAMMING STYLE, 2ND EDITION, CHAPTER 2

Debugging is twice as hard as writing the code in the first place.

Therefore, if you write the code as cleverly as possible, you are, by definition, not smart enough to debug it.

BRIAN KERNIGHAN?

It’s wrong

We rarely debug just our code

- When writing the code, we made assumptions about everything around
- When debugging, we can verify these assumptions

Debugging is just a different skill

- I may not be the best cook in the world, but I can still recognize good and bad food
- Debugging happens after writing the code. During debugging, we often know what doesn’t work (which side effect is incorrect)

Debugging requires different tools

- We code with IDEs (and all they bring like static code analysis, linters, etc.)
- We debug with debuggers, tracers, profilers, monitors, analyzers, etc.

Debugging is not harder than writing the code. Unfortunately, it’s not easier either. It’s just different.

How to Debug?

We hypothesize how things work.

To come up with reliable hypotheses, **we need to know how people do things** (or how things work).

We check what's going on.

- Without seeing (and reproducing on demand) it's much harder.

In order to see things, **we need to have tools**.

Next, we confirm and reject our hypotheses.

To do that, **we need to practice our skills**.

Patterns

Patterns

*The principle of least astonishment (POLA), also known as principle of least surprise, proposes that a **component of a system should behave in a way that most users will expect it to behave**, and therefore not astonish or surprise users*

During coding, we make tons of assumptions. We rely on our knowledge about computers, networks, hardware, infrastructure...

The more patterns we know, the more efficient we are. However, we need to set our expectations right.

We need to know how others do things to be good engineers.

We are not alone

AND THE TRUTH IS OUT THERE

Music makes your games slower

Multimedia Class Scheduler Service (MMCSS) enables multimedia applications to ensure that their time-sensitive processing receives prioritized access to CPU resources.

https://learn.microsoft.com/en-us/windows/win32/procthread/multimedia-class-scheduler-service

When playing music:

- 80% of your CPU is dedicated to multimedia activities (***SystemResponsiveness***)
- At most 10 non-multimedia network packets are handled each millisecond (***NetworkThrottlingIndex***)

Do not listen to the music while playing online games.

Observing application makes it faster

Time quantum for Windows Server is set to 12 clock cycles (~180 milliseconds). For client edition, it's 2 clock cycles (~30 milliseconds).

Default quantum for Linux varies. It can be 100 milliseconds. However, threads there get time slice based on their load and can be even hundreds of milliseconds.

Foreground thread get a priority boost. Windows assigns 4 clock cycles (~60 milliseconds).

Keep the app faster by looking at it.

Other examples:

- Priority inversion – if a thread waits for a resource (like mutex), the OS will boost the priorities of other threads holding the resource. Windows does that every 5 seconds.
- If a thread has been runnable for 4 seconds and hasn't been given a chance to run, the OS will boost its priority to avoid starvation. Windows does that every 1 second.

You must know bugs in the industry

Two common approaches:

- With a system-wide lock identified by name
- With a file

Do not copy blindly from Stack Overflow

- https://x.com/Foone/status/1229641258370355200
- https://www.reddit.com/r/ProgrammerHumor/comments/f6csjp/so_both_these_tools_copied_from_the_same_wrong/
- https://stackoverflow.com/questions/502303/how-do-i-programmatically-get-the-guid-of-an-application-in-c-sharp-with-net/502323#502323
- https://www.pcreview.co.uk/threads/assembly-guid.1394335/

So, both programs want to ensure you only run one copy of themselves. So they create a global mutex using the GUID of their .NET assembly, right?

except! they do it wrong. And they both do it wrong in the same way. The code involved is something like this:

```
string.Format("Global\{0}", (object) Assembly.GetExecutingAssembly().GetType().GUID);
```

The idea is to get the GUID of the assembly that's executing and to create a GUID based on that, so now you can only run one copy of it.

But it's wrong. The .GetType() part isn't supposed to be there. That gets the type of the assembly, not the assembly itself. And that type is System.Reflection.RuntimeAssembly, part of .NET itself.

So what happens is that both of them are creating a global mutex to ensure only one copy runs, but instead of basing the GUID on their own code, they're both using the GUID of a part of .NET itself. And they're using the same one!

So how'd that happen? Well, it turns out we can tell EXACTLY how that happened. Because the answer is... STACK OVERFLOW

Back in 2009, the user "Nathan" asked how to get the GUID of the running assembly. Twelve minutes later, "Cerebrus" answered. And that answer was wrong.

A year and a month later, it was pointed out (by "Yoopergeek") that it gives the wrong GUID. Three years later, Cerebrus returns and fixes the answer. They can't delete it, because it was accepted

But because they made an error in replying to someone in 2009... this flawed code caused bugs that still exist as recently as March of 2018.

Interactions can be really surprising

DLL-injection is not hacking

Many applications use ***DLL***-injection.

Windows provides multiple techniques for that:

- Hooks
- Loading libraries based on registry
- Creating threads in remote processes

Examples:

- *ForceBindIP*
- *ConEmu*
- Anti-viruses

Keyloggers are first class citizens

React to keyboard handler
- Works inside our process only

Poll the keys every millisecond
- Works across RDP sessions
- Uses more CPU

Register for a hotkey with ***RegisterHotKey***
- Sends ***WM_HOTKEY***
- No polling required
- Some keys are reserved

Register a global handler for all processes with ***SetWindowsHookEx***
- Requires ***DLL*** that will get injected
- Runs in the target process

Use paradoxes to lock critical sections

You can lock non-existent part of a file to use it as mutex:

- https://devblogs.microsoft.com/oldnewthing/20140905-00/?p=63

This works between languages, machines, or even systems not connected directly but sharing some resource (like ***SMB***)

Not-so-fancy solutions

- Mutexes
- Semaphores
- Spin locks
- Existence of a file
- Open socket
- Shared memory with integer variable and Compare-and-Swap

TCP is not the only way to talk

Applications can communicate with

- ***Object Linking and Embedding*** (***OLE***) and ***Component Object Model*** (***COM***)
- Network sockets, Unix sockets, Windows sockets
- Data Copy (***WM_COPYDATA***)
- ***Dynamic Data Exchange*** (***DDE***)
- Files and memory-mapped files
- Pipes, mailslots
- Signals
- Serial ports and other devices
- Clipboard
- ***RPC*** with ***Microsoft Interface Definition Language*** (***MIDL***)

Others can run code in our programs

- ***Asynchronous Procedure Call*** (***APC***)
- ***CreateRemoteThread***
- Hooks, DLL-injection

Each thread may have a message loop

- Each message may contain additional data
- We pump messages with ***GetMessage***, ***DispatchMessage***, ***TranslateMessage***, ***PeekMessage***

Anyone can send us a message

- ***PostMessage***, ***PostThreadMessage***, ***SendMessage***

async/await may use the message loop (depending on the synchronization context).

```
typedef struct tagMSG {
  HWND   hwnd;
  UINT   message;
  WPARAM wParam;
  LPARAM lParam;
  DWORD  time;
  POINT  pt;
  DWORD  lPrivate;
} MSG, *PMSG, *NPMSG, *LPMSG;
```

TCP optimizations break applications

Sockets after closing are in ***TIME_WAIT*** state for 2 minutes (can be changed).

Internet Protocol (IP) packages have ***TTL***

- Changing ***TTL*** to higher value may enable tethering in some mobile carriers

Routing table is used for full-tunnel VPN-s

- Can be monitored automatically to prevent tunnel escapes

TCP connections can be routed over various channels

- ***DNS***, ***ICMP***, file systems, serial ports, sound, ***S3***

TCP have many heuristics that may break performance

- ***TCP_NODELAY*** (Nagle's algorithm) that reduces number of packets is one of them
- https://brooker.co.za/blog/2024/05/09/nagle.html

Our code may be changed dynamically

There is no file…

Many ways of storing configuration

- INI files, registry, dotfiles, group policy, environment variables, databases, app configs

They can be redirected

- Windows can run 32-bit applications on 64-bit system with ***WoW64***
- Files get redirected (*C:\Windows\system32* to *C:\Windows\SysWoW64*)
- Registry gets redirected (*HKLM\Software* to *HKLM\Software\Wow6432Node*)

Windows supports many more techniques:

- WoW (to run 16-bit apps on 32-bit systems)
- ARM64EC
- ARM64X

This gets really dirty

- C:\Windows\System
  - 16-bit x86 binaries on 16-bit and 32-bit x86 system
- C:\Windows\System32
  - 32-bit x86 binaries on 32-bit x86 system
  - 64-bit x86 binaries on 64-bit x86 system
  - 64-bit ARM binaries on 64-bit ARM system
- C:\Windows\SysWoW64
  - 32-bit x86 binaries on 64-bit x86 system
  - 32-bit x86 binaries on 64-bit ARM system
- C:\Windows\SysArm32
  - 32-bit ARM binaries on 64-bit ARM system

Compilers turn back time

C# null-check is not explicit (same in other languages).

Syscall parameters are verified implicitly by failing and handling page fault.

JVM can remove the explicit null-check and add it back if there was a ***NullPointerException***.

Many things are just executed inside a ***try-catch*** block.

Compilers can create a time travel.

```
public static void Foo(Class clazz){
    clazz.Method();
}
```

```
Class.Foo(Class)
    L0000: push ebp
    L0001: mov ebp, esp
    L0003: mov eax, [ecx]
    L0005: mov eax, [eax+0x28]
    L0008: call dword ptr [eax+0x10]
    L000b: pop ebp
    L000c: ret
```

We rarely run „just our code”

```
55                      push   ebp
89 e5                   mov    ebp,esp
81 ec 34 12 00 00       sub    esp,0x1234
8b 45 08                mov    eax,DWORD PTR [ebp+0x8]

89 ec                   mov    esp,ebp
5d                      pop    ebp
c3                      ret
```

Frame pointer omission

- We don’t save ***esp*** in ***ebp***
- We save one general register but we decrease eperformance, break the stack traces, and break the exception handling

Devirtualization

- Instead of calling functions with ***callvirt***, we call them directly since we know if there is exactly one implementation

Volatile and double-checked-lock

- Compilers can cache values and break our code

Undefined behavior in C++

- Whole code blocks can be removed

```
81 ec 34 12 00 00       sub    esp,0x1234
8b 84 24 3c 12 00 00    mov    eax,DWORD PTR [esp+0x1234+0x8]


81 c4 34 12 00 00       add    esp,0x1234
c3                      ret
```

CPU is a world on its own

Memory model

- Reads and writes can be reordered. Barriers must be used to stop that from happening (which decreases performance)

Speculative execution

- CPUs may execute both code branches to improve performance

Branch prediction

- Processing an ordered array is faster than unordered one
- https://stackoverflow.com/questions/11227809/why-is-processing-a-sorted-array-faster-than-processing-an-unsorted-array
- This can be exploited (Spectre, Meltdown)

This is a super-super-super-user in Windows

Kernel mode + user mode = RING0 + RING3
- This is how we typically think about security

RING0 + RING3 + RING1 + RING3
- This is how we used to run virtual machines with trap-and-emulate

Root Mode RING0 + RING3 + Non-Root Mode RING0 + RING3
- This is how we run VMs with VT-x. Can be nested with enlightened VMCS

VTL0 + VTL1
- Virtual Secure Mode (VSM) with Virtual Trust Levels (VTLs)

RING -1 + RING -2 + RING -3
- Hypervisor + System Management Mode + Intel Management Engine

Mandatory Integrity Control
- Low – Metro apps
- Medium – regular code
- High – after we elevate with UAC or (g)sudo
- System – system services
- TrustedInstaller – trusted installer service

User „levels”
- Regular user
- Administrator
- SYSTEM
- TrustedInstaller

JobObjects, Silos, Server Silos
- Solutions for Windows Containers

We all follow the crowd

When we don’t see the code, we can’t be sure how things are done.

Typically, there are many „good” ways to do every little thing in software engineering.

However, we don’t reinvent the wheel every single time. We just learn the „best practices” and „software patterns”.

Great minds think alike.

Tools

Seeing the Code

Visual Studio

- Visual Studio can decompile the code automatically starting with VS 2022 17.7 (since August 2023)
  - https://learn.microsoft.com/en-us/visualstudio/debugger/decompilation?view=vs-2022#autodecompile-code
- Works for code exploration and debugging
- You need to disable „Just My Code”

dnSPY

- https://dnspy.co/
- ~200MB binaries
- You can copy it on your production server
- Works for code exploration and debugging
- Uses ILSpy behind the scenes

Low Level Debugging

WinDBG, CDB, NTSD

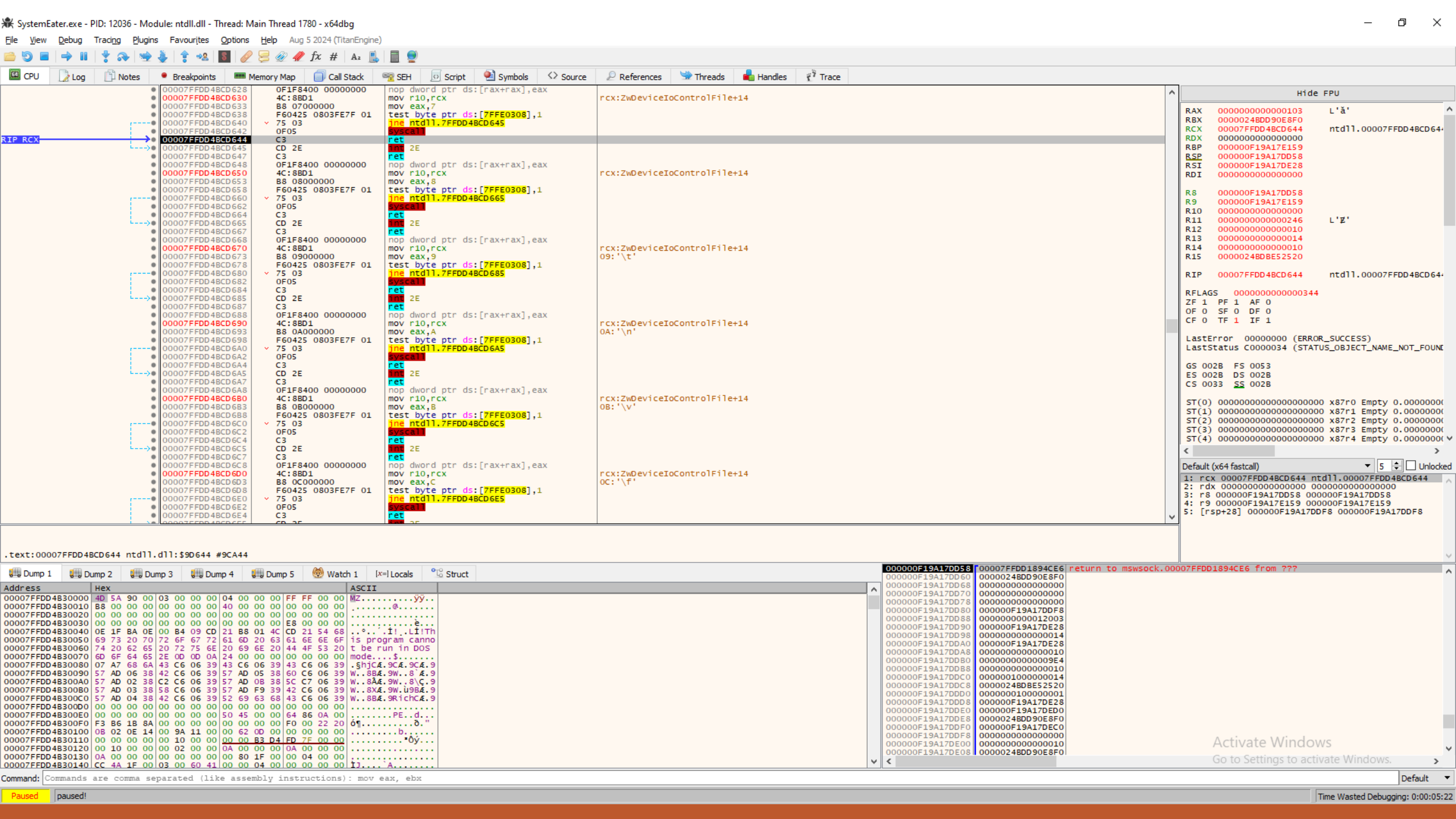
- Generic debuggers with many extensions
- https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools

KD, NTKD

- Kernel debuggers

x64dbg

- More UI-friendly than WinDBG


SystemEater.exe - PID: 12036 - Module: ntdll.dll - Thread: Main Thread 1780 - x64dbg
File View Debug Tracing Plugins Favourites Options Help Aug 5 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
RIP RCX
00007FFDD4BCD644 C3 ret
Hide FPU
RAX 0000000000000103 L'ă'
RBX 0000024BDD90E8F0
RCX 00007FFDD4BCD644 ntdll.00007FFDD4BCD644
RDX 0000000000000000
RBP 000000F19A17E159
RSP 000000F19A17DD58
RSI 000000F19A17DE28
RDI 0000000000000000
R8 000000F19A17DD58
R9 000000F19A17E159
R10 0000000000000000
R11 0000000000000246 L'Ƶ'
R12 0000000000000010
R13 0000000000000014
R14 0000000000000010
R15 0000024BDBE52520
RIP 00007FFDD4BCD644 ntdll.00007FFDD4BCD644
RFLAGS 0000000000000344
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 IF 1
LastError 00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND
GS 002B FS 0053
ES 002B DS 002B
CS 0033 SS 002B
ST(0) 00000000000000000000 x87r0 Empty 0.0000000
ST(1) 00000000000000000000 x87r1 Empty 0.0000000
ST(2) 00000000000000000000 x87r2 Empty 0.0000000
ST(3) 00000000000000000000 x87r3 Empty 0.0000000
ST(4) 00000000000000000000 x87r4 Empty 0.0000000
Default (x64 fastcall)
Unlocked
1: rcx 00007FFDD4BCD644 ntdll.00007FFDD4BCD644
2: rdx 0000000000000000 0000000000000000
3: r8 000000F19A17DD58 000000F19A17DD58
4: r9 000000F19A17E159 000000F19A17E159
5: [rsp+28] 000000F19A17DDF8 000000F19A17DDF8
.text:00007FFDD4BCD644 ntdll.dll:$9D644 #9CA44
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct
Address Hex ASCII
000000F19A17DD58 00007FFDD1894CE6 return to mswsock.00007FFDD1894CE6 from ???
Activate Windows
Go to Settings to activate Windows.
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
paused!
Time Wasted Debugging: 0:00:05:22

SystemEater.exe - PID: 12036 - Module: ntdll.dll - Thread: Main Thread 1780 - x64dbg

File View Debug Tracing Plugins Favourites Options Help Aug 5 2024 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

Thread ID	Address	To	From	Size	Party	Comment
1780 - Main Thread						
	000000F19A17DD58	00007FFDD1894CE6	00007FFDD4BCD644	140	System	ntdll.ZwDeviceIoControlFile+14
	000000F19A17DE98	00007FFDD18A4DA0	00007FFDD1894CE6	90	System	mswsock.00007FFDD1894CE6
	000000F19A17DF28	00007FFDD189FDDB	00007FFDD18A4DA0	1D0	System	mswsock.Tcpip6_WSHGetWildcardSockaddr+4230
	000000F19A17E0F8	00007FFDD305184A	00007FFDD189FDDB	B0	System	mswsock.Tcpip4_WSHSetSocketInformation+5DB
	000000F19A17E1A8	00007FFCAB614EEC	00007FFDD305184A	8	User	ws2_32.sendto+EA
	000000F19A17E1B0	000000000000000C	00007FFCAB614EEC	8	User	00007FFCAB614EEC
	000000F19A17E1B8	0000024BBC694740	000000000000000C	8	User	000000000000000C
	000000F19A17E1C0	0000024BBC694780	0000024BBC694740	8	User	0000024BBC694740
	000000F19A17E1C8	0000000000000000	0000024BBC694780		User	0000024BBC694780
2368						
	000000F19A8FFAB8	00007FFDD2474030	00007FFDD4BCE0B4	2F0	System	ntdll.NtWaitForMultipleObjects+14
	000000F19A8FFDA8	00007FFD0AF60FB9	00007FFDD2474030	C0	User	kernelbase.WaitForMultipleObjectsEx+F0
	000000F19A8FFE68	00007FFD0AF60EB5	00007FFD0AF60FB9	60	User	coreclr.MetaDataGetDispenser+3A769
	000000F19A8FFEC8	00007FFD0AF60D3E	00007FFD0AF60EB5	30	User	coreclr.MetaDataGetDispenser+3A665
	000000F19A8FFEF8	00007FFDD4207374	00007FFD0AF60D3E	30	System	coreclr.MetaDataGetDispenser+3A4EE
	000000F19A8FFF28	00007FFDD4B7CC91	00007FFDD4207374	80	System	kernel32.BaseThreadInitThunk+14
	000000F19A8FFFA8	0000000000000000	00007FFDD4B7CC91		User	ntdll.RtlUserThreadStart+21
3636						
	000000F19A5FFAD8	00007FFDD4B7D407	00007FFDD4BD0FF4	300	System	ntdll.NtWaitForWorkViaWorkerFactory+14
	000000F19A5FFDD8	00007FFDD4207374	00007FFDD4B7D407	30	System	ntdll.TpReleaseCleanupGroupMembers+747
	000000F19A5FFE08	00007FFDD4B7CC91	00007FFDD4207374	80	System	kernel32.BaseThreadInitThunk+14
	000000F19A5FFE88	0000000000000000	00007FFDD4B7CC91		User	ntdll.RtlUserThreadStart+21
10548 - .NET ThreadPool Gate						
	000000F199D1F108	00007FFDD2474030	00007FFDD4BCE0B4	2F0	System	ntdll.NtWaitForMultipleObjects+14
	000000F199D1F3F8	00007FFD0AE9587F	00007FFDD2474030	F0	User	kernelbase.WaitForMultipleObjectsEx+F0
	000000F199D1F4E8	00007FFD0AE956F1	00007FFD0AE9587F	80	User	coreclr.00007FFD0AE9587F
	000000F199D1F568	00007FFD0AE95260	00007FFD0AE956F1	180	User	coreclr.00007FFD0AE956F1
	000000F199D1F6E8	00007FFD07DE8AEA	00007FFD0AE95260	60	User	coreclr.00007FFD0AE95260
	000000F199D1F748	00007FFD07DE978F	00007FFD07DE8AEA	30	User	system.private.corelib.00007FFD07DE8AEA
	000000F199D1F778	00007FFD07DFBBF1	00007FFD07DE978F	150	User	system.private.corelib.00007FFD07DE978F
	000000F199D1F8C8	00007FFD07DE2EAF	00007FFD07DFBBF1	40	User	system.private.corelib.00007FFD07DFBBF1
	000000F199D1F908	00007FFD0AFBAF03	00007FFD07DE2EAF	40	User	system.private.corelib.00007FFD07DE2EAF
	000000F199D1F948	00007FFD0AEB6DAC	00007FFD0AFBAF03	90	User	coreclr.coreclr_shutdown_2+16003
	000000F199D1F9D8	00007FFD0AF9C853	00007FFD0AEB6DAC	60	User	coreclr.00007FFD0AEB6DAC
	000000F199D1FA38	00007FFD0AE936F5	00007FFD0AF9C853	E0	User	coreclr.coreclr_execute_assembly+26723
	000000F199D1FB18	00007FFD0AE935FA	00007FFD0AE936F5	A0	User	coreclr.00007FFD0AE936F5
	000000F199D1FBB8	00007FFD0AE93419	00007FFD0AE935FA	60	User	coreclr.00007FFD0AE935FA
	000000F199D1FC18	00007FFDD4207374	00007FFD0AE93419	30	System	coreclr.00007FFD0AE93419
	000000F199D1FC48	00007FFDD4B7CC91	00007FFDD4207374	80	System	kernel32.BaseThreadInitThunk+14
	000000F199D1FCC8	0000000000000000	00007FFDD4B7CC91		User	ntdll.RtlUserThreadStart+21
14516						
	000000F19A77EE38	00007FFDD2474030	00007FFDD4BCE0B4	2F0	System	ntdll.NtWaitForMultipleObjects+14
	000000F19A77F128	00007FFDD2473F2E	00007FFDD2474030	40	System	kernelbase.WaitForMultipleObjectsEx+F0
	000000F19A77F168	00007FFD0AF7385B	00007FFDD2473F2E	280	User	kernelbase.WaitForMultipleObjects+E
	000000F19A77F3E8	00007FFD0AF737D0	00007FFD0AF7385B	2F0	User	coreclr.MetaDataGetDispenser+4D00B
	000000F19A77F6D8	00007FFD0AF73209	00007FFD0AF737D0	70	User	coreclr.MetaDataGetDispenser+4CF80
	000000F19A77F748	00007FFDD4207374	00007FFD0AF73209	30	System	coreclr.MetaDataGetDispenser+4C9B9
	000000F19A77F778	00007FFDD4B7CC91	00007FFDD4207374	80	System	kernel32.BaseThreadInitThunk+14
	000000F19A77F7F8	0000000000000000	00007FFDD4B7CC91		User	ntdll.RtlUserThreadStart+21
6076						
	000000F19A2FF958	00007FFDD4B7D407	00007FFDD4BD0FF4	300	System	ntdll.NtWaitForWorkViaWorkerFactory+14
	000000F19A2FFC58	00007FFDD4207374	00007FFDD4B7D407	30	System	ntdll.TpReleaseCleanupGroupMembers+747
	000000F19A2FFC88	00007FFDD4B7CC91	00007FFDD4207374	80	System	kernel32.BaseThreadInitThunk+14
	000000F19A2FFD08	0000000000000000	00007FFDD4B7CC91		User	ntdll.RtlUserThreadStart+21
13572						
	000000F19A47F948	00007FFDD4B7D407	00007FFDD4BD0FF4	300	System	ntdll.NtWaitForWorkViaWorkerFactory+14
	000000F19A47FC48	00007FFDD4207374	00007FFDD4B7D407	30	System	ntdll.TpReleaseCleanupGroupMembers+747
	000000F19A47FC78	00007FFDD4B7CC91	00007FFDD4207374	80	System	kernel32.BaseThreadInitThunk+14
	000000F19A47FCF8	0000000000000000	00007FFDD4B7CC91		User	ntdll.RtlUserThreadStart+21
13300 - .NET Finalizer						
	000000F19AA7F538	00007FFDD243920E	00007FFDD4BCD5E4	A0	System	ntdll.NtWaitForSingleObject+14
	000000F19AA7F5D8	00007FFD0AE952E0	00007FFDD243920E	60	User	kernelbase.WaitForSingleObjectEx+8E
	000000F19AA7F638	00007FFD0AE942FD	00007FFD0AE952E0	40	User	coreclr.00007FFD0AE952E0
	000000F19AA7F678	00007FFD0AE94229	00007FFD0AE942FD	30	User	coreclr.00007FFD0AE942FD
	000000F19AA7F6A8	00007FFD0AE936F5	00007FFD0AE94229	E0	User	coreclr.00007FFD0AE94229
	000000F19AA7F788	00007FFD0AE935FA	00007FFD0AE936F5	A0	User	coreclr.00007FFD0AE936F5
	000000F19AA7F828	00007FFD0AF71661	00007FFD0AE935FA	110	User	coreclr.00007FFD0AE935FA
	000000F19AA7F938	00007FFDD4207374	00007FFD0AF71661	30	System	coreclr.MetaDataGetDispenser+4AE11
	000000F19AA7F968	00007FFDD4B7CC91	00007FFDD4207374	80	System	kernel32.BaseThreadInitThunk+14
	000000F19AA7F9E8	0000000000000000	00007FFDD4B7CC91		User	ntdll.RtlUserThreadStart+21
10740 - .NET ThreadPool Worker						
	000000F19AD7F808	00007FFDD247683F	00007FFDD4BCD684	60	System	ntdll.ZwRemoveIoCompletion+14
	000000F19AD7F868	00007FFD07CC8641	00007FFDD247683F	100	User	kernelbase.GetQueuedCompletionStatus+4F
	000000F19AD7F968	00007FFD07DFF255	00007FFD07CC8641	70	User	system.private.corelib.00007FFD07CC8641
	000000F19AD7F9D8	00007FFD07DFF06F	00007FFD07DFF255	60	User	system.private.corelib.00007FFD07DFF255
	000000F19AD7FA38	00007FFD07DFE483	00007FFD07DFF06F	110	User	system.private.corelib.00007FFD07DFF06F
	000000F19AD7FB48	00007FFD07DE2EAF	00007FFD07DFE483	40	User	system.private.corelib.00007FFD07DFE483
	000000F19AD7FB88	00007FFD0AFBAF03	00007FFD07DE2EAF	40	User	system.private.corelib.00007FFD07DE2EAF
	000000F19AD7FBC8	00007FFD0AEB6DAC	00007FFD0AFBAF03	90	User	coreclr.coreclr_shutdown_2+16003

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Default

Paused paused!

Time Wasted Debugging: 0:00:05:14

Decompilers

ILSpy

DotPeek

IDA

Ghidra

We can always use debuggers as decompilers

IDA - SystemEater.exe C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Debug\net6.0\SystemEater.exe

File Edit Jump Search View Debugger Options Windows Help

Local Windows debugger

Library function | Regular function | Instruction | Data | Unexplored | External symbol | Lumina function

Functions

Function name | Seg

_SetThrowImageBase .tex
__CxxFrameHandler4 .tex
__DestructExceptionObject .tex
_CallMemberFunction0(void * const,void * const) .tex
_IsExceptionObjectToBeDestroyed .tex
__AdjustPointer .tex
__FrameUnwindFilter .tex
__current_exception .tex
__current_exception_context .tex
__std_exception_copy .tex
__std_exception_destroy .tex
_get_purecall_handler .tex
_purecall .tex
_CxxThrowException .tex
memcpy_repmovs .tex
memmove .tex
__uncaught_exception .tex
memchr .tex
memset_repmovs .tex
memset .tex
memcmp .tex
__vcrt_initialize .tex
__vcrt_uninitialize .tex
__C_specific_handler .tex
__std_type_info_compare .tex
__vcrt_freefls .tex
__vcrt_getptd .tex
__vcrt_getptd_noexit .tex
__vcrt_getptd_noinit .tex
__vcrt_initialize_ptd .tex
__vcrt_uninitialize_ptd .tex
FrameHandler4::StateFromControlPc(FH4::FuncInfo4 *,... .tex

Line 364 of 521, /BuildCatchObjectInternal___FrameHandler4_

Graph overview

IDA View-A | Hex View-1 | Local Types | Imports | Exports

```
; Attributes: library function static

; void __fastcall BuildCatchObjectInternal___FrameHandler4_(EHExceptionRecord *pExcept, void *pRN, FH4::HandlerType4 *pCatch, const _s_CatchableType *pConv)
BuildCatchObjectInternal___FrameHandler4_ proc near

arg_0= qword ptr  8
arg_8= qword ptr  10h
arg_10= qword ptr  18h

pExcept = rcx
pRN = rdx
pCatch = r8
pConv = r9
; __unwind { // __C_specific_handler
mov     [rsp+arg_0], rbx
mov     [rsp+arg_8], rsi
mov     [rsp+arg_10], rdi
push    r14
sub     rsp, 20h
mov     rdi, pConv
mov     r14, pExcept
xor     ebx, ebx
cmp     [pCatch+4], ebx
jge     short loc_140015BA4
```

```
mov     rsi, pRN
jmp     short loc_140015BAB
```

```
loc_140015BA4:
mov     esi, [pCatch+0Ch]
add     rsi, [pRN]
```

```
loc_140015BAB:
;   __try { // __except at $LN18_1
call    BuildCatchObjectHelperInternal___FrameHandler4_
sub     eax, 1
jz      short loc_140015BF1
```

```
;   __except(1) // owned by 1
call    abort_0
BuildCatchObjectInternal___Fr
```

100.00% (110,46) (1341,537) 00014F7C 0000000140015B7C: BuildCatchObjectInternal___FrameHandler4_ (Synchronized with Hex View-1)

Output

```
  The decompilation hotkey is F5.
  Please check the Edit/Plugins menu for more information.
Using FLIRT signature: Microsoft VisualC v14 64bit runtime
Using FLIRT signature: Microsoft VisualC 64bit universal runtime
Using FLIRT signature: SEH for vc64 7-14
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```


IDC

AU: idle Down Disk: 13GB

CodeBrowser: SystemEater:/SystemEater.exe

File Edit Analysis Graph Navigation Search Select Tools Window Help

Program Trees

SystemEater.exe
Headers
.text
.rdata
.data
.pdata
_RDATA
.rsrc
.reloc
Debug Data
tdb

Program Tree

Symbol Tree

USER32.DLL
Exports
Functions
_
atexit
BuildCatchObject
capture_previous_context
CatchIt<class___FrameHandler4>
do_
entry
ExFilterRethrow
F
Is_bad_exception_allowed
memcmp
operator_new
TypeMatchHelper<class___FrameHandler
use_facet<>
~_Sentry_base
Labels
Classes
Namespaces

Filter:

Data Type M...

Data Types
BuiltInTypes
SystemEater.exe
basetsd.h
CFG
crtdefs.h
Demangler
DOS
ehdata.h
excpt.h
mbstring.h
PDB
PE
std
stdlib.h
time.h
wchar.h
winbase.h
WinDef.h
winnls.h
winnt.h

Filter:

Listing: SystemEater.exe

```
                        LAB_140015646                           XREF[1]:     140015600(j)
140015646 8b 44 d3 10     MOV       EAX,dword ptr [RBX + EstablisherFrame*0x8 + 0x...
14001564a 85 c0           TEST      EAX,EAX
14001564c 74 0c           JZ        LAB_14001565a
14001564e 48 3b f8        CMP       RDI,RAX
140015651 75 24           JNZ       LAB_140015677
140015653 45 85 db        TEST      R11D,R11D
140015656 75 2c           JNZ       LAB_140015684
140015658 eb 1d           JMP       LAB_140015677

                        LAB_14001565a                           XREF[1]:     14001564c(j)
14001565a 8d 46 01        LEA       EAX,[RSI + 0x1]
14001565d b1 01           MOV       ExceptionRecord,0x1
14001565f 41 89 47 48     MOV       dword ptr [R15 + 0x48],EAX
140015663 44 8b 44        MOV       ContextRecord,dword ptr [RBX + EstablisherFram...
          d3 0c
140015668 49 8b d5        MOV       EstablisherFrame,R13
14001566b 4d 03 c4        ADD       ContextRecord,R12
14001566e 41 ff d0        CALL      ContextRecord
140015671 44 8b 0b        MOV       DispatcherContext,dword ptr [RBX]
140015674 41 8b c9        MOV       ExceptionRecord,DispatcherContext

                        LAB_140015677                           XREF[4]:     1400155e9(j), 1400155f6(j),
                                                                             140015651(j), 140015658(j)
140015677 ff c6           INC       ESI
140015679 44 8b c1        MOV       ContextRecord,ExceptionRecord
14001567c 3b f1           CMP       ESI,ExceptionRecord
14001567e 0f 82 56        JC        LAB_1400155da
          ff ff ff

                        LAB_140015684                           XREF[4]:     1400154f4(j), 1400155d1(j),
                                                                             140015644(j), 140015656(j)
140015684 b8 01 00        MOV       EAX,0x1
          00 00

                        LAB_140015689                           XREF[1]:     1400155bf(j)
140015689 4c 8d 5c        LEA       R11=>local_28,[RSP + 0x40]
          24 40
14001568e 49 8b 5b 30     MOV       RBX,qword ptr [R11 + local_res8]
140015692 49 8b 6b 38     MOV       RBP,qword ptr [R11 + local_res10]
140015696 49 8b 73 40     MOV       RSI,qword ptr [R11 + local_res18]
14001569a 49 8b e3        MOV       RSP,R11
14001569d 41 5f           POP       R15
14001569f 41 5e           POP       R14
1400156a1 41 5d           POP       R13
1400156a3 41 5c           POP       R12
1400156a5 5f              POP       RDI
1400156a6 c3              RET

                        LAB_1400156a7                           XREF[1]:     14002606c(*)
1400156a7 cc              INT3

                        ********************************************************************
                        * Library Function - Single Match                                  *
```

Decompile: do_is - (SystemEater.exe)

```
/* Library Function - Multiple Matches With Same Base Name
   protected: virtual bool __cdecl std::ctype<unsigned short>::do_is(short,unsigned short)const
  __ptr64
   protected: virtual bool __cdecl std::ctype<wchar_t>::do_is(short,wchar_t)const __ptr64

  Libraries: Visual Studio 2017 Release, Visual Studio 2019 Release */

bool do_is(longlong param_1,ushort param_2,wchar_t param_3)

{
  ushort uVar1;

  uVar1 = _Getwctype(param_3,(_Ctypevec *)(param_1 + 0x10));
  return (param_2 & uVar1) != 0;
}
```

Console - Scripting

Profilers

Visual Studio Diagnostic Tools

- CPU Profile
  - You need to disable „Show Just My Code” in the CPU Usage pane
  - Shows flamegraphs
- Memory snapshots
- File reads and writes
- Database queries
- Async activities
- Events
- Counters
- https://learn.microsoft.com/en-us/visualstudio/profiling/profiling-feature-tour?view=vs-2022

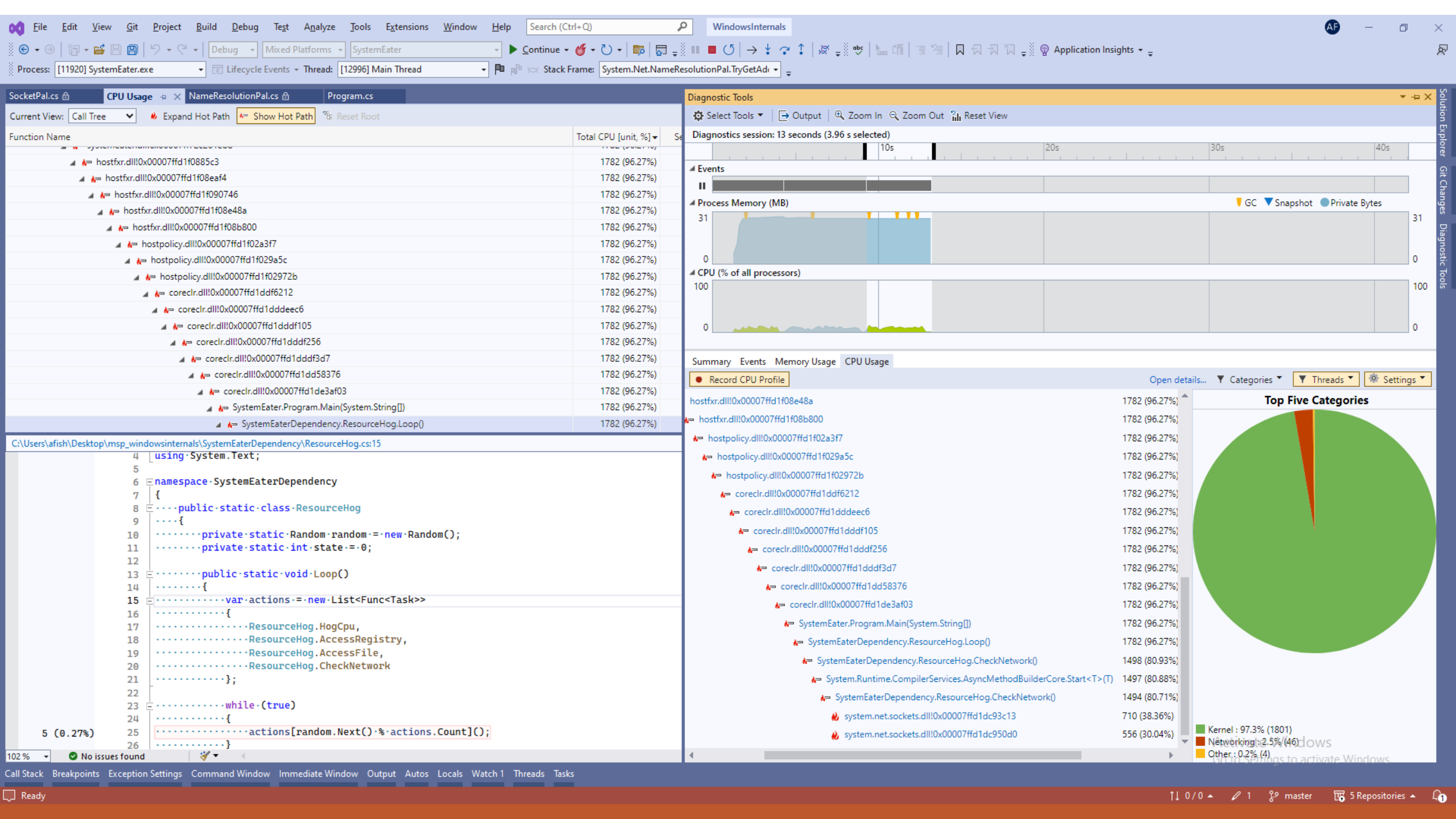
Visual Studio Instrumentation

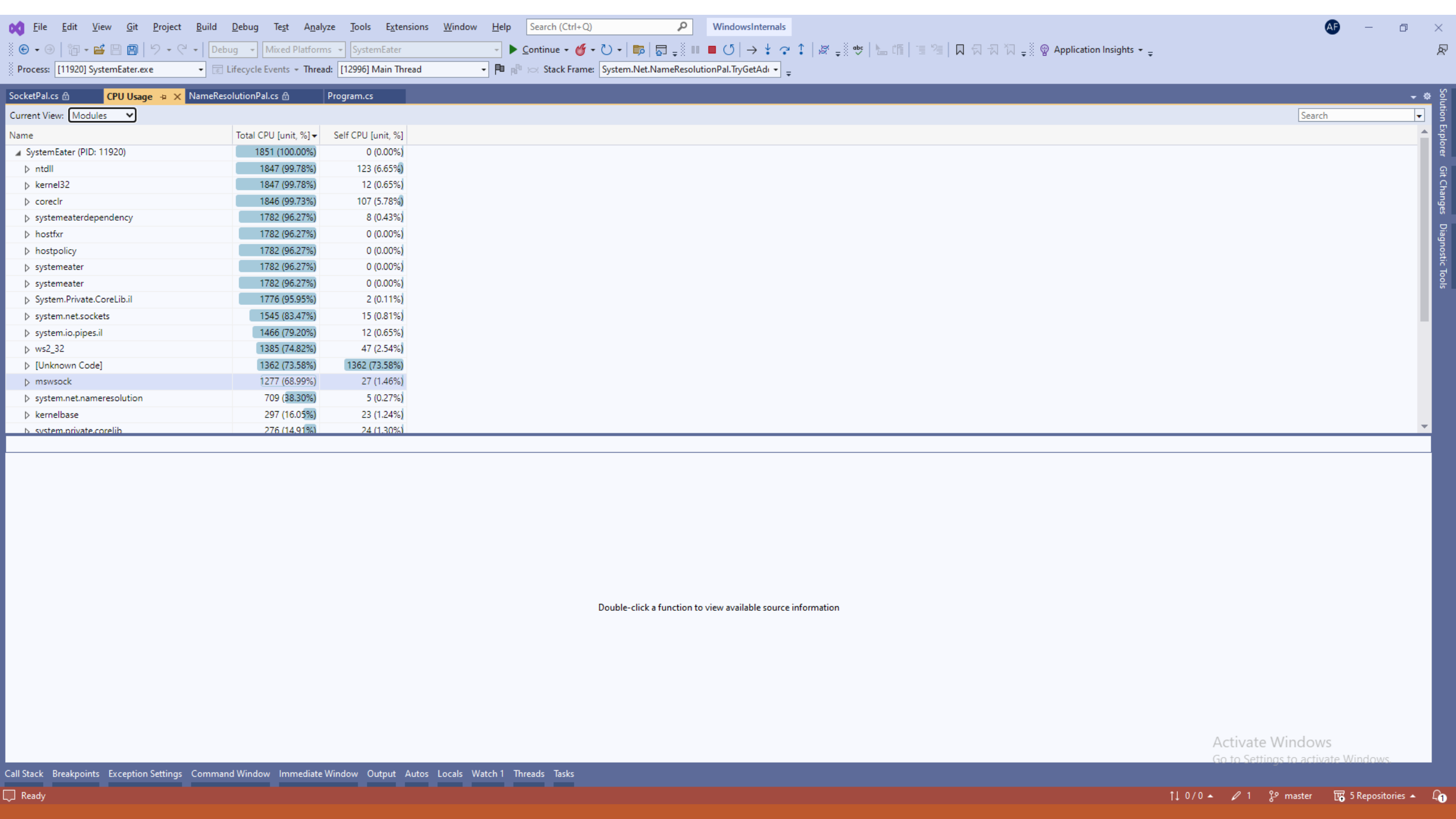
dotnet-trace

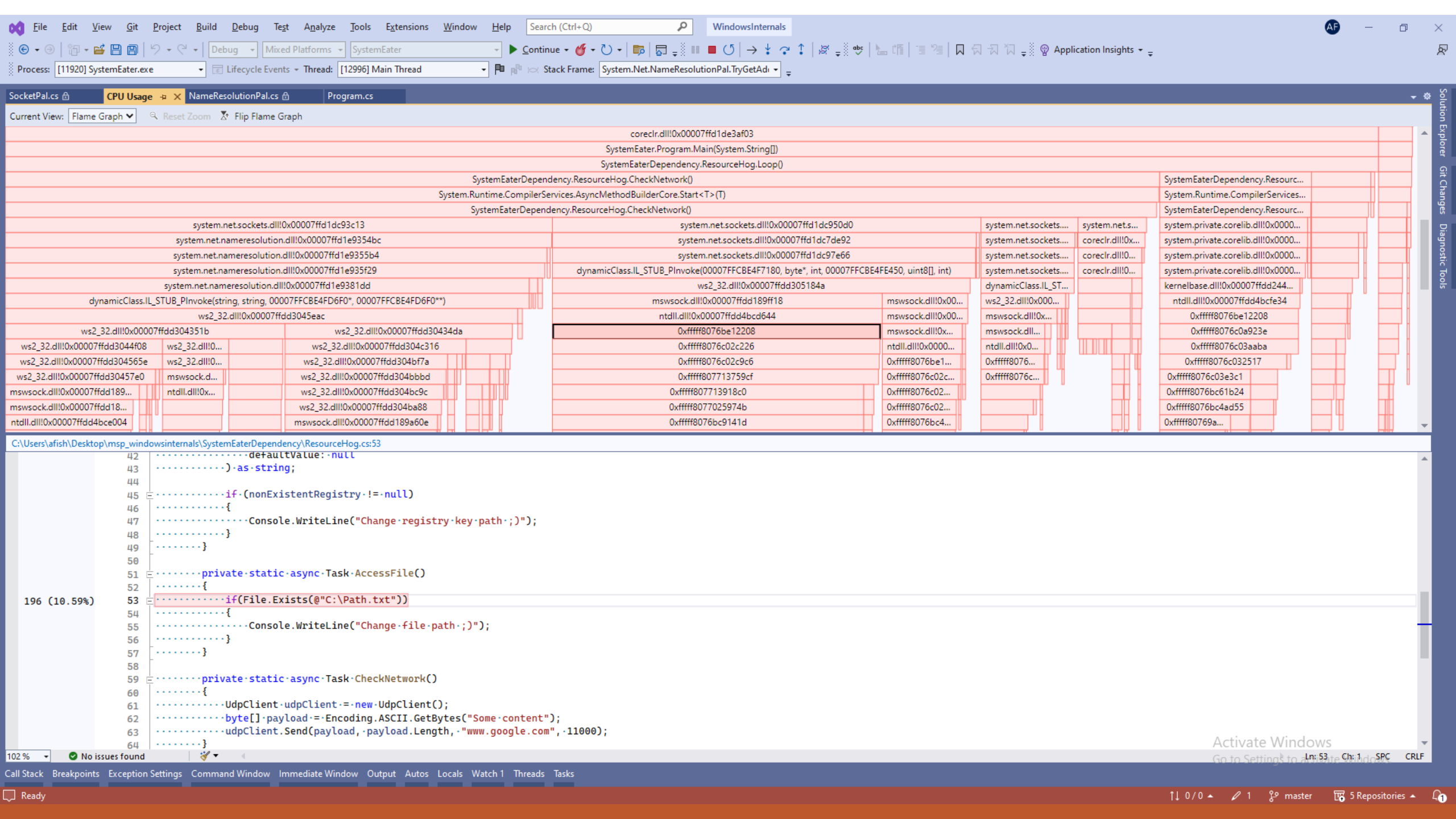
DotTrace

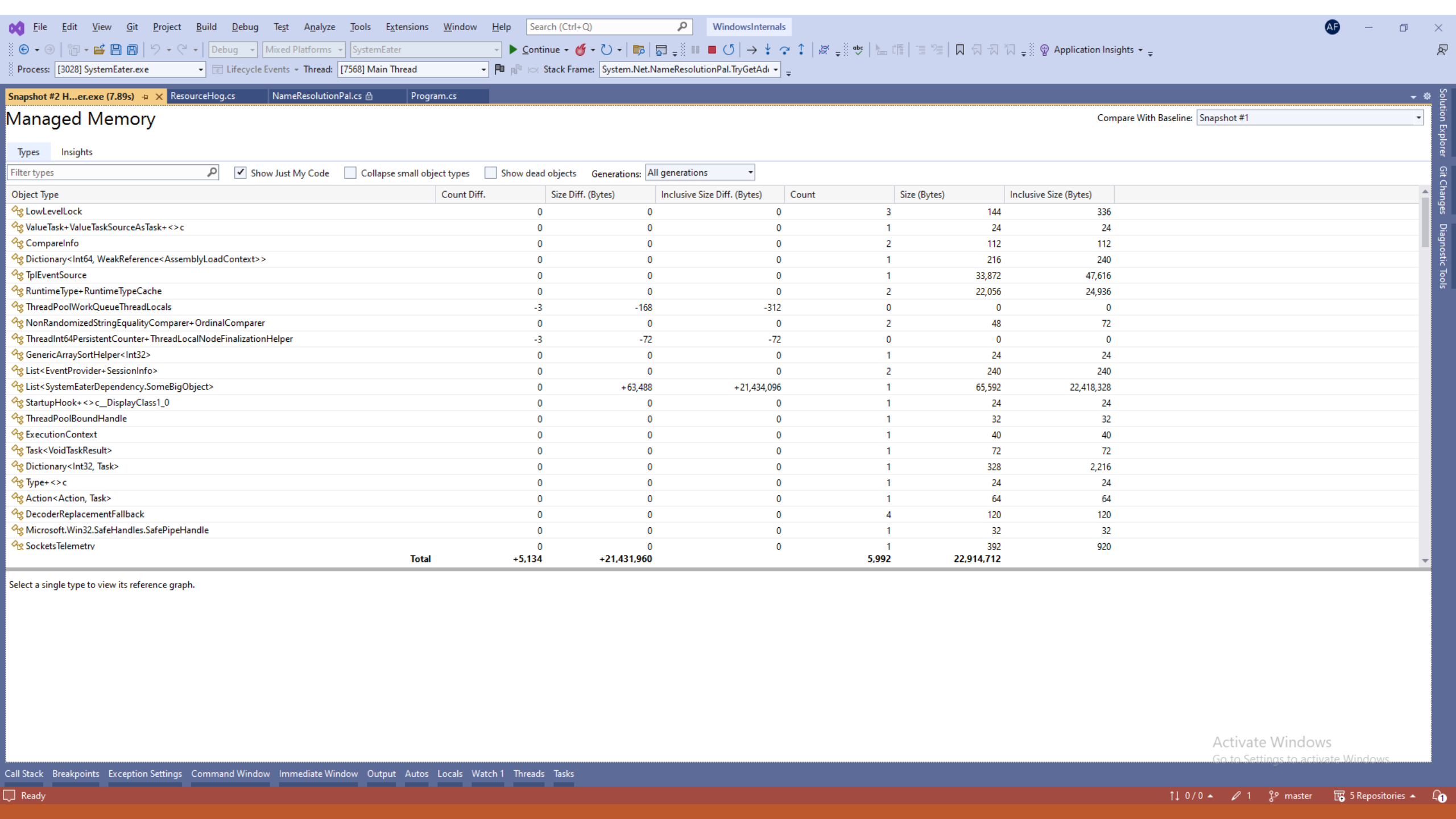
Windows Performance Toolkit

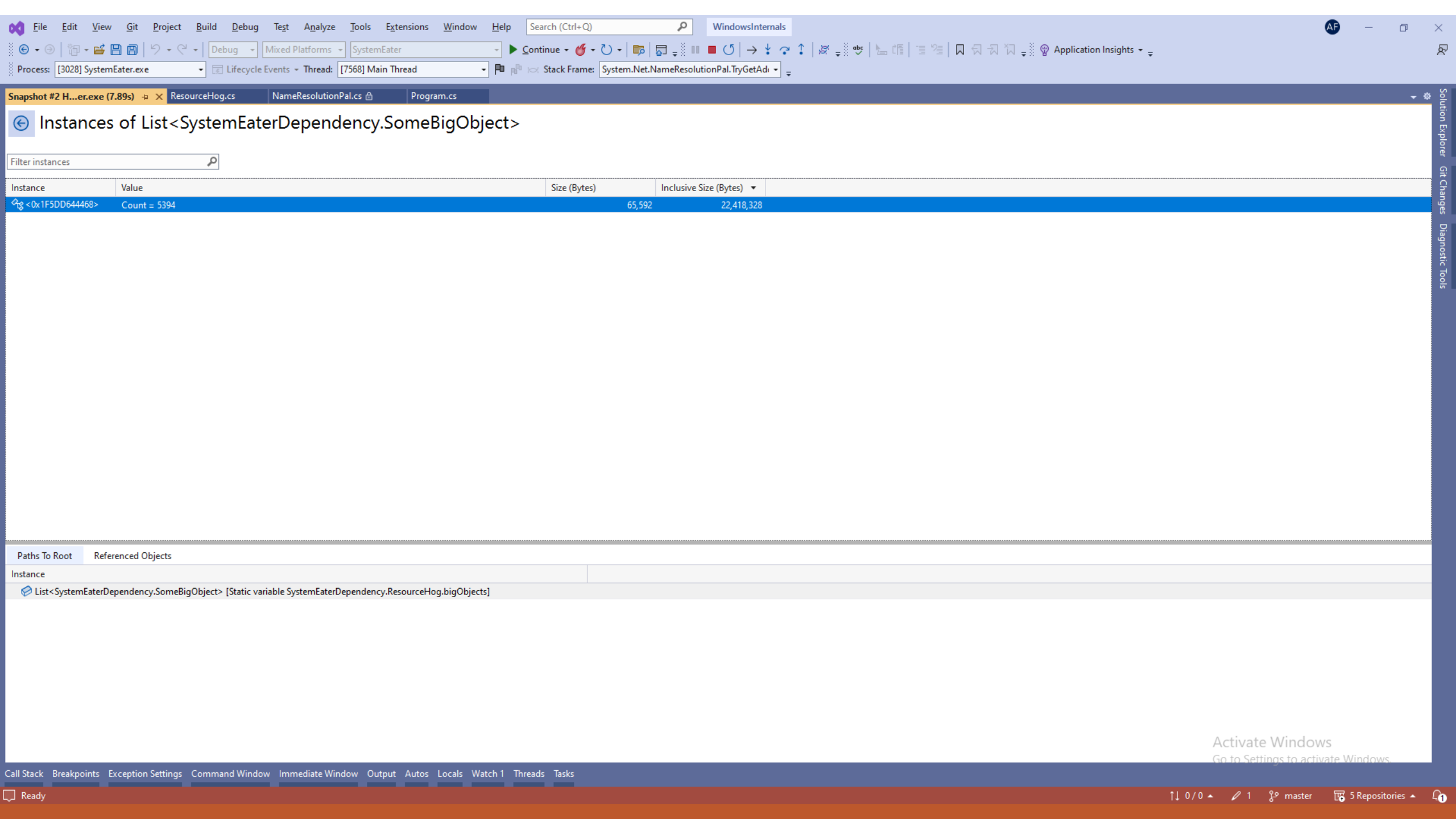
ETW

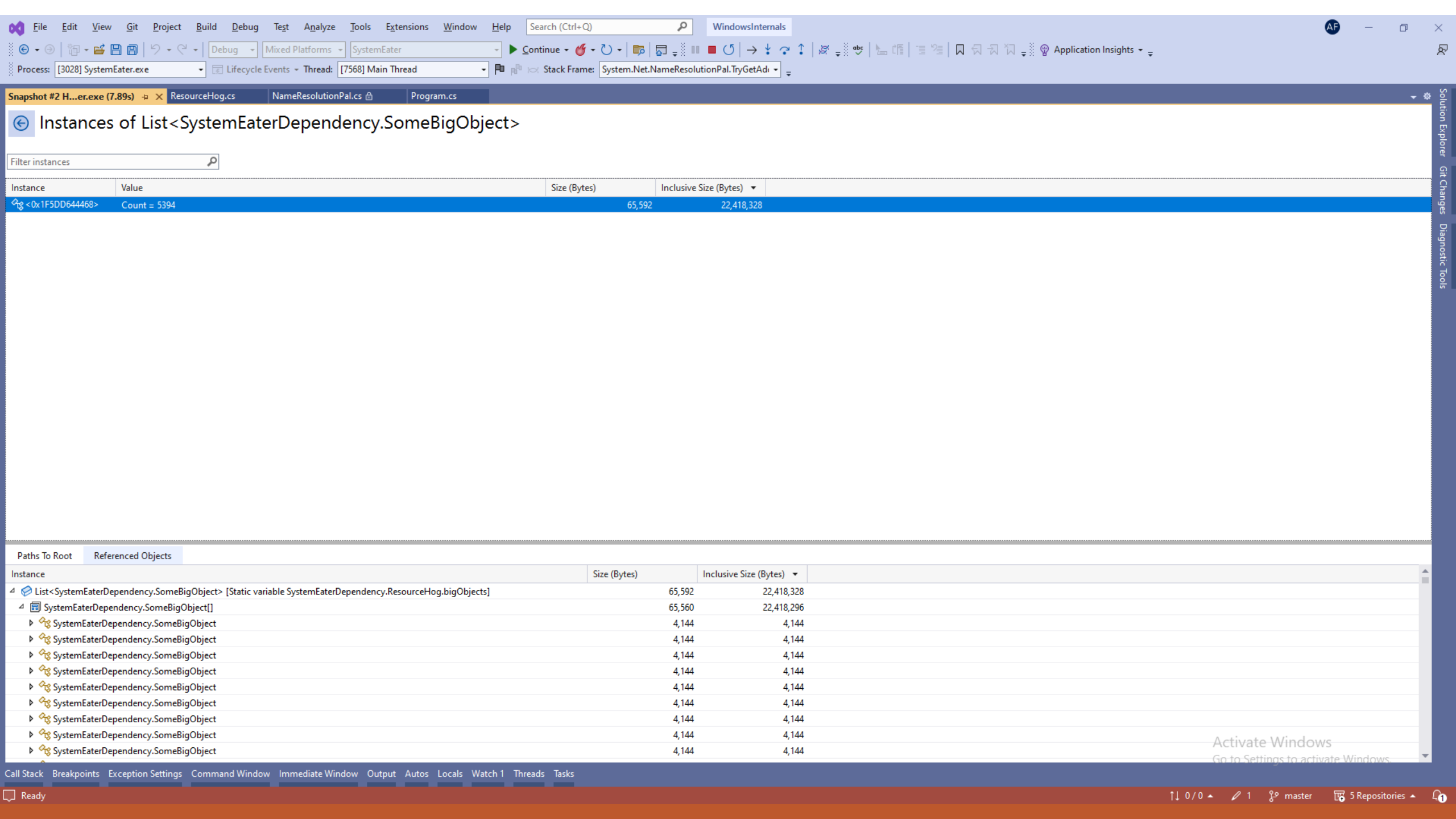

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
Continue
Application Insights
Process: [11920] SystemEater.exe
Lifecycle Events
Thread: [12996] Main Thread
Stack Frame: System.Net.NameResolutionPal.TryGetAd
SocketPal.cs
CPU Usage
NameResolutionPal.cs
Program.cs
Current View: Call Tree
Expand Hot Path
Show Hot Path
Reset Root
Function Name
Total CPU [unit, %]
hostfxr.dll!0x00007ffd1f0885c3 1782 (96.27%)
hostfxr.dll!0x00007ffd1f08eaf4 1782 (96.27%)
hostfxr.dll!0x00007ffd1f090746 1782 (96.27%)
hostfxr.dll!0x00007ffd1f08e48a 1782 (96.27%)
hostfxr.dll!0x00007ffd1f08b800 1782 (96.27%)
hostpolicy.dll!0x00007ffd1f02a3f7 1782 (96.27%)
hostpolicy.dll!0x00007ffd1f029a5c 1782 (96.27%)
hostpolicy.dll!0x00007ffd1f02972b 1782 (96.27%)
coreclr.dll!0x00007ffd1ddf6212 1782 (96.27%)
coreclr.dll!0x00007ffd1dddeec6 1782 (96.27%)
coreclr.dll!0x00007ffd1dddf105 1782 (96.27%)
coreclr.dll!0x00007ffd1dddf256 1782 (96.27%)
coreclr.dll!0x00007ffd1dddf3d7 1782 (96.27%)
coreclr.dll!0x00007ffd1dd58376 1782 (96.27%)
coreclr.dll!0x00007ffd1de3af03 1782 (96.27%)
SystemEater.Program.Main(System.String[]) 1782 (96.27%)
SystemEaterDependency.ResourceHog.Loop() 1782 (96.27%)
C:\Users\afish\Desktop\msp_windowsinternals\SystemEaterDependency\ResourceHog.cs:15
using System.Text;
namespace SystemEaterDependency
{
public static class ResourceHog
{
private static Random random = new Random();
private static int state = 0;
public static void Loop()
{
var actions = new List<Func<Task>>
{
ResourceHog.HogCpu,
ResourceHog.AccessRegistry,
ResourceHog.AccessFile,
ResourceHog.CheckNetwork
};
while (true)
{
actions[random.Next() % actions.Count]();
}
5 (0.27%)
102 %
No issues found
Diagnostic Tools
Select Tools
Output
Zoom In
Zoom Out
Reset View
Diagnostics session: 13 seconds (3.96 s selected)
10s
20s
30s
40s
Events
Process Memory (MB)
GC
Snapshot
Private Bytes
31
0
CPU (% of all processors)
100
0
Summary
Events
Memory Usage
CPU Usage
Record CPU Profile
Open details...
Categories
Threads
Settings
hostfxr.dll!0x00007ffd1f08e48a 1782 (96.27%)
hostfxr.dll!0x00007ffd1f08b800 1782 (96.27%)
hostpolicy.dll!0x00007ffd1f02a3f7 1782 (96.27%)
hostpolicy.dll!0x00007ffd1f029a5c 1782 (96.27%)
hostpolicy.dll!0x00007ffd1f02972b 1782 (96.27%)
coreclr.dll!0x00007ffd1ddf6212 1782 (96.27%)
coreclr.dll!0x00007ffd1dddeec6 1782 (96.27%)
coreclr.dll!0x00007ffd1dddf105 1782 (96.27%)
coreclr.dll!0x00007ffd1dddf256 1782 (96.27%)
coreclr.dll!0x00007ffd1dddf3d7 1782 (96.27%)
coreclr.dll!0x00007ffd1dd58376 1782 (96.27%)
coreclr.dll!0x00007ffd1de3af03 1782 (96.27%)
SystemEater.Program.Main(System.String[]) 1782 (96.27%)
SystemEaterDependency.ResourceHog.Loop() 1782 (96.27%)
SystemEaterDependency.ResourceHog.CheckNetwork() 1498 (80.93%)
System.Runtime.CompilerServices.AsyncMethodBuilderCore.Start<T>(T) 1497 (80.88%)
SystemEaterDependency.ResourceHog.CheckNetwork() 1494 (80.71%)
system.net.sockets.dll!0x00007ffd1dc93c13 710 (38.36%)
system.net.sockets.dll!0x00007ffd1dc950d0 556 (30.04%)
Top Five Categories
Kernel : 97.3% (1801)
Networking : 2.5% (46)
Other : 0.2% (4)
Call Stack
Breakpoints
Exception Settings
Command Window
Immediate Window
Output
Autos
Locals
Watch 1
Threads
Tasks
Ready
0 / 0
1
master
5 Repositories
Solution Explorer
Git Changes
Diagnostic Tools

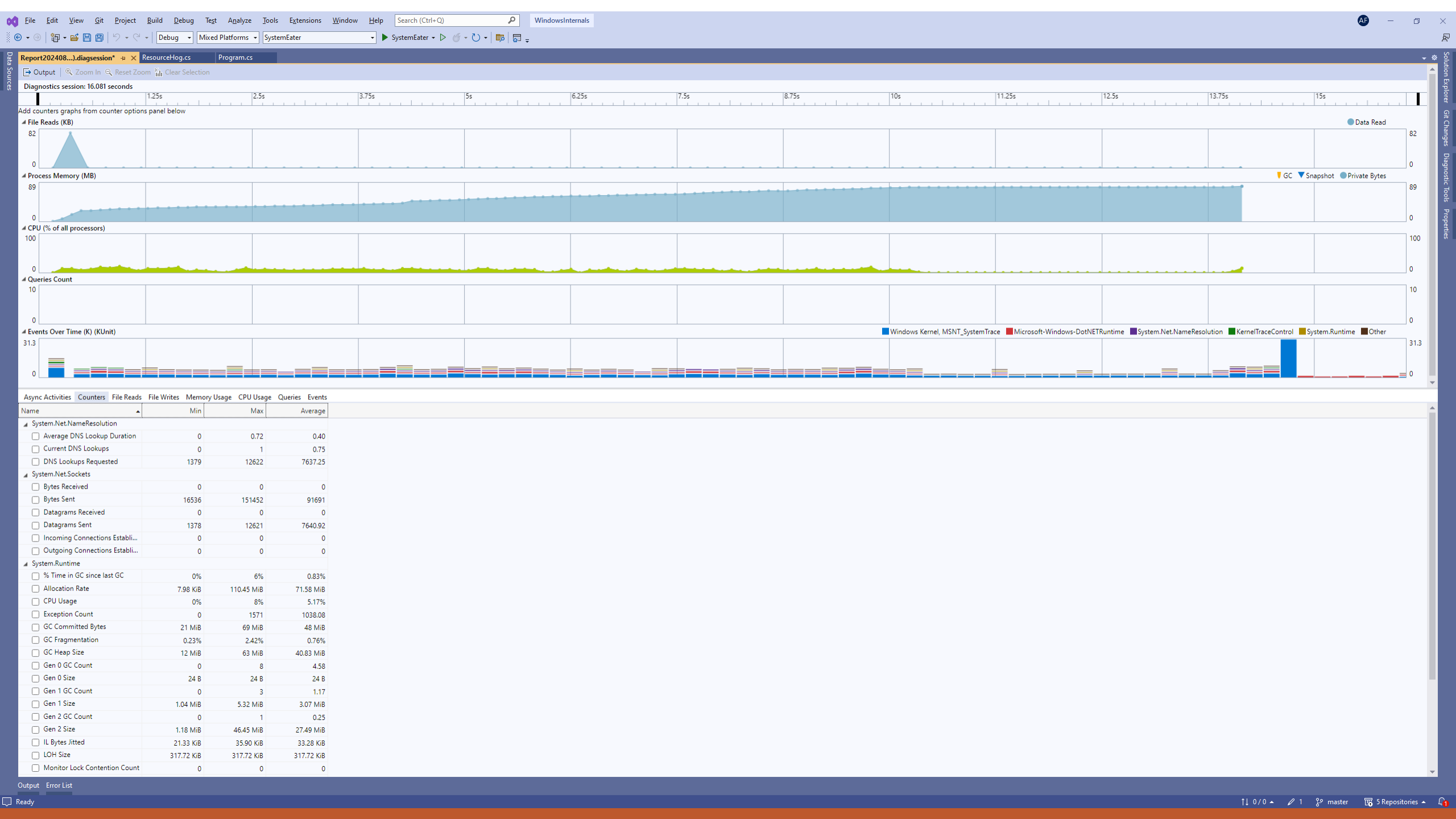

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
Continue
Application Insights
Process: [11920] SystemEater.exe
Lifecycle Events
Thread: [12996] Main Thread
Stack Frame: System.Net.NameResolutionPal.TryGetAd
SocketPal.cs
CPU Usage
NameResolutionPal.cs
Program.cs
Current View: Modules
Search
Name
Total CPU [unit, %]
Self CPU [unit, %]
SystemEater (PID: 11920) 1851 (100.00%) 0 (0.00%)
ntdll 1847 (99.78%) 123 (6.65%)
kernel32 1847 (99.78%) 12 (0.65%)
coreclr 1846 (99.73%) 107 (5.78%)
systemeaterdependency 1782 (96.27%) 8 (0.43%)
hostfxr 1782 (96.27%) 0 (0.00%)
hostpolicy 1782 (96.27%) 0 (0.00%)
systemeater 1782 (96.27%) 0 (0.00%)
systemeater 1782 (96.27%) 0 (0.00%)
System.Private.CoreLib.il 1776 (95.95%) 2 (0.11%)
system.net.sockets 1545 (83.47%) 15 (0.81%)
system.io.pipes.il 1466 (79.20%) 12 (0.65%)
ws2_32 1385 (74.82%) 47 (2.54%)
[Unknown Code] 1362 (73.58%) 1362 (73.58%)
mswsock 1277 (68.99%) 27 (1.46%)
system.net.nameresolution 709 (38.30%) 5 (0.27%)
kernelbase 297 (16.05%) 23 (1.24%)
system.private.corelib 276 (14.91%) 24 (1.30%)
Double-click a function to view available source information
Solution Explorer
Git Changes
Diagnostic Tools
Call Stack
Breakpoints
Exception Settings
Command Window
Immediate Window
Output
Autos
Locals
Watch 1
Threads
Tasks
Ready
master
5 Repositories

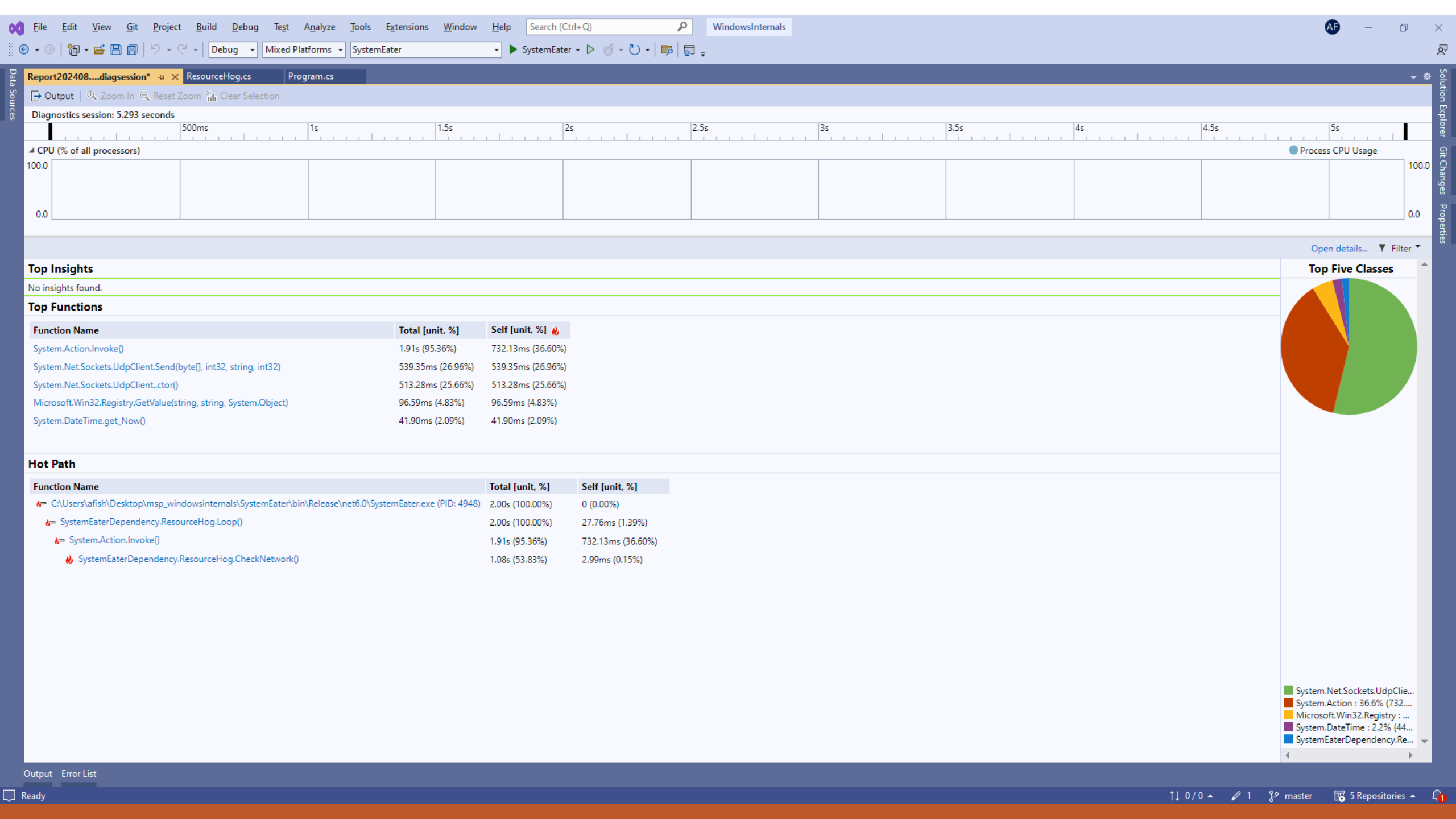

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
Continue
Application Insights
Process: [11920] SystemEater.exe
Lifecycle Events
Thread: [12996] Main Thread
Stack Frame: System.Net.NameResolutionPal.TryGetAdd
SocketPal.cs
CPU Usage
NameResolutionPal.cs
Program.cs
Current View: Flame Graph
Reset Zoom
Flip Flame Graph
coreclr.dll!0x00007ffd1de3af03
SystemEater.Program.Main(System.String[])
SystemEaterDependency.ResourceHog.Loop()
SystemEaterDependency.ResourceHog.CheckNetwork()
System.Runtime.CompilerServices.AsyncMethodBuilderCore.Start<T>(T)
SystemEaterDependency.ResourceHog.CheckNetwork()
system.net.sockets.dll!0x00007ffd1dc93c13
system.net.sockets.dll!0x00007ffd1dc950d0
system.net.nameresolution.dll!0x00007ffd1e9354bc
system.net.sockets.dll!0x00007ffd1dc7de92
system.net.nameresolution.dll!0x00007ffd1e9355b4
system.net.sockets.dll!0x00007ffd1dc97e66
system.net.nameresolution.dll!0x00007ffd1e935f29
dynamicClass.IL_STUB_PInvoke(00007FFCBE4F7180, byte*, int, 00007FFCBE4FE450, uint8[], int)
system.net.nameresolution.dll!0x00007ffd1e9381dd
ws2_32.dll!0x00007ffdd305184a
dynamicClass.IL_STUB_PInvoke(string, string, 00007FFCBE4FD6F0*, 00007FFCBE4FD6F0**)
mswsock.dll!0x00007ffdd189ff18
ws2_32.dll!0x00007ffdd3045eac
ntdll.dll!0x00007ffdd4bcd644
ws2_32.dll!0x00007ffdd304351b
ws2_32.dll!0x00007ffdd30434da
0xfffff8076be12208
ws2_32.dll!0x00007ffdd3044f08
ws2_32.dll!0x00007ffdd304c316
0xfffff8076c02c226
ws2_32.dll!0x00007ffdd304565e
ws2_32.dll!0x00007ffdd304bf7a
0xfffff8076c02c9c6
ws2_32.dll!0x00007ffdd30457e0
ws2_32.dll!0x00007ffdd304bbbd
0xfffff807713759cf
mswsock.dll!0x00007ffdd189...
ws2_32.dll!0x00007ffdd304bc9c
0xfffff807713918c0
mswsock.dll!0x00007ffdd18...
ws2_32.dll!0x00007ffdd304ba88
0xfffff8077025974b
ntdll.dll!0x00007ffdd4bce004
mswsock.dll!0x00007ffdd189a60e
0xfffff8076bc9141d
C:\Users\afish\Desktop\msp_windowsinternals\SystemEaterDependency\ResourceHog.cs:53
196 (10.59%)
if(File.Exists(@"C:\Path.txt"))
Console.WriteLine("Change file path ;)");
private static async Task AccessFile()
private static async Task CheckNetwork()
UdpClient udpClient = new UdpClient();
byte[] payload = Encoding.ASCII.GetBytes("Some content");
udpClient.Send(payload, payload.Length, "www.google.com", 11000);
102 %
No issues found
Ln: 53
Ch: 1
SPC
CRLF
Call Stack
Breakpoints
Exception Settings
Command Window
Immediate Window
Output
Autos
Locals
Watch 1
Threads
Tasks
Ready
master
5 Repositories


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
Continue
Application Insights
Process: [3028] SystemEater.exe
Lifecycle Events
Thread: [7568] Main Thread
Stack Frame: System.Net.NameResolutionPal.TryGetAdd
Snapshot #2 H...er.exe (7.89s)
ResourceHog.cs
NameResolutionPal.cs
Program.cs
Managed Memory
Compare With Baseline: Snapshot #1
Types
Insights
Filter types
Show Just My Code
Collapse small object types
Show dead objects
Generations: All generations
Object Type
Count Diff.
Size Diff. (Bytes)
Inclusive Size Diff. (Bytes)
Count
Size (Bytes)
Inclusive Size (Bytes)
LowLevelLock 0 0 0 3 144 336
ValueTask+ValueTaskSourceAsTask+<>c 0 0 0 1 24 24
CompareInfo 0 0 0 2 112 112
Dictionary<Int64, WeakReference<AssemblyLoadContext>> 0 0 0 1 216 240
TplEventSource 0 0 0 1 33,872 47,616
RuntimeType+RuntimeTypeCache 0 0 0 2 22,056 24,936
ThreadPoolWorkQueueThreadLocals -3 -168 -312 0 0 0
NonRandomizedStringEqualityComparer+OrdinalComparer 0 0 0 2 48 72
ThreadInt64PersistentCounter+ThreadLocalNodeFinalizationHelper -3 -72 -72 0 0 0
GenericArraySortHelper<Int32> 0 0 0 1 24 24
List<EventProvider+SessionInfo> 0 0 0 2 240 240
List<SystemEaterDependency.SomeBigObject> 0 +63,488 +21,434,096 1 65,592 22,418,328
StartupHook+<>c__DisplayClass1_0 0 0 0 1 24 24
ThreadPoolBoundHandle 0 0 0 1 32 32
ExecutionContext 0 0 0 1 40 40
Task<VoidTaskResult> 0 0 0 1 72 72
Dictionary<Int32, Task> 0 0 0 1 328 2,216
Type+<>c 0 0 0 1 24 24
Action<Action, Task> 0 0 0 1 64 64
DecoderReplacementFallback 0 0 0 4 120 120
Microsoft.Win32.SafeHandles.SafePipeHandle 0 0 0 1 32 32
SocketsTelemetry 0 0 0 1 392 920
Total +5,134 +21,431,960 5,992 22,914,712
Select a single type to view its reference graph.
Activate Windows
Go to Settings to activate Windows.
Call Stack Breakpoints Exception Settings Command Window Immediate Window Output Autos Locals Watch 1 Threads Tasks
Ready
master
5 Repositories
Solution Explorer
Git Changes
Diagnostic Tools


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
Continue
Application Insights
Process: [3028] SystemEater.exe
Lifecycle Events
Thread: [7568] Main Thread
Stack Frame: System.Net.NameResolutionPal.TryGetAd
Snapshot #2 H...er.exe (7.89s)
ResourceHog.cs
NameResolutionPal.cs
Program.cs
Instances of List<SystemEaterDependency.SomeBigObject>
Filter instances
Instance
Value
Size (Bytes)
Inclusive Size (Bytes)
<0x1F5DD644468>
Count = 5394
65,592
22,418,328
Paths To Root
Referenced Objects
Instance
List<SystemEaterDependency.SomeBigObject> [Static variable SystemEaterDependency.ResourceHog.bigObjects]
Activate Windows
Go to Settings to activate Windows.
Call Stack
Breakpoints
Exception Settings
Command Window
Immediate Window
Output
Autos
Locals
Watch 1
Threads
Tasks
Ready
master
5 Repositories
Solution Explorer
Git Changes
Diagnostic Tools

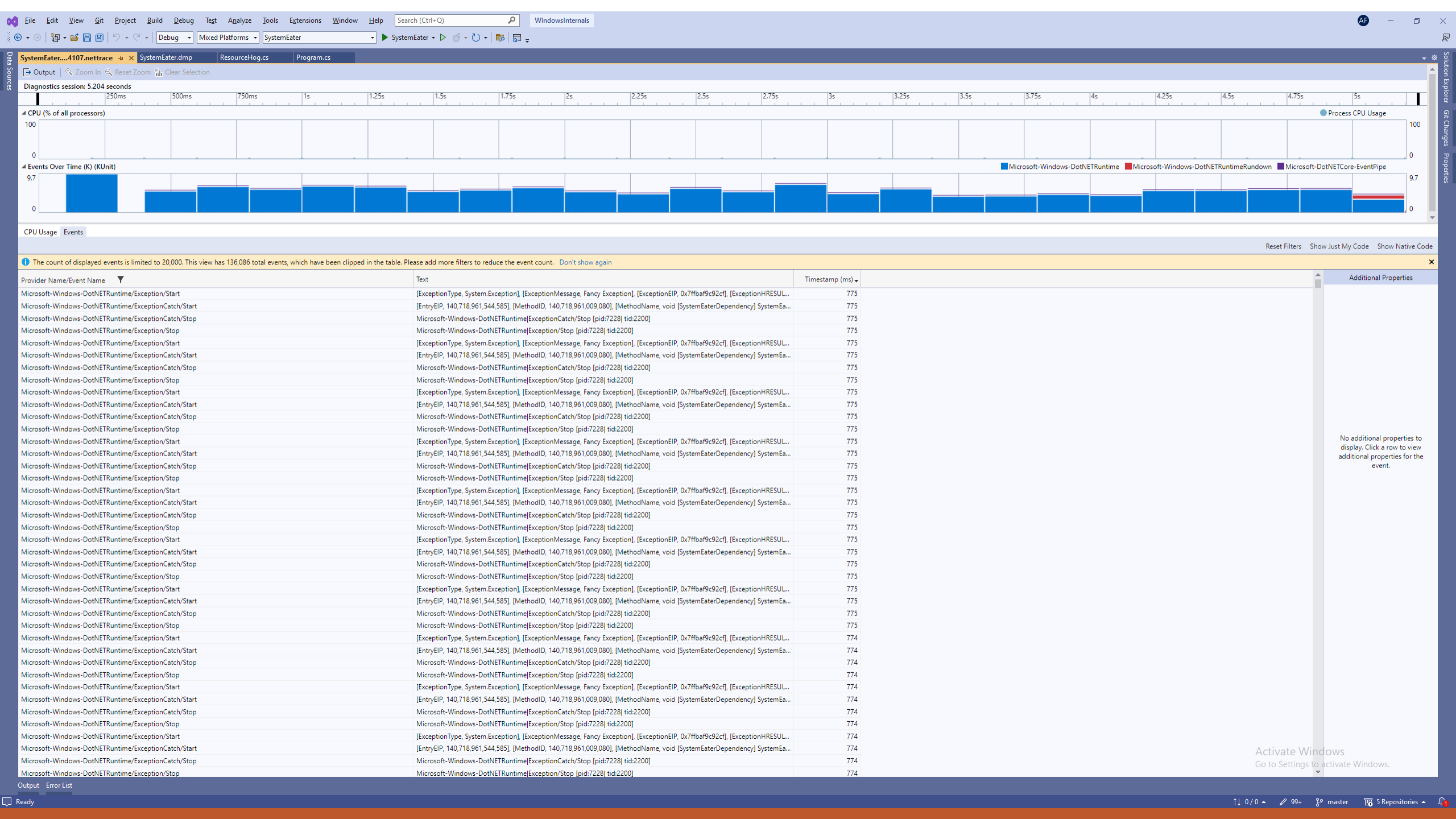

File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
Continue
Application Insights
Process: [3028] SystemEater.exe
Lifecycle Events
Thread: [7568] Main Thread
Stack Frame: System.Net.NameResolutionPal.TryGetAd
Snapshot #2 H...er.exe (7.89s)
ResourceHog.cs
NameResolutionPal.cs
Program.cs
Instances of List<SystemEaterDependency.SomeBigObject>
Filter instances
Instance
Value
Size (Bytes)
Inclusive Size (Bytes)
<0x1F5DD644468>
Count = 5394
65,592
22,418,328
Paths To Root
Referenced Objects
Instance
Size (Bytes)
Inclusive Size (Bytes)
List<SystemEaterDependency.SomeBigObject> [Static variable SystemEaterDependency.ResourceHog.bigObjects]
65,592
22,418,328
SystemEaterDependency.SomeBigObject[]
65,560
22,418,296
SystemEaterDependency.SomeBigObject
4,144
4,144
Solution Explorer
Git Changes
Diagnostic Tools
Call Stack
Breakpoints
Exception Settings
Command Window
Immediate Window
Output
Autos
Locals
Watch 1
Threads
Tasks
Ready
master
5 Repositories


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
SystemEater
Report202408...).diagsession*
ResourceHog.cs
Program.cs
Output
Zoom In
Reset Zoom
Clear Selection
Diagnostics session: 16.081 seconds
1.25s
2.5s
3.75s
5s
6.25s
7.5s
8.75s
10s
11.25s
12.5s
13.75s
15s
Add counters graphs from counter options panel below
File Reads (KB)
Data Read
82
0
Process Memory (MB)
GC
Snapshot
Private Bytes
89
0
CPU (% of all processors)
100
0
Queries Count
10
0
Events Over Time (K) (KUnit)
Windows Kernel, MSNT_SystemTrace
Microsoft-Windows-DotNETRuntime
System.Net.NameResolution
KernelTraceControl
System.Runtime
Other
31.3
0
Async Activities
Counters
File Reads
File Writes
Memory Usage
CPU Usage
Queries
Events
Name
Min
Max
Average
System.Net.NameResolution
Average DNS Lookup Duration 0 0.72 0.40
Current DNS Lookups 0 1 0.75
DNS Lookups Requested 1379 12622 7637.25
System.Net.Sockets
Bytes Received 0 0 0
Bytes Sent 16536 151452 91691
Datagrams Received 0 0 0
Datagrams Sent 1378 12621 7640.92
Incoming Connections Establi... 0 0 0
Outgoing Connections Establi... 0 0 0
System.Runtime
% Time in GC since last GC 0% 6% 0.83%
Allocation Rate 7.98 KiB 110.45 MiB 71.58 MiB
CPU Usage 0% 8% 5.17%
Exception Count 0 1571 1038.08
GC Committed Bytes 21 MiB 69 MiB 48 MiB
GC Fragmentation 0.23% 2.42% 0.76%
GC Heap Size 12 MiB 63 MiB 40.83 MiB
Gen 0 GC Count 0 8 4.58
Gen 0 Size 24 B 24 B 24 B
Gen 1 GC Count 0 3 1.17
Gen 1 Size 1.04 MiB 5.32 MiB 3.07 MiB
Gen 2 GC Count 0 1 0.25
Gen 2 Size 1.18 MiB 46.45 MiB 27.49 MiB
IL Bytes Jitted 21.33 KiB 35.90 KiB 33.28 KiB
LOH Size 317.72 KiB 317.72 KiB 317.72 KiB
Monitor Lock Contention Count 0 0 0
Output
Error List
Ready
master
5 Repositories


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
SystemEater
Report202408....diagsession*
ResourceHog.cs
Program.cs
Output
Zoom In
Reset Zoom
Clear Selection
Diagnostics session: 5.293 seconds
500ms
1s
1.5s
2s
2.5s
3s
3.5s
4s
4.5s
5s
CPU (% of all processors)
Process CPU Usage
100.0
0.0
100.0
0.0
Open details...
Filter
Top Insights
No insights found.
Top Functions
Function Name
Total [unit, %]
Self [unit, %]
System.Action.Invoke()
1.91s (95.36%)
732.13ms (36.60%)
System.Net.Sockets.UdpClient.Send(byte[], int32, string, int32)
539.35ms (26.96%)
539.35ms (26.96%)
System.Net.Sockets.UdpClient..ctor()
513.28ms (25.66%)
513.28ms (25.66%)
Microsoft.Win32.Registry.GetValue(string, string, System.Object)
96.59ms (4.83%)
96.59ms (4.83%)
System.DateTime.get_Now()
41.90ms (2.09%)
41.90ms (2.09%)
Top Five Classes
System.Net.Sockets.UdpClie...
System.Action : 36.6% (732....
Microsoft.Win32.Registry : ...
System.DateTime : 2.2% (44...
SystemEaterDependency.Re...
Hot Path
Function Name
Total [unit, %]
Self [unit, %]
C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Release\net6.0\SystemEater.exe (PID: 4948)
2.00s (100.00%)
0 (0.00%)
SystemEaterDependency.ResourceHog.Loop()
2.00s (100.00%)
27.76ms (1.39%)
System.Action.Invoke()
1.91s (95.36%)
732.13ms (36.60%)
SystemEaterDependency.ResourceHog.CheckNetwork()
1.08s (53.83%)
2.99ms (0.15%)
Output
Error List
Ready
0 / 0
1
master
5 Repositories
Data Sources
Solution Explorer
Git Changes
Properties

C:\Windows\System32\cmd.exe

Top 100 Functions (Exclusive)	Inclusive	Exclusive
1. SafeSocketHandle.DoCloseHandle(bool)	49.16%	49.16%
2. SocketPal.CreateSocket(value class System.Net.Sockets.AddressFamily,va	12.42%	12.42%
3. Socket.SendTo(unsigned int8[],int32,int32,value class System.Net.Socke	12.12%	11.36%
4. Missing Symbol	10.77%	10.77%
5. ResourceHog.ThrowException()	7.4%	7.4%
6. DateTime.get_Now()	4.34%	4.03%
7. RegistryKey.InternalOpenSubKeyCore(class System.String,bool)	3.24%	3.24%
8. SocketPal.SendTo(class System.Net.Sockets.SafeSocketHandle,value class	0.74%	0.74%
9. DateTime.get_UtcNow()	0.23%	0.23%
10. Socket.Dispose(bool)	49.24%	0.08%
11. EventSource.Initialize(value class System.Guid,class System.String,cla	0.28%	0.04%
12. Buffer._Memmove(unsigned int8&,unsigned int8&,unsigned int)	0.04%	0.04%
13. Program.Main(class System.String[])	50.46%	0.04%
14. CastHelpers.StelemRef_Helper(class System.Object&,void*,class System.O	0.04%	0.04%
15. TimeZoneInfo.GetIsDaylightSavingsFromUtc(value class System.DateTime,i	0.03%	0.03%
16. IPAddress.TryParse(class System.String,class System.Net.IPAddress&)	0.04%	0.03%
17. Path.Join(value class System.ReadOnlySpan`1<wchar>,value class System.	0.02%	0.02%
18. __Canon].PopulateProperties(value class Filter,class System.RuntimeTyp	0.02%	0.02%
19. IcuLocaleData.SearchCultureName(class System.String)	0.02%	0.02%
20. Socket.Serialize(class System.Net.EndPoint&)	0.02%	0.02%
21. __Canon].Populate(class System.String,value class MemberListType,value	0.05%	0.02%
22. String.Ctor(wchar*)	0.02%	0.02%
23. AssemblyLoadContext.StartAssemblyLoad(value class System.Guid&,value c	0.28%	0.02%
24. __Canon].Initialize(int32)	0.02%	0.02%
25. EventSource.CreateManifestAndDescriptors(class System.Type,class Syste	0.24%	0.02%
26. RuntimeType.GetMethodCandidates(class System.String,int32,value class	0.02%	0.02%
27. il!Interop.GetRandomBytes(unsigned int8*,int32)	0.02%	0.02%
28. CustomAttribute.FilterCustomAttributeRecord(value class System.Reflect	0.02%	0.02%
29. Random+XoshiroImpl.Next()	0.02%	0.02%
30. ResourceHog.AllocateMemory()	0.02%	0.02%
31. Encoding.GetBytes(class System.String)	0.02%	0.02%
32. Path.GetFullPath(class System.String)	1.19%	0.01%
33. __Canon].get_Keys()	0.01%	0.01%
34. .cctor()	0.01%	0.01%
35. IPv4AddressHelper.ParseNonCanonical(wchar*,int32,int32&,bool)	0.01%	0.01%
36. OrdinalCasing.IndexOf(value class System.ReadOnlySpan`1<wchar>,value c	0.01%	0.01%
37. Array.Resize(!!0[]&,int32)	0.01%	0.01%
38. CustomAttribute.GetCustomAttributes(class System.RuntimeType,class Sys	0.06%	0%
39. RuntimeType.GetFieldCandidates(class System.String,value class System.	0.01%	0%
40. __Canon].PopulateFields(value class Filter)	0.01%	0%
41. __Canon].PopulateProperties(value class Filter)	0.02%	0%
42. Attribute.GetCustomAttribute(class System.Reflection.MemberInfo,class	0.06%	0%
43. __Canon].GetListByName(wchar*,int32,unsigned int8*,int32,value class M	0.03%	0%
44. __Canon].PopulateLiteralFields(value class Filter,class System.Runtime	0.01%	0%
45. RuntimeType.GetPropertyCandidates(class System.String,value class Syst	0.04%	0%
46. RuntimeType.GetPropertyImpl(class System.String,value class System.Ref	0.04%	0%
47. Attribute.GetCustomAttributes(class System.Reflection.MemberInfo,class	0.06%	0%
48. RuntimeType.GetCustomAttributes(class System.Type,bool)	0.06%	0%
49. Type.GetProperty(class System.String,value class System.Reflection.Bin	0.04%	0%
50. __Canon].Add(!0)	0.01%	0%
51. CustomAttribute.AddCustomAttributes(value class ListBuilder`1<class Sy	0.06%	0%
52. CustomAttribute.GetCustomAttributes(class System.Reflection.RuntimeMod	0.06%	0%
53. __Canon].GetMemberList(value class MemberListType,class System.String,	0.05%	0%
54. ManifestBuilder.CreateManifest()	0.05%	0%
55. StringBuilder.CopyTo(int32,value class System.Span`1<wchar>,int32)	0.04%	0%
56. StringBuilder.AppendCore(class System.Text.StringBuilder,int32,int32)	0.04%	0%
57. CultureData.get_LCID()	0.02%	0%
58. CultureData.InitIcuCultureDataCore()	0.02%	0%
59. CultureData.InitCultureDataCore()	0.02%	0%
60. CultureData.CreateCultureData(class System.String,bool)	0.02%	0%
61. CultureData.GetCultureData(class System.String,bool)	0.02%	0%
62. .ctor(class System.String,bool)	0.02%	0%
63. CultureInfo.GetCultureByName(class System.String)	0.02%	0%
64. ManifestBuilder.StartEvent(class System.String,class System.Diagnostic	0.02%	0%
65. CultureInfo.GetUserDefaultCulture()	0.02%	0%
66. CultureInfo.InitializeUserDefaultCulture()	0.02%	0%
67. ManifestBuilder.CreateManifestString()	0.05%	0%
68. CultureInfo.get_CurrentCulture()	0.02%	0%
69. EventSource.GetCustomAttributeHelper(class System.Reflection.MemberInf	0.06%	0%
70. __Canon].TryInsert(!0,!1,value class System.Collections.Generic.Insert	0.02%	0%
71. String.Compare(class System.String,int32,class System.String,int32,int	0.02%	0%
72. RuntimeType.GetMethods(value class System.Reflection.BindingFlags)	0.02%	0%
73. RuntimeParameterInfo.GetParameters(class System.IRuntimeMethodInfo,cla	0.04%	0%
74. RuntimeMethodInfo.FetchNonReturnParameters()	0.04%	0%
75. RuntimeMethodInfo.GetParameters()	0.04%	0%
76. Buffer.Memmove(unsigned int8&,unsigned int8&,unsigned int)	0.04%	0%
77. IcuLocaleData.GetLocaleDataNumericPart(class System.String,value class	0.02%	0%
78. RuntimeType.GetFields(value class System.Reflection.BindingFlags)	0.01%	0%
79. ManifestBuilder.GetTaskName(value class System.Diagnostics.Tracing.Eve	0.02%	0%
80. CultureData.IcuLocaleNameToLCID(class System.String)	0.02%	0%
81. Socket.Finalize()	49.24%	0%
82. EventSource.DoCommand(class System.Diagnostics.Tracing.EventCommandEve	0.24%	0%
83. PathHelper.GetFullPathName(value class System.ReadOnlySpan`1<wchar>,va	0.1%	0%
84. PathHelper.Normalize(class System.String)	1.17%	0%
85. FileSystem.FillAttributeInfo(class System.String,value class WIN32_FIL	9.58%	0%


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
SystemEater
SystemEater....4107.nettrace
SystemEater.dmp
ResourceHog.cs
Program.cs
Output
Zoom In
Reset Zoom
Clear Selection
Diagnostics session: 5.204 seconds
250ms 500ms 750ms 1s 1.25s 1.5s 1.75s 2s 2.25s 2.5s 2.75s 3s 3.25s 3.5s 3.75s 4s 4.25s 4.5s 4.75s 5s
CPU (% of all processors)
Process CPU Usage
100
0
Events Over Time (K) (KUnit)
Microsoft-Windows-DotNETRuntime
Microsoft-Windows-DotNETRuntimeRundown
Microsoft-DotNETCore-EventPipe
9.7
0
CPU Usage
Events
Reset Filters
Show Just My Code
Show Native Code
The count of displayed events is limited to 20,000. This view has 136,086 total events, which have been clipped in the table. Please add more filters to reduce the event count.
Don't show again
Provider Name/Event Name
Text
Timestamp (ms)
Additional Properties
No additional properties to display. Click a row to view additional properties for the event.
Microsoft-Windows-DotNETRuntime/Exception/Start
[ExceptionType, System.Exception], [ExceptionMessage, Fancy Exception], [ExceptionEIP, 0x7ffbaf9c92cf], [ExceptionHRESUL...
775
Microsoft-Windows-DotNETRuntime/ExceptionCatch/Start
[EntryEIP, 140,718,961,544,585], [MethodID, 140,718,961,009,080], [MethodName, void [SystemEaterDependency] SystemEa...
775
Microsoft-Windows-DotNETRuntime/ExceptionCatch/Stop
Microsoft-Windows-DotNETRuntime|ExceptionCatch/Stop [pid:7228| tid:2200]
775
Microsoft-Windows-DotNETRuntime/Exception/Stop
Microsoft-Windows-DotNETRuntime|Exception/Stop [pid:7228| tid:2200]
775
774
Activate Windows
Go to Settings to activate Windows.
Output
Error List
Ready
0 / 0
99+
master
5 Repositories

SystemEater.exe - 8/15/2024, 5:50:10 AM – JetBrains dotTrace Viewer

File Edit View Help

Filters

Events

Not Selected	17,237 ms
.NET Memory Allocations	537 MB
Exceptions	7,941 events
Native Allocations	31,927 KB
Debug Output	2 events
Garbage Collection	76 ms
JIT Compilation	237 ms
File Operations	197 ms

Thread State

	ms	%
Not Selected	17,237 ms	
Running	5,139 ms	29.8
Waiting	12,098 ms	70.2

Subsystems

	ms	%
Native code	12,293 ms	71.3
User code	2,267 ms	13.2
System code	1,432 ms	8.3
File I/O	607 ms	3.5
GC Wait	292 ms	1.7

Timeline

No filters applied

CPU 10.5% GC Wait 1.3% Filtered intervals

out in

0 1 s 2 s 3 s 4 s 5 s 6

ID	Name	↓ ms	↓ %
12864	Main	6,169 ms	35.8
7300	Finalizer	4,620 ms	26.8
12792	JIT Thread	4,549 ms	26.4
13256	Garbage Coll...	1,898 ms	11.0

Visible Threads

SystemEater.exe - 8/15/2024, 5:50:10 AM

Hotspots

Own+System ↓ / Total time | Plain List

Search Functions

71.4 % Stack traces without user methods • 12,312 ms
10.9 % ThrowException • 1,875 ms • SystemEaterDependency.**ResourceHog**.ThrowException()
6.5 % CheckNetwork • 1,126 ms • SystemEaterDependency.**ResourceHog**.CheckNetwork()
3.5 % exe_start • 603 ms / 4,922 ms • **SystemEater.exe!**exe_start
2.6 % AccessFile • 450 ms • SystemEaterDependency.**ResourceHog**.AccessFile()
1.4 % CheckNetwork • 249 ms • SystemEaterDependency.**ResourceHog**.CheckNetwork()
1.0 % ThrowException • 179 ms • SystemEaterDependency.**ResourceHog**.ThrowException()
1.0 % Loop • 164 ms / 4,312 ms • SystemEaterDependency.**ResourceHog**.Loop(Int32)
0.6 % AccessRegistry • 102 ms • SystemEaterDependency.**ResourceHog**.AccessRegistry()
0.5 % AccessFile • 84 ms • SystemEaterDependency.**ResourceHog**.AccessFile()
0.2 % AllocateMemory • 40 ms • SystemEaterDependency.**ResourceHog**.AllocateMemory()
0.2 % AccessRegistry • 29 ms • SystemEaterDependency.**ResourceHog**.AccessRegistry()
0.06 % SomeBigObject..ctor • 10 ms • SystemEaterDependency.**SomeBigObject**..ctor()
0.03 % Main • 5.1 ms / 4,317 ms • SystemEater.**Program**.Main(String[])
0.01 % pre_c_initialization • 1.9 ms • **SystemEater.exe!**pre_c_initialization
<0.01 % pal::load_library • 1.2 ms • **SystemEater.exe!**pal::load_library
<0.01 % init_resb_result • 1.0 ms • **icu.dll!**init_resb_result
<0.01 % HogCpu • 1.0 ms • SystemEaterDependency.**ResourceHog**.HogCpu()
<0.01 % ResourceHog..cctor • 1.0 ms • SystemEaterDependency.**ResourceHog**..cctor()
<0.01 % checkDataItem • 0.9 ms • **icu.dll!**checkDataItem

User code | System co... | Native code

Call Tree

Backtraces | Flame Graph

100 % All Calls • 17,237 ms
28.6 % __scrt_common_main_seh • 4,924 ms • **SystemEater.exe!**__scrt_common_main_seh
28.6 % wmain • 4,922 ms • **SystemEater.exe!**wmain
0.01 % ucrtbase.dll • 1.9 ms

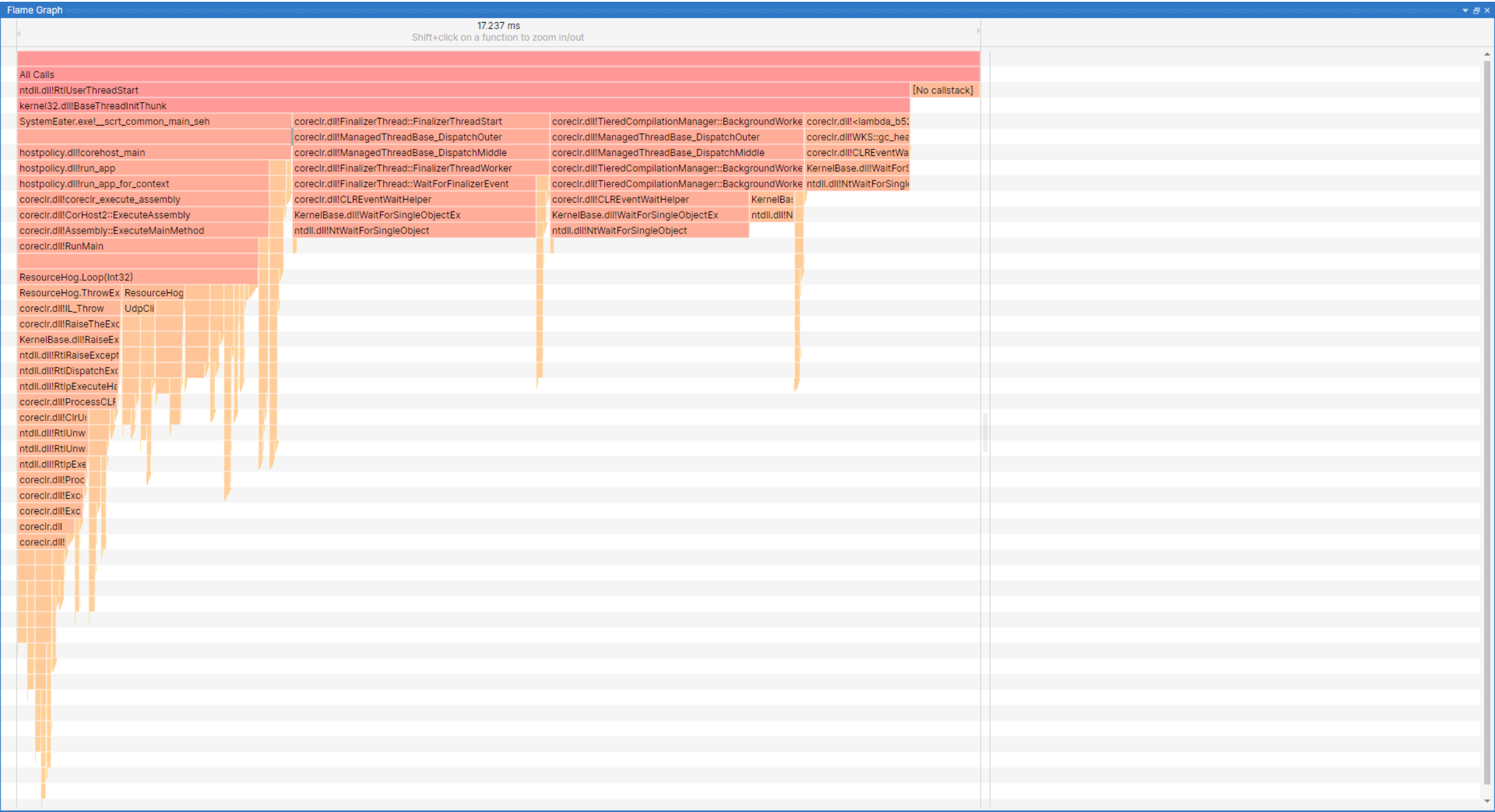
17,237 ms in 4 intervals at 4 threads

Source View

ResourceHog.cs | Decompiled source

Show IL code | Open in Visual Studio

```
45                  "Installed",
46                  defaultValue: null
47              ) as string;
48
49              if (nonExistentRegistry != null)
50              {
51                  Console.WriteLine("Change registry key path ;)");
52              }
53          }
54
55          private static void AccessFile()
56          {
57              if(File.Exists(@"C:\Path.txt"))
58              {
59                  Console.WriteLine("Change file path ;)");
60              }
61          }
62
63          private static void CheckNetwork()
64          {
64              UdpClient udpClient = new UdpClient();
65  53.7%       byte[] payload = Encoding.ASCII.GetBytes("Some content");
66  46.2%       udpClient.Send(payload, payload.Length, "127.0.0.1", 11000);
68          }
69
70          private static void AllocateMemory()
71          {
72              bigObjects.Add(new SomeBigObject());
73          }
74
75          private static void ThrowException()
76          {
77              try
78              {
79                  throw new Exception("Fancy Exception");
80              }
81              catch(Exception e)
82              {
83              }
84          }
```


Flame Graph
17.237 ms
Shift+click on a function to zoom in/out
All Calls
ntdll.dll!RtlUserThreadStart
[No callstack]
kernel32.dll!BaseThreadInitThunk
SystemEater.exe!__scrt_common_main_seh
coreclr.dll!FinalizerThread::FinalizerThreadStart
coreclr.dll!TieredCompilationManager::BackgroundWorke
coreclr.dll!<lambda_b5
coreclr.dll!ManagedThreadBase_DispatchOuter
coreclr.dll!ManagedThreadBase_DispatchOuter
coreclr.dll!WKS::gc_hea
hostpolicy.dll!corehost_main
coreclr.dll!ManagedThreadBase_DispatchMiddle
coreclr.dll!ManagedThreadBase_DispatchMiddle
coreclr.dll!CLREventWa
hostpolicy.dll!run_app
coreclr.dll!FinalizerThread::FinalizerThreadWorker
coreclr.dll!TieredCompilationManager::BackgroundWorke
KernelBase.dll!WaitFor
hostpolicy.dll!run_app_for_context
coreclr.dll!FinalizerThread::WaitForFinalizerEvent
coreclr.dll!TieredCompilationManager::BackgroundWorke
ntdll.dll!NtWaitForSingl
coreclr.dll!coreclr_execute_assembly
coreclr.dll!CLREventWaitHelper
coreclr.dll!CLREventWaitHelper
KernelBa
coreclr.dll!CorHost2::ExecuteAssembly
KernelBase.dll!WaitForSingleObjectEx
KernelBase.dll!WaitForSingleObjectEx
ntdll.dll!N
coreclr.dll!Assembly::ExecuteMainMethod
ntdll.dll!NtWaitForSingleObject
ntdll.dll!NtWaitForSingleObject
coreclr.dll!RunMain
ResourceHog.Loop(Int32)
ResourceHog.ThrowEx
ResourceHog
coreclr.dll!IL_Throw
UdpCli
coreclr.dll!RaiseTheExc
KernelBase.dll!RaiseEx
ntdll.dll!RtlRaiseExcept
ntdll.dll!RtlDispatchExc
ntdll.dll!RtlpExecuteHa
coreclr.dll!ProcessCLR
coreclr.dll!ClrU
ntdll.dll!RtlUnw
ntdll.dll!RtlUnw
ntdll.dll!RtlpExe
coreclr.dll!Proc
coreclr.dll!Exc
coreclr.dll!Exc
coreclr.dll
coreclr.dll!

C:\Users\afish\Desktop\AdditionalTools\Traces\DESKTOP-EIHJ7RK.08-15-2024.06-23-25.etl - Windows® Performance Analyzer

File Trace Profiles Window Help

Graph Explorer - DESKTOP-...

System Activity
Generic Events Activity by Provider, T...

Computation
CPU Usage (Sampled) Utilization by P...
CPU Usage (Attributed) Utilization by...
CPU Usage (Precise) Utilization by Pro...
CPU Usage (Sampled) Utilization by P...
DPC/ISR DPC/ISR Duration by Module...

Storage
Disk Usage Utilization by Disk, Priority

Memory
Memory Utilization Utilization by Cat...

Power

Other

Analysis

CPU Usage (Sampled) Flame by Process, Stack *

Line #	Process	Stack	Count Sum	Weight (in v... Sum	TimeStamp (s)	% Weight Sum	Legend
20		| | coreclr.dll!<Symbols disabled>	5,296	5,087.351400		1.82	
21		| | coreclr.dll!<Symbols disabled>	5,296	5,087.351400		1.82	
22		| | coreclr.dll!<Symbols disabled>	5,296	5,087.351400		1.82	
23		| | SystemEater.dll!SystemEater.Program::Main 0x0	5,296	5,087.351400		1.82	
24		| | SystemEaterDependency.dll!SystemEaterDependency.ResourceHog::Loop 0x0	5,296	5,087.351400		1.82	
25		| | |- SystemEaterDependency.dll!SystemEaterDependency.ResourceHog::CheckNetwork 0x0	2,564	2,464.357500		0.88	
26		| | |- SystemEaterDependency.dll!SystemEaterDependency.ResourceHog::ThrowException 0x0	1,397	1,340.932300		0.48	
27		| | |- SystemEaterDependency.dll!SystemEaterDependency.ResourceHog::AccessFile 0x0	887	849.626700		0.30	
28		| | |- SystemEaterDependency.dll!SystemEaterDependency.ResourceHog::AccessRegistry 0x0	260	251.234900		0.09	

Start: 0.090804500s
End: 34.957842600s
Duration: 34.867038100s

Analysis Assistant My Presets Details

Diagnostic Console Symbols Hub

C:\Users\afish\Desktop\AdditionalTools\Traces\DESKTOP-EIHJ7RK.08-15-2024.06-23-25.etl - Windows® Performance Analyzer

File Trace Profiles Window Help

Graph Explorer - DESKTOP-...

System Activity
Generic Events Activity by Provider, T...

Computation
CPU Usage (Sampled) Utilization by P...
CPU Usage (Attributed) Utilization by...
CPU Usage (Precise) Utilization by Pro...
CPU Usage (Sampled) Utilization by P...
DPC/ISR DPC/ISR Duration by Module...

Storage
Disk Usage Utilization by Disk, Priority

Memory
Memory Utilization Utilization by Cat...
Hard Faults Count
Memory Utilization Utilization by Cat...
Total Commit Process View
No data
Virtual Memory Snapshots Default

Power

Other

Analysis
Analysis (2)

Virtual Memory Snapshots Default

Peak Outstanding Working Set using resource time as [Time,EndTime(internal use)] (Aggregation: Max)

Series
devenv.exe (11508)
PagedPoolWs
ServiceHub.RoslynCod...
SystemEater.exe (6836)
GitExtensions.exe (9660)
PhoneExperienceHost....
explorer.exe (8904)
MsMpEng.exe (5612)

1000000000 B
500000000 B
0 B

Line #	Process	Time (s)	Working Set... Max	Legend
9		2.626919000	134,987,776	
10		3.126984700	145,448,960	
11		3.643665100	155,131,904	
12		4.144119000	164,323,328	
13		4.661963200	171,859,968	
14		5.173810900	180,858,880	
15		5.674542500	190,513,152	
16		6.175902900	200,757,248	
17		7.081396400	214,003,712	

Start: 0.090804500s
End: 34.957842600s
Duration: 34.867038100s

Analysis Assistant
My Presets
Details

Diagnostic Console
Symbols Hub

Strace

Process Monitor

API Monitor

Process Monitor - C:\Users\afish\Desktop\AdditionalTools\Traces\Logfile.PML

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
6:01:3...	SystemEater.exe	7320	CreateFile	C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Release\net6.0	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7fff78b70000, Image Size: 0xc1000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7fff77e80000, Image Size: 0x2d000
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys	REPARSE	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled	NAME NOT FOUND	Length: 80
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers	SUCCESS	
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Query Value
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem\	REPARSE	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\System\CurrentControlSet\Control\FileSystem\LongPathsEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS	
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7fff789d0000, Image Size: 0x19d000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\win32u.dll	SUCCESS	Image Base: 0x7fff77c50000, Image Size: 0x22000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x7fff78180000, Image Size: 0x2b000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\gdi32full.dll	SUCCESS	Image Base: 0x7fff77c80000, Image Size: 0x117000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\msvcp_win.dll	SUCCESS	Image Base: 0x7fff77800000, Image Size: 0x9d000
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\ucrtbase.dll	SUCCESS	Image Base: 0x7fff77ab0000, Image Size: 0x100000
6:01:3...	SystemEater.exe	7320	Thread Create		SUCCESS	Thread ID: 7584
6:01:3...	SystemEater.exe	7320	Thread Create		SUCCESS	Thread ID: 13952
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\shell32.dll	SUCCESS	Image Base: 0x7fff78d70000, Image Size: 0x76f000
6:01:3...	SystemEater.exe	7320	Thread Create		SUCCESS	Thread ID: 11028
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7fff79890000, Image Size: 0xb0000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x7fff78420000, Image Size: 0x9e000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7fff796f0000, Image Size: 0xa0000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7fff78290000, Image Size: 0x123000
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\bcrypt.dll	SUCCESS	Image Base: 0x7fff77c20000, Image Size: 0x27000
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	REPARSE	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\(Default)	SUCCESS	Type: REG_SZ, Length: 18, Data: 00060305
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\000603xx	SUCCESS	Type: REG_SZ, Length: 26, Data: kernel32.dll
6:01:3...	SystemEater.exe	7320	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open...
6:01:3...	SystemEater.exe	7320	QueryBasicInfor...	C:\Windows\System32\imm32.dll	SUCCESS	CreationTime: 6/15/2024 11:27:07 PM, LastAcces...
6:01:3...	SystemEater.exe	7320	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
6:01:3...	SystemEater.exe	7320	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: Read Data/List Directory, Synchr...
6:01:3...	SystemEater.exe	7320	CreateFileMapp...	C:\Windows\System32\imm32.dll	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtectio...
6:01:3...	SystemEater.exe	7320	QueryStandardI...	C:\Windows\System32\imm32.dll	SUCCESS	AllocationSize: 188,416, EndOfFile: 184,432, Numb...
6:01:3...	SystemEater.exe	7320	CreateFileMapp...	C:\Windows\System32\imm32.dll	SUCCESS	SyncType: SyncTypeOther
6:01:3...	SystemEater.exe	7320	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
6:01:3...	SystemEater.exe	7320	Load Image	C:\Windows\System32\imm32.dll	SUCCESS	Image Base: 0x7fff79860000, Image Size: 0x2f000
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument\	REPARSE	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SystemEater.exe	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SystemEater.exe	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Display	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles	NAME NOT FOUND	Length: 20
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableUmpdBufferSizeCheck	NAME NOT FOUND	Length: 20
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SystemEater.exe	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKCU\Control Panel\Desktop\EnablePerProcessSystemDPI	NAME NOT FOUND	Length: 20
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\SystemEater	NAME NOT FOUND	Length: 172
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility	NAME NOT FOUND	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, Granted Acces...
6:01:3...	SystemEater.exe	7320	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	Desired Access: Read
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SystemEater.exe	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
6:01:3...	SystemEater.exe	7320	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
6:01:3...	SystemEater.exe	7320	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
6:01:3...	SystemEater.exe	7320	QueryNameInfo...	C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Release\net6.0\SystemEater.exe	SUCCESS	Name: \Users\afish\Desktop\msp_windowsinterna...

Showing 15,005 of 18,312 events (81%) Backed by C:\Users\afish\Desktop\AdditionalTools\Traces\Logfile.PML

Monitoring - API Monitor v2 64-bit

File Edit View Filter Tools Window Help

API Filter

All Modules

- Additional Resources
- Application Installation and Servicing
- Audio and Video
- Component Object Model (COM)
- Data Access and Storage
- Delta Compression
- Devices
- Diagnostics
- Documents and Printing
- Graphics and Gaming
- Internet
- Microsoft .NET
- NT Native
- Netscape Portable Runtime
- Network Security Services (NSS)
- Networking
- Office Development
- Scripting Runtime Library
- Security and Identity
- System Administration
- System Services
- Undocumented (UnDoc'd)
- Virtualization
- Visual C++ Run-Time Library
- Web Development
- Windows Application UI Development
- Windows Data Types
- Windows Driver Kit
- Windows Environment Development
- Wireless Networking

Capture | Display | External DLL

Running Processes

Process	PID
backgroundTaskHost....	3484
devenv.exe	11508
dllhost.exe	10832
explorer.exe	8904
GitExtensions.exe	9660
Microsoft.ServiceHub....	10504
msedge.exe	2680
msedge.exe	10644
msedge.exe	4884
msedge.exe	4856
msedge.exe	11236
PerfWatson2.exe	11772
PhoneExperienceHost....	10764
rdpclip.exe	8032
RtkAudUService64.exe	2224
RuntimeBroker.exe	9644
RuntimeBroker.exe	10032
RuntimeBroker.exe	11060
RuntimeBroker.exe	13148
SearchApp.exe	9876
SecurityHealthSystray....	10756
ServiceHub.Host.AnyC...	5416
ServiceHub.Host.dotn...	12460
ServiceHub.IndexingS...	10820

Processes | Services

Monitored Processes

C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\

Summary | 26,536 calls | 9.15 MB used | SystemEater.exe

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
11581	6:51:42.284 AM	4	coreclr.dll	setsockopt (1052, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000004
11582	6:51:42.284 AM	4	coreclr.dll	closesocket (1052)	0		0.0000091
11583	6:51:42.284 AM	4	coreclr.dll	setsockopt (1500, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000003
11584	6:51:42.284 AM	4	coreclr.dll	closesocket (1500)	0		0.0000135
11585	6:51:42.284 AM	4	coreclr.dll	setsockopt (1504, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000006
11586	6:51:42.284 AM	4	coreclr.dll	closesocket (1504)	0		0.0000100
11587	6:51:42.284 AM	4	coreclr.dll	setsockopt (1524, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000009
11588	6:51:42.284 AM	4	coreclr.dll	closesocket (1524)	0		0.0000128
11589	6:51:42.284 AM	4	coreclr.dll	setsockopt (1588, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000006
11590	6:51:42.284 AM	4	coreclr.dll	closesocket (1588)	0		0.0000159
11591	6:51:42.284 AM	4	coreclr.dll	setsockopt (1160, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000006
11592	6:51:42.284 AM	4	coreclr.dll	closesocket (1160)	0		0.0000146
11593	6:51:42.284 AM	4	coreclr.dll	setsockopt (1852, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000010
11594	6:51:42.284 AM	4	coreclr.dll	closesocket (1852)	0		0.0000137
11595	6:51:42.284 AM	1	coreclr.dll	WSASocketW (AF_INET, SOCK_DGRAM, IPPROTO_UDP, NULL, 0, WSA_FLA...	1752		0.0000430
11596	6:51:42.284 AM	4	coreclr.dll	setsockopt (1652, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000004
11597	6:51:42.284 AM	4	coreclr.dll	closesocket (1652)	0		0.0000163
11598	6:51:42.284 AM	4	coreclr.dll	setsockopt (1972, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000003
11599	6:51:42.284 AM	4	coreclr.dll	closesocket (1972)	0		0.0000131
11600	6:51:42.284 AM	1	coreclr.dll	sendto (1752, 0x000001db80b5bf28, 12, 0, 0x000001db80b5bfe0, 16)	12		0.0000345
11601	6:51:42.284 AM	1	mswsock.dll	└ntohs (63530)	11000		0.0000001
11602	6:51:42.284 AM	4	coreclr.dll	setsockopt (896, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000003
11603	6:51:42.284 AM	4	coreclr.dll	closesocket (896)	0		0.0000616
11604	6:51:42.284 AM	4	coreclr.dll	setsockopt (1528, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000005
11605	6:51:42.284 AM	4	coreclr.dll	closesocket (1528)	0		0.0000131
11606	6:51:42.284 AM	4	coreclr.dll	setsockopt (1420, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000005
11607	6:51:42.284 AM	1	coreclr.dll	WSASocketW (AF_INET, SOCK_DGRAM, IPPROTO_UDP, NULL, 0, WSA_FLA...	1904		0.0000220
11608	6:51:42.284 AM	4	coreclr.dll	closesocket (1420)	0		0.0000141
11609	6:51:42.284 AM	4	coreclr.dll	setsockopt (948, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000007
11610	6:51:42.284 AM	1	coreclr.dll	sendto (1904, 0x000001db80b6c120, 12, 0, 0x000001db80b6c1d8, 16)	12		0.0000317
11611	6:51:42.284 AM	4	coreclr.dll	closesocket (948)	0		0.0000135
11612	6:51:42.284 AM	1	mswsock.dll	└ntohs (63530)	11000		0.0000000
11613	6:51:42.284 AM	4	coreclr.dll	setsockopt (1324, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000004
11614	6:51:42.284 AM	4	coreclr.dll	closesocket (1324)	0		0.0000141
11615	6:51:42.284 AM	4	coreclr.dll	setsockopt (1196, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000009
11616	6:51:42.284 AM	4	coreclr.dll	closesocket (1196)	0		0.0000179
11617	6:51:42.284 AM	4	coreclr.dll	setsockopt (1396, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000009
11618	6:51:42.284 AM	4	coreclr.dll	closesocket (1396)	0		0.0000168
11619	6:51:42.284 AM	4	coreclr.dll	setsockopt (928, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000005
11620	6:51:42.284 AM	1	coreclr.dll	WSASocketW (AF_INET, SOCK_DGRAM, IPPROTO_UDP, NULL, 0, WSA_FLA...	1392		0.0000172
11621	6:51:42.284 AM	4	coreclr.dll	closesocket (928)	0		0.0000176
11622	6:51:42.284 AM	1	coreclr.dll	sendto (1392, 0x000001db80b7e898, 12, 0, 0x000001db80b7e950, 16)	12		0.0000367
11623	6:51:42.284 AM	4	coreclr.dll	setsockopt (1924, SOL_SOCKET, SO_LINGER, 0x00000080c247f8c8, 4)	SOCKET_ERROR	10042 = An unknown, invalid, or unsupported option or level was specified in a getsockopt...	0.0000015
11624	6:51:42.284 AM	4	coreclr.dll	closesocket (1924)	0		0.0000167

Parameters: sendto (Ws2_32.dll)

#	Type	Name	Pre-Call Value	Post-Call Value
1	SOCKET	s	1904	1904
2	const char*	buf	0x000001db80b6c120	0x000001db80b6c120
3	int	len	12	12
4	int	flags	0	0
5	const struct so...	to	0x000001db80b6c1d8 = { sa_family ...	0x000001db80b6c1d8 = { sa_family ...
6	int	tolen	16	16

Hex Buffer: 12 bytes (Pre-Call)

```
0000  53 6f 6d 65 20 63 6f 6e 74 65 6e 74                Some content
```

Call Stack: sendto (Ws2_32.dll)

#	Module	Address	Offset	Location
1	0x00000000000...	0x00007ffa7a7a...	0x7a7a6f0c	
2	0x00000000000...	0x00007ffa7a7...	0x7a7b581d	
3	0x00000000000...	0x00007ffa7a7...	0x7a7b518e	
4	0x00000000000...	0x00007ffa7a7...	0x7a7b36f8	

Output

```
------ Loading Files from C:\Users\afish\Desktop\Tools\API Monitor\API ------
------ Finished Loading 2119 Files ------
Categories:      835
Variables:       19678
DLLs:            222
APIs:            15885
COM Interfaces:  1826
COM Methods:     22262
```

API Loader | Monitoring | Output

Ready | 9.15 MB | Mode: Portable

Memory

Visual Studio

WinDBG

WinObj

TaskManager, ProcessExplorer

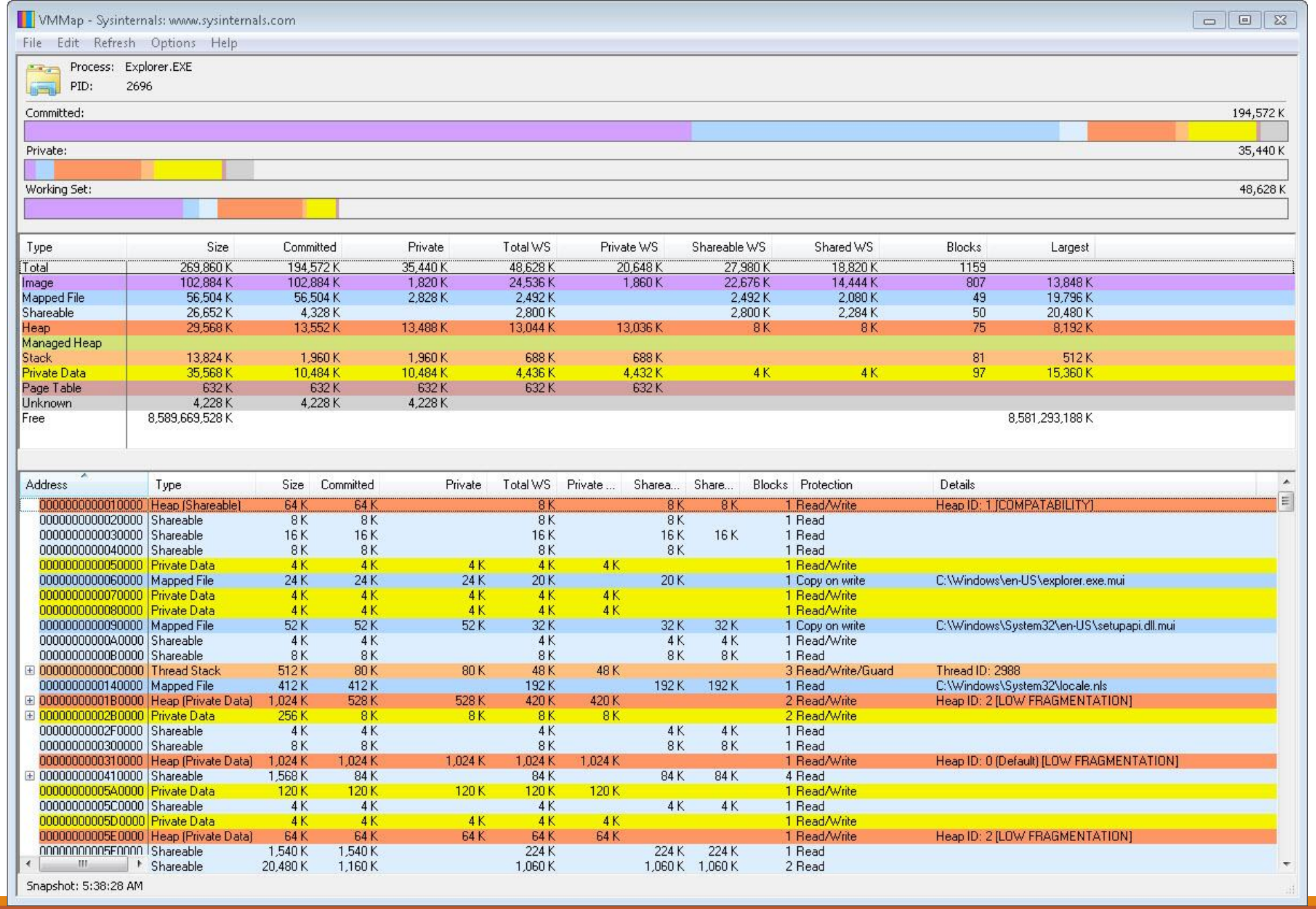
VMMap

WinObj - Sysinternals: www.sysinternals.com

File View Help

- \
  - ArcName
  - BaseNamedObjects
    - Restricted
  - Callback
  - Device
    - cimfs
    - Harddisk0
    - Http
    - Ide
  - Driver
  - DriverStores
  - FileSystem
    - Filters
  - GLOBAL??
  - KernelObjects
  - KnownDlls
  - KnownDlls32
  - NLS
  - ObjectTypes
  - RPC Control
  - Security
  - Sessions
    - 0
      - AppContainerNamedObjects
        - S-1-15-2-95739096-486727260-2033287795-3853587803-1685597119-444378811-2746676523
      - DosDevices
        - 00000000-000003e4
        - 00000000-000003e5
        - 00000000-0000d72d
        - 00000000-0000d743
        - 00000000-00016819
        - 00000000-001fff4b
        - 00000000-0020027b
        - 00000000-0020d700
        - 00000000-0020d729
    - 1
      - AppContainerNamedObjects
      - BaseNamedObjects
        - Restricted
      - DosDevices
      - Windows
        - WindowStations
    - 2
    - BNOLINKS
  - UMDFCommunicationPorts
  - Windows
    - WindowStations

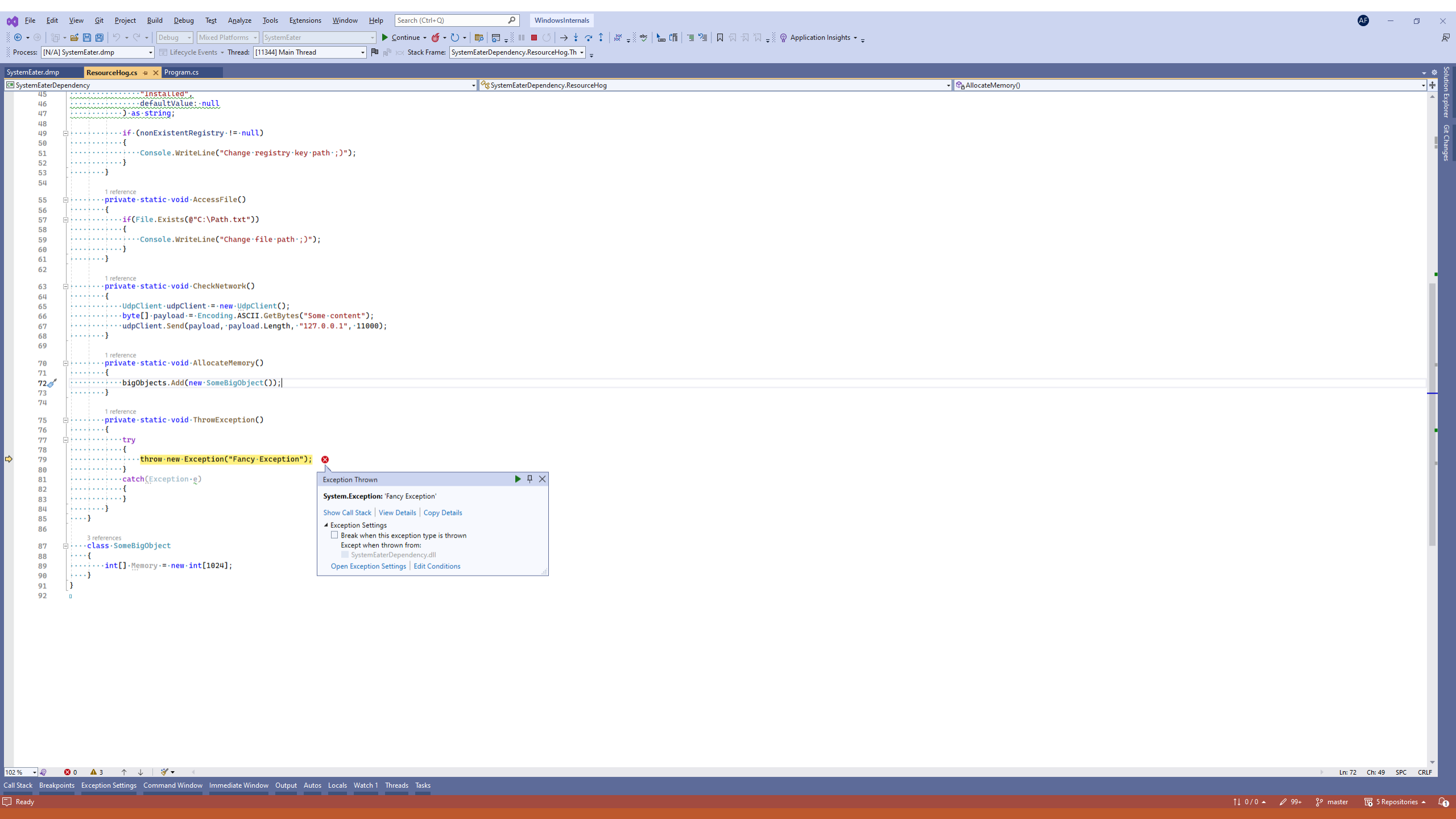
Name	Type	SymLink
784HWNDInterface:1003c	Section	
AppContainerNamedObjects	SymbolicLink	\Sessions\1\AppContainerNamedObjects
DBWinMutex	Mutant	
DWM_DX_FULLSCREEN_TRANSITION_EVENT	Event	
DwmComposedEvent_1	Event	
EventRitExited	Event	
EventShutDownCSRSS	Event	
Global	SymbolicLink	\BaseNamedObjects
Local	SymbolicLink	\Sessions\1\BaseNamedObjects
ScNetDrvMsg	Event	
Session	SymbolicLink	\Sessions\BNOLINKS
SessionImmersiveColorMutex	Mutant	
SessionImmersiveColorPreference	Section	
SIPC_{2819B8FF-EB1C-4652-80F0-7AB4EFA88BE4}	ALPC Port	
SM0:1924:120:WilError_03	Mutant	
SM0:1924:120:WilError_03_p0	Semaphore	
SM0:1924:120:WilError_03_p0h	Semaphore	
SM0:1924:304:WilStaging_02	Mutant	
SM0:1924:304:WilStaging_02_p0	Semaphore	
SM0:1924:304:WilStaging_02_p0h	Semaphore	
SM0:1948:120:WilError_03	Mutant	
SM0:1948:120:WilError_03_p0	Semaphore	
SM0:1948:120:WilError_03_p0h	Semaphore	
SM0:1948:304:WilStaging_02	Mutant	
SM0:1948:304:WilStaging_02_p0	Semaphore	
SM0:1948:304:WilStaging_02_p0h	Semaphore	
SM0:796:304:WilStaging_02	Mutant	
SM0:796:304:WilStaging_02_p0	Semaphore	
SM0:796:304:WilStaging_02_p0h	Semaphore	
SM0:864:120:WilError_03	Mutant	
SM0:864:120:WilError_03_p0	Semaphore	
SM0:864:120:WilError_03_p0h	Semaphore	
SM0:864:304:WilStaging_02	Mutant	
SM0:864:304:WilStaging_02_p0	Semaphore	
SM0:864:304:WilStaging_02_p0h	Semaphore	
ThemesStartEvent	Event	
WinSta0_DesktopSwitch	Event	
{773F1B9A-35B9-4E95-83A0-A210F2DE3B37}-request	Event	
{773F1B9A-35B9-4E95-83A0-A210F2DE3B37}-running	Event	
{773F1B9A-35B9-4E95-83A0-A210F2DE3B37}-sdl	Event	
{DFFDE213-8CB4-46a9-90EB-3DA843AF66F9}-request2	Event	



Type	Size	Committed	Private	Total WS	Private WS	Shareable WS	Shared WS	Blocks	Largest
Total	269,860 K	194,572 K	35,440 K	48,628 K	20,648 K	27,980 K	18,820 K	1159	
Image	102,884 K	102,884 K	1,820 K	24,536 K	1,860 K	22,676 K	14,444 K	807	13,848 K
Mapped File	56,504 K	56,504 K	2,828 K	2,492 K		2,492 K	2,080 K	49	19,796 K
Shareable	26,652 K	4,328 K		2,800 K		2,800 K	2,284 K	50	20,480 K
Heap	29,568 K	13,552 K	13,488 K	13,044 K	13,036 K	8 K	8 K	75	8,192 K
Managed Heap									
Stack	13,824 K	1,960 K	1,960 K	688 K	688 K			81	512 K
Private Data	35,568 K	10,484 K	10,484 K	4,436 K	4,432 K	4 K	4 K	97	15,360 K
Page Table	632 K	632 K	632 K	632 K	632 K				
Unknown	4,228 K	4,228 K	4,228 K						
Free	8,589,669,528 K								8,581,293,188 K

Address	Type	Size	Committed	Private	Total WS	Private ...	Sharea...	Share...	Blocks	Protection	Details
0000000000010000	Heap (Shareable)	64 K	64 K		8 K		8 K	8 K	1	Read/Write	Heap ID: 1 [COMPATABILITY]
0000000000020000	Shareable	8 K	8 K		8 K		8 K		1	Read	
0000000000030000	Shareable	16 K	16 K		16 K		16 K	16 K	1	Read	
0000000000040000	Shareable	8 K	8 K		8 K		8 K		1	Read	
0000000000050000	Private Data	4 K	4 K	4 K	4 K	4 K			1	Read/Write	
0000000000060000	Mapped File	24 K	24 K	24 K	20 K		20 K		1	Copy on write	C:\Windows\en-US\explorer.exe.mui
0000000000070000	Private Data	4 K	4 K	4 K	4 K	4 K			1	Read/Write	
0000000000080000	Private Data	4 K	4 K	4 K	4 K	4 K			1	Read/Write	
0000000000090000	Mapped File	52 K	52 K	52 K	32 K		32 K	32 K	1	Copy on write	C:\Windows\System32\en-US\setupapi.dll.mui
00000000000A0000	Shareable	4 K	4 K		4 K		4 K	4 K	1	Read/Write	
00000000000B0000	Shareable	8 K	8 K		8 K		8 K	8 K	1	Read	
00000000000C0000	Thread Stack	512 K	80 K	80 K	48 K	48 K			3	Read/Write/Guard	Thread ID: 2988
0000000000140000	Mapped File	412 K	412 K		192 K		192 K	192 K	1	Read	C:\Windows\System32\locale.nls
00000000001B0000	Heap (Private Data)	1,024 K	528 K	528 K	420 K	420 K			2	Read/Write	Heap ID: 2 [LOW FRAGMENTATION]
00000000002B0000	Private Data	256 K	8 K	8 K	8 K	8 K			2	Read/Write	
00000000002F0000	Shareable	4 K	4 K		4 K		4 K	4 K	1	Read	
0000000000300000	Shareable	8 K	8 K		8 K		8 K	8 K	1	Read	
0000000000310000	Heap (Private Data)	1,024 K	1,024 K	1,024 K	1,024 K	1,024 K			1	Read/Write	Heap ID: 0 (Default) [LOW FRAGMENTATION]
0000000000410000	Shareable	1,568 K	84 K		84 K		84 K	84 K	4	Read	
00000000005A0000	Private Data	120 K	120 K	120 K	120 K	120 K			1	Read/Write	
00000000005C0000	Shareable	4 K	4 K		4 K		4 K	4 K	1	Read	
00000000005D0000	Private Data	4 K	4 K	4 K	4 K	4 K			1	Read/Write	
00000000005E0000	Heap (Private Data)	64 K	64 K	64 K	64 K	64 K			1	Read/Write	Heap ID: 2 [LOW FRAGMENTATION]
00000000005F0000	Shareable	1,540 K	1,540 K		224 K		224 K	224 K	1	Read	
	Shareable	20,480 K	1,160 K		1,060 K		1,060 K	1,060 K	2	Read	

Snapshot: 5:38:28 AM


File Edit View Git Project Build Debug Test Analyze Tools Extensions Window Help
Search (Ctrl+Q)
WindowsInternals
Debug
Mixed Platforms
SystemEater
Continue
Application Insights
Process: [N/A] SystemEater.dmp
Lifecycle Events
Thread: [11344] Main Thread
Stack Frame: SystemEaterDependency.ResourceHog.Th
SystemEater.dmp
ResourceHog.cs
Program.cs
SystemEaterDependency
SystemEaterDependency.ResourceHog
AllocateMemory()
"Installed",
defaultValue: null
) as string;
if (nonExistentRegistry != null)
{
Console.WriteLine("Change registry key path ;)");
}
1 reference
private static void AccessFile()
{
if(File.Exists(@"C:\Path.txt"))
{
Console.WriteLine("Change file path ;)");
}
}
1 reference
private static void CheckNetwork()
{
UdpClient udpClient = new UdpClient();
byte[] payload = Encoding.ASCII.GetBytes("Some content");
udpClient.Send(payload, payload.Length, "127.0.0.1", 11000);
}
1 reference
private static void AllocateMemory()
{
bigObjects.Add(new SomeBigObject());
}
1 reference
private static void ThrowException()
{
try
{
throw new Exception("Fancy Exception");
}
catch(Exception e)
{
}
}
}
3 references
class SomeBigObject
{
int[] Memory = new int[1024];
}
Exception Thrown
System.Exception: 'Fancy Exception'
Show Call Stack | View Details | Copy Details
Exception Settings
Break when this exception type is thrown
Except when thrown from:
SystemEaterDependency.dll
Open Exception Settings | Edit Conditions
102 %
0
3
Ln: 72
Ch: 49
SPC
CRLF
Call Stack
Breakpoints
Exception Settings
Command Window
Immediate Window
Output
Autos
Locals
Watch 1
Threads
Tasks
Ready
0 / 0
99+
master
5 Repositories
Solution Explorer
Git Changes

Dump C:\Users\afish\Desktop\AdditionalTools\Traces\SystemEater.dmp - WinDbg:10.0.22621.1778 AMD64

File Edit View Debug Window Help

Command

```
************* Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*C:\tmp*http://msdl.microsoft.com/download/symbols
Symbol search path is: srv*C:\tmp*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 10 Version 19045 MP (8 procs) Free x64
Product: WinNt, suite: SingleUserTS
Edition build lab: 19041.1.amd64fre.vb_release.191206-1406
Machine Name:
Debug session time: Thu Aug 15 06:53:16.000 2024 (UTC - 7:00)
System Uptime: 0 days 0:36:23.449
Process Uptime: 0 days 0:00:18.000
.....................................
This dump file has an exception of interest stored in it.
The stored exception information can be accessed via .ecxr.
(2e48.2c50): CLR exception - code e0434f4d (first/second chance not available)
For analysis of this file, run !analyze -v
ntdll!NtWaitForSingleObject+0x14:
00007ffb`90d8d5e4 c3              ret
0:000> kb
 # RetAddr               : Args to Child                                                   : Call Site
00 00007ffb`8e6a920e     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!NtWaitForSingleObject+0x14
01 00007ffa`da2152e0     : 00000000`00000000 00000000`00000000 000098ae`00000000 00000000`000001fc : KERNELBASE!WaitForSingleObjectEx+0x8e
02 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!CLREventWaitHelper2+0x6 [D:\a\_work\1\s\src\coreclr\vm\synch.cpp @ 372]
03 00007ffa`da4903dc     : 00000000`04242420 00000000`00000000 00007ffb`8e6bb699 00000218`00000003 : coreclr!CLREventWaitHelper+0x20 [D:\a\_work\1\s\src\coreclr\vm\synch.cpp @ 397]
04 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!CLREventBase::WaitEx+0x12 [D:\a\_work\1\s\src\coreclr\vm\synch.cpp @ 466]
05 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!CLREventBase::Wait+0x12 [D:\a\_work\1\s\src\coreclr\vm\synch.cpp @ 412]
06 00007ffa`da36900a     : 00000001`00000000 00007ffa`000aa028 00000000`0002a028 00007ffb`0002a028 : coreclr!Thread::WaitSuspendEventsHelper+0xc8 [D:\a\_work\1\s\src\coreclr\vm\threadsuspend.cpp @ 4626]
07 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!Thread::WaitSuspendEvents+0x8 [D:\a\_work\1\s\src\coreclr\vm\threadsuspend.cpp @ 4663]
08 00007ffa`da2b94f0     : 00000218`7a49be50 00000218`7a42cfb0 00000218`7a410c90 00007ffb`90d1f2c7 : coreclr!Thread::RareEnablePreemptiveGC+0x808da [D:\a\_work\1\s\src\coreclr\vm\threadsuspend.cpp @ 2414]
09 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!Thread::EnablePreemptiveGC+0x16 [D:\a\_work\1\s\src\coreclr\vm\threads.h @ 2044]
0a 00007ffa`da3e79d6     : 0000008c`63d9e3a0 00000000`00000000 00000218`7a42d450 00000000`00000000 : coreclr!Thread::RareDisablePreemptiveGC+0xc8 [D:\a\_work\1\s\src\coreclr\vm\threadsuspend.cpp @ 2156]
0b (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!Thread::DisablePreemptiveGC+0x16 [D:\a\_work\1\s\src\coreclr\vm\threads.h @ 1992]
0c 00007ffa`da538c0f     : 0000008c`63d9e3a0 00000218`7a42d450 00000218`7a42d450 00007ffa`7a7ae5c1 : coreclr!EEDbgInterfaceImpl::DisablePreemptiveGC+0x36 [D:\a\_work\1\s\src\coreclr\vm\eedbginterfaceimpl.cpp @ 649]
0d (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!GCHolderEEInterface<0,1,1>::LeaveInternal+0x39 [D:\a\_work\1\s\src\coreclr\debug\ee\debugger.h @ 260]
0e (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!GCHolderEEInterface<0,1,1>::{dtor}+0x39 [D:\a\_work\1\s\src\coreclr\debug\ee\debugger.h @ 303]
0f 00007ffa`da5385ea     : 00000000`00000100 00000000`00000000 00000218`7a3a1258 00007ffa`7a7ae500 : coreclr!Debugger::SendExceptionHelperAndBlock+0x2af [D:\a\_work\1\s\src\coreclr\debug\ee\debugger.cpp @ 7444]
10 00007ffa`da53838b     : 0000008c`00000020 00000218`7a497220 00000000`00000001 00000000`00000001 : coreclr!Debugger::SendExceptionEventsWorker+0x196 [D:\a\_work\1\s\src\coreclr\debug\ee\debugger.cpp @ 7536]
11 00007ffa`da52da77     : 00000000`00000000 0000008c`63d9e3a0 00000000`00000000 00007ffa`7a7ae5c1 : coreclr!Debugger::SendException+0x1a3 [D:\a\_work\1\s\src\coreclr\debug\ee\debugger.cpp @ 7748]
12 00007ffa`da3b1de1     : 00000000`00000000 00000000`00000000 00000218`7a499e50 00000000`00000001 : coreclr!Debugger::FirstChanceManagedException+0x27 [D:\a\_work\1\s\src\coreclr\debug\ee\debugger.cpp @ 7894]
13 00007ffa`da2d9272     : 00000000`00000000 0000008c`63d9e3a0 0000008c`63d9e3a0 00000000`00000001 : coreclr!EEToDebuggerExceptionInterfaceWrapper::FirstChanceManagedException+0xd964d [D:\a\_work\1\s\src\coreclr\vm\eedbginterfaceimpl.inl @ 38]
14 00007ffa`da2da4eb     : 0000008c`63d9e3a0 0000008c`63d9c100 0000008c`63d9e3a0 0000008c`63d9e3a0 : coreclr!ExceptionTracker::ProcessManagedCallFrame+0x546 [D:\a\_work\1\s\src\coreclr\vm\exceptionhandling.cpp @ 2583]
15 00007ffa`da2d9f1c     : 0000008c`63d9de30 00000000`00000000 0000008c`63d9de30 00007ffa`da628d42 : coreclr!ExceptionTracker::ProcessOSExceptionNotification+0x317 [D:\a\_work\1\s\src\coreclr\vm\exceptionhandling.cpp @ 1937]
16 00007ffb`90d9292f     : 0000008c`63d9de30 0000008c`63d9e3a0 00000000`00000000 0000008c`63d9d7c0 : coreclr!ProcessCLRException+0x21c [D:\a\_work\1\s\src\coreclr\vm\exceptionhandling.cpp @ 1066]
17 00007ffb`90d42554     : 00000000`00000000 0000008c`63d9d770 0000008c`63d9de30 00000000`00000001 : ntdll!RtlpExecuteHandlerForException+0xf
18 00007ffb`90d9143e     : 0000008c`63d9da10 00007ffb`90d20e7b 00000218`00411178 00007ffb`90d42e23 : ntdll!RtlDispatchException+0x244
19 00007ffb`8e6bb699     : 00000218`00411178 00000218`00411178 00000000`00000001 0000008c`63d9e3d0 : ntdll!KiUserExceptionDispatch+0x2e
1a 00007ffa`da2d669e     : 00000218`00411178 0000008c`63d9e0f0 00000218`7c4172b0 00007ffa`da2933fe : KERNELBASE!RaiseException+0x69
1b 00007ffa`da2d5a0f     : 00000000`7000011f 00000218`0040ffa8 00000218`00411178 00000218`0011cdb0 : coreclr!RaiseTheExceptionInternalOnly+0x28a [D:\a\_work\1\s\src\coreclr\vm\excep.cpp @ 2806]
1c 00007ffa`7a7ae5c1     : 48dcbd31`93f3b66f 00007ffa`d99ebbb7 3fffffff`ffffffff 00000218`00411178 : coreclr!IL_Throw+0xdf [D:\a\_work\1\s\src\coreclr\vm\jithelpers.cpp @ 4119]
1d 00007ffa`7a7a839d     : 00000218`0011cfb8 00000000`00000005 d40f1433`b987cce4 179c5126`448a3a96 : 0x00007ffa`7a7ae5c1
1e 00007ffa`7a7a7d3e     : 00000000`00000078 0000008c`63d9e6c0 00007ffa`da2df40b 0000008c`00000001 : 0x00007ffa`7a7a839d
1f 00007ffa`da33af03     : 00000218`0000a010 0000008c`63d9e6c0 00007ffa`da2df40b 0000008c`00000001 : 0x00007ffa`7a7a7d3e
20 00007ffa`da258376     : 00000000`00000000 0000008c`63d9e698 00000000`00000020 0000008c`63d9e628 : coreclr!CallDescrWorkerInternal+0x83
21 00007ffa`da2df3d7     : 0000008c`63d9e718 00000000`00000000 00000000`00000000 00000000`00000000 : coreclr!MethodDescCallSite::CallTargetWorker+0x176 [D:\a\_work\1\s\src\coreclr\vm\callhelpers.cpp @ 551]
22 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : coreclr!MethodDescCallSite::Call+0xb [D:\a\_work\1\s\src\coreclr\vm\callhelpers.h @ 458]
23 00007ffa`da2df256     : 00000218`0000a010 00000218`0000a010 00000000`00000000 0000008c`63d9eb58 : coreclr!RunMainInternal+0x11f [D:\a\_work\1\s\src\coreclr\vm\assembly.cpp @ 1483]
24 00007ffa`da2df105     : 00000218`7a49be50 0000008c`00000000 00000218`7a49be50 00007ffa`7a83c5b0 : coreclr!RunMain+0xd2 [D:\a\_work\1\s\src\coreclr\vm\assembly.cpp @ 1554]
25 00007ffa`da2deec6     : 00000218`00000000 00000130`00000000 00000218`00000130 00007ffa`7a429c10 : coreclr!Assembly::ExecuteMainMethod+0x1c9 [D:\a\_work\1\s\src\coreclr\vm\assembly.cpp @ 1672]
26 00007ffa`da2f5212     : 00000218`7c3dda60 00000000`00000001 00000000`00000001 00000000`00000000 : coreclr!CorHost2::ExecuteAssembly+0x1c6 [D:\a\_work\1\s\src\coreclr\vm\corhost.cpp @ 384]
27 00007ffa`e09f972b     : 00000218`7a4c9060 00000218`7a4127b0 00000218`7a467e60 00000218`7a4127b0 : coreclr!coreclr_execute_assembly+0xe2 [D:\a\_work\1\s\src\coreclr\dlls\mscoree\unixinterface.cpp @ 475]
28 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : hostpolicy!coreclr_t::execute_assembly+0x2a [D:\a\_work\1\s\src\native\corehost\hostpolicy\coreclr.cpp @ 89]
29 00007ffa`e09f9a5c     : 00000218`7a3f9988 0000008c`63d9f169 00007ffa`e0a3bc40 00000218`7a3f9988 : hostpolicy!run_app_for_context+0x56b [D:\a\_work\1\s\src\native\corehost\hostpolicy\hostpolicy.cpp @ 255]
2a 00007ffa`e09fa3f7     : 00000000`00000000 00000218`7a3f9980 00000218`7a3f9980 00000000`00000000 : hostpolicy!run_app+0x3c [D:\a\_work\1\s\src\native\corehost\hostpolicy\hostpolicy.cpp @ 284]
2b 00007ffa`e0a5b800     : 00007ffb`8e51f4e8 00007ffa`e09fc0f0 00007ffa`e09fc0f0 00000000`00000001 : hostpolicy!corehost_main+0x107 [D:\a\_work\1\s\src\native\corehost\hostpolicy\hostpolicy.cpp @ 430]
2c 00007ffa`e0a5e48a     : 00000218`7a40e5c0 0000008c`63d9f500 00000000`00000000 00000000`00000000 : hostfxr!execute_app+0x330 [D:\a\_work\1\s\src\native\corehost\fxr\fx_muxer.cpp @ 146]
2d 00007ffa`e0a60746     : 00007ffa`e0a99868 00000218`7a407d30 0000008c`63d9f440 0000008c`63d9f3f0 : hostfxr!`anonymous namespace'::read_config_and_execute+0xaa [D:\a\_work\1\s\src\native\corehost\fxr\fx_muxer.cpp @ 533]
2e 00007ffa`e0a5eaf4     : 0000008c`63d9f500 0000008c`63d9f520 0000008c`63d9f471 00000000`00000013 : hostfxr!fx_muxer_t::handle_exec_host_command+0x166 [D:\a\_work\1\s\src\native\corehost\fxr\fx_muxer.cpp @ 1018]
2f 00007ffa`e0a585c3     : 0000008c`63d9f520 00000218`7a407e20 00000000`00000001 00000000`0000005e : hostfxr!fx_muxer_t::execute+0x494 [D:\a\_work\1\s\src\native\corehost\fxr\fx_muxer.cpp @ 579]
*** WARNING: Unable to verify checksum for SystemEater.exe
30 00007ff6`20bf1eb8     : 00007ffb`8e51f4e8 00007ffa`e0a59a90 00007ffa`e0a59a90 00000218`7a3fbf10 : hostfxr!hostfxr_main_startupinfo+0xb3 [D:\a\_work\1\s\src\native\corehost\fxr\hostfxr.cpp @ 61]
31 00007ff6`20bf222b     : 00007ff6`20bfc3d0 00000000`00000007 00000218`7a3f9980 00000000`0000005e : SystemEater_exe!exe_start+0x8d8 [D:\a\_work\1\s\src\native\corehost\corehost.cpp @ 235]
32 00007ff6`20bf36d8     : 00000000`00000000 00000218`7a3f9980 00000000`00000000 00000000`00000000 : SystemEater_exe!wmain+0xab [D:\a\_work\1\s\src\native\corehost\corehost.cpp @ 304]
33 (Inline Function)     : -------`-------- -------`-------- -------`-------- -------`-------- : SystemEater_exe!invoke_main+0x22 [D:\a\_work\1\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl @ 90]
34 00007ffb`903a7374     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : SystemEater_exe!__scrt_common_main_seh+0x10c [D:\a\_work\1\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl @ 288]
35 00007ffb`90d3cc91     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : kernel32!BaseThreadInitThunk+0x14
36 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21
0:000> !threads
ThreadCount:      2
UnstartedThread:  0
BackgroundThread: 1
PendingThread:    0
DeadThread:       0
Hosted Runtime:   no
                                                                                                  Lock
 DBG   ID     OSID ThreadOBJ           State GC Mode     GC Alloc Context                  Domain           Count Apt Exception
   0    1     2c50 000002187A49BE50    aa028 Preemptive  0000021800411258:0000021800413210 000002187a429c10 -00001 MTA System.Exception 0000021800411178
   7    2     1f04 000002187A4C7A90    21228 Preemptive  0000000000000000:0000000000000000 000002187a429c10 -00001 Ukn (Finalizer)
0:000> !clrstack
OS Thread Id: 0x2c50 (0)
        Child SP               IP Call Site
0000008C63D9E2A8 00007ffb90d8d5e4 [HelperMethodFrame: 0000008c63d9e2a8]
0000008C63D9E3A0 00007ffa7a7ae5c1 SystemEaterDependency.ResourceHog.ThrowException() [C:\Users\afish\Desktop\msp_windowsinternals\SystemEaterDependency\ResourceHog.cs @ 79]
0000008C63D9E3E0 00007ffa7a7a839d SystemEaterDependency.ResourceHog.Loop(Int32)
0000008C63D9E420 00007ffa7a7a7d3e SystemEater.Program.Main(System.String[]) [C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\Program.cs @ 9]
```

0:000>

Ln 0, Col 0 | Sys 0:C:\User | Proc 000:2e48 | Thrd 000:2c50 | ASM | OVR | CAPS | NUM

Dump C:\Users\afish\Desktop\AdditionalTools\Traces\SystemEater.dmp - WinDbg:10.0.22621.1778 AMD64

File Edit View Debug Window Help

Command

```
7ffa7a870798     3        184 System.WeakReference<System.Diagnostics.Tracing.EventSource>[]
7ffa7a8caf80     1        184 System.Buffers.ArrayPoolEventSource
7ffa7a8e8560     1        184 System.Net.NetEventSource
7ffa7a8ed4d0     1        184 System.Net.NetEventSource
7ffa7a875310     3        192 System.Reflection.RuntimeModule
7ffa7a876530     4        192 System.Reflection.RuntimeAssembly
7ffa7a880e38     3        192 System.Reflection.MemberFilter
7ffa7a816e10     8        192 System.UInt32
7ffa7a87d388     1        200 System.Collections.Generic.HashSet<System.RuntimeType>+Entry[]
7ffa7a8c8370     1        200 System.Globalization.NumberFormatInfo
7ffa7a85d970     1        208 System.Globalization.CalendarData[]
7ffa7a895208     1        208 System.Double[]
7ffa7a88fb88     7        224 System.Diagnostics.Tracing.EventSourceAttribute[]
7ffa7a89c578     4        224 System.RuntimeType+RuntimeTypeCache+MemberInfoCache<System.Reflection.RuntimeFieldInfo>
7ffa7a87d058     5        232 System.Type[]
7ffa7a873608    10        240 System.Diagnostics.Tracing.EventTask
7ffa7a873868    10        240 System.Diagnostics.Tracing.EventOpcode
7ffa7a8cad78     1        240 System.Buffers.TlsOverPerCoreLockedStacksArrayPool<System.Char>+PerCoreLockedStacks[]
7ffa7a85f160     8        256 Internal.Win32.SafeHandles.SafeRegistryHandle
7ffa7a8c64d8     3        264 System.TimeZoneInfo+AdjustmentRule
7ffa7a88db68     9        279 System.Boolean[]
7ffa7a873370     7        280 System.Diagnostics.Tracing.EventSourceAttribute
7ffa7a8edbf8     1        280 System.Net.Sockets.SocketsTelemetry
7ffa7a82ed28     1        288 System.Collections.Generic.Dictionary<System.String, System.Object>+Entry[]
7ffa7a8e1a70     6        288 Microsoft.Win32.RegistryKey
7ffa7a870728     4        352 System.Diagnostics.Tracing.EventCommandEventArgs
7ffa7a815fd0    15        360 System.Int32
7ffa7a8a6658     2        376 System.UInt64[]
7ffa7a83e3b0     1        384 System.Diagnostics.Tracing.RuntimeEventSource
7ffa7a8c3a00     6        384 System.Action
7ffa7a8c59b0     5        400 System.TimeZoneInfo
7ffa7a88ea98     4        432 System.Reflection.RuntimePropertyInfo[][]
7ffa7a85bfb0     4        448 System.Globalization.CultureInfo
7ffa7a8c9698     1        456 System.Buffers.TlsOverPerCoreLockedStacksArrayPool<System.Char>+ThreadLocalArray[]
7ffa7a855b68     6        480 System.Collections.Generic.Dictionary<System.String, System.String>
7ffa7a8815b8    12        488 System.Reflection.RuntimePropertyInfo[]
7ffa7a83f1b0     6        624 System.IntPtr[]
7ffa7a89cc28     5        640 System.Reflection.FieldInfo[]
7ffa7a8c0f30    10        640 System.Diagnostics.Tracing.ScalarTypeInfo
7ffa7a8c2410    10        640 System.Func<System.Object, System.Diagnostics.Tracing.PropertyValue>
7ffa7a8e20a0     5        680 System.UInt16[]
7ffa7a8502e8    12        768 Interop+Advapi32+EtwEnableCallback
7ffa7a8ce5e8    34        816 SystemEaterDependency.SomeBigObject
7ffa7a817c68    37        888 System.Int64
7ffa7a879f18     9        936 System.Reflection.RuntimePropertyInfo
7ffa7a8cf3b0     6      1,136 SystemEaterDependency.SomeBigObject[]
7ffa7a8c4b78     5      1,244 System.UInt32[]
7ffa7a83f900    12      1,344 System.Diagnostics.Tracing.EventSource+OverrideEventProvider
7ffa7a8e1ca0    44      1,408 Microsoft.Win32.SafeHandles.SafeRegistryHandle
7ffa7a8e5bb0    44      1,408 System.Net.IPAddress[]
7ffa7a8e56b8    44      1,408 System.Net.IPEndPoint
7ffa7a8e4f18    44      1,760 System.Net.Sockets.UdpClient
7ffa7a8edf00    44      1,760 System.Net.Internals.SocketAddress
7ffa7a85d060     4      1,824 System.Globalization.CultureData
7ffa7a8e5b20    47      1,880 System.Net.IPAddress
7ffa7a8e22a0     1      2,072 System.UInt16[][]
7ffa7a89cae0    14      2,104 System.Reflection.RuntimeFieldInfo[]
7ffa7a8ea528    44      2,112 System.Net.Sockets.SafeSocketHandle
7ffa7a822100    38      2,736 System.SByte[]
7ffa7a778398    76      3,040 System.RuntimeType
7ffa7a878b58     2      3,120 System.Reflection.MethodInfo[]
7ffa7a83e000   148      3,552 System.Diagnostics.Tracing.EventKeywords
7ffa7a813488   149      3,576 System.Byte
7ffa7a83df68   149      3,576 System.Diagnostics.Tracing.EventLevel
7ffa7a8a11b8   149      3,576 System.Reflection.RuntimeExceptionHandlingClause[]
7ffa7a89c8c0    56      3,584 System.Reflection.MdFieldInfo
7ffa7a8a1460   149      3,584 System.Reflection.RuntimeLocalVariableInfo[]
7ffa7a8747d8    24      3,648 System.RuntimeType+RuntimeTypeCache
7ffa7a89eee0     5      3,792 System.Collections.Generic.Dictionary<System.UInt64, System.String>+Entry[]
7ffa7a83b9f0    36      4,048 System.String[]
02187a46ad20   191      4,600 Free
7ffa7a89f828   150      4,792 System.Diagnostics.Tracing.EventAttribute[]
7ffa7a827dc0    38      4,864 System.Exception
7ffa7a890878   117      5,616 System.Text.StringBuilder
7ffa7a8e7310    44      5,632 System.Net.Sockets.Socket
7ffa7a878860    31      7,120 System.Reflection.RuntimeMethodInfo[]
7ffa7a87f258   160      7,656 System.Reflection.CustomAttributeRecord[]
7ffa7a8955c0     8      8,832 System.Collections.Generic.Dictionary<System.Int32, System.String>+Entry[]
7ffa7a8a0d68   149      9,536 System.Reflection.RuntimeMethodBody
7ffa7a873908   150      9,600 System.Diagnostics.Tracing.EventAttribute
7ffa7a87e708   188     10,040 System.RuntimeType[]
7ffa7a87f4d8   149     13,112 System.RuntimeMethodInfoStub
7ffa7a88ef88   285     17,544 System.Reflection.ParameterInfo[]
7ffa7a88ee60   236     18,880 System.Signature
7ffa7a8c08e8   149     19,440 System.Diagnostics.Tracing.EventParameterInfo[]
7ffa7a872370   249     25,896 System.Reflection.RuntimeMethodInfo
7ffa7a8a1628    13     27,456 System.Collections.Generic.Dictionary<System.String, System.String>+Entry[]
7ffa7a77a0f0   494     55,680 System.Object[]
7ffa7a8730e0   669     64,224 System.Reflection.RuntimeParameterInfo
7ffa7a822520    80    152,208 System.Int32[]
7ffa7a879258    11    249,480 System.Diagnostics.Tracing.EventSource+EventMetadata[]
7ffa7a8269b8 2,537    384,300 System.String
7ffa7a8937c8   121    386,060 System.Char[]
7ffa7a870318   443  3,037,149 System.Byte[]
Total 8,446 objects, 4,616,918 bytes
```

0:000>

Ln 0, Col 0 | Sys 0:C:\User | Proc 000:2e48 | Thrd 000:2c50 | ASM | OVR | CAPS | NUM

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-EIHJ7RK\afish]

File Options View Process Find Handle Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		7,084 K	23,056 K	5160	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,380 K	18,556 K	4092	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,324 K	20,564 K	7536	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	1,864 K	7,928 K	1356	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,136 K	11,224 K	2864	Host Process for Windows S...	Microsoft Corporation
svchost.exe		14,152 K	21,092 K	7632	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,500 K	7,044 K	1696	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,852 K	22,316 K	7392	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,936 K	34,864 K	7200	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,772 K	8,752 K	4992	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,792 K	8,328 K	4516	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	3,944 K	21,656 K	7544	Host Process for Windows S...	Microsoft Corporation
svchost.exe		5,364 K	20,096 K	9832	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,964 K	7,880 K	7748	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,708 K	8,588 K	4180	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,308 K	10,160 K	8488	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,716 K	8,488 K	6340	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,696 K	12,616 K	7348	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,036 K	8,384 K	6404	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	5,352 K	18,400 K	6436	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,024 K	10,372 K	4752	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,956 K	6,784 K	560	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,880 K	9,852 K	10120	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,596 K	11,696 K	8680	Host Process for Windows S...	Microsoft Corporation
svchost.exe		8,800 K	16,424 K	10768	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,868 K	7,940 K	1228	Host Process for Windows S...	Microsoft Corporation
SynTPEnh.exe	0.01	2,840 K	9,504 K	3588	Synaptics TouchPad 64-bit ...	Synaptics Incorporated
SynTPEnhService.exe		2,020 K	9,004 K	3456	64-bit Synaptics Pointing En...	Synaptics Incorporated
SysInfoCap.exe		7,004 K	28,244 K	2184		HP Inc.
System	0.42	196 K	148 K	4		
System Idle Process	76.50	60 K	8 K	0		
SystemEater.exe	13.21	268,184 K	277,624 K	5920	SystemEater	SystemEater
SystemSettingsBroker.exe		3,908 K	18,344 K	6944	System Settings Broker	Microsoft Corporation
TabTip.exe	0.02	4,000 K	17,120 K	2928		
taskhostw.exe		7,940 K	19,980 K	7712	Host Process for Windows T...	Microsoft Corporation
taskhostw.exe		7,216 K	21,372 K	5472		
TextInputHost.exe	0.06	9,180 K	40,620 K	4568		Microsoft Corporation
ThunderboltService.exe		18,244 K	19,348 K	5188	ThunderboltService	Intel Corporation
TiWorker.exe		22,556 K	30,484 K	3620		

Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\2\BaseNamedObjects
Event	\KernelObjects\LowMemoryCondition
File	C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Release\net6.0
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\ConDrv
File	\Device\KsecDD
File	\Device\NamedPipe\dotnet-diagnostic-5920
File	\Device\CNG
File	\Device\NamedPipe\dotnet-diagnostic-5920
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Private.CoreLib.dll
File	\Device\ConDrv
File	C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Release\net6.0\SystemE...
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Runtime.dll
File	\Device\Afd
File	C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Release\net6.0\SystemE...
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Collections.dll
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Console.dll
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Net.Sockets.dll
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\Microsoft.Win32.Registry.dll
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Net.Primitives.dll
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\Microsoft.Win32.Primitives.dll
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Diagnostics.Tracin...
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Net.NameResoluti...
File	C:\Program Files\dotnet\shared\Microsoft.NETCore.App\6.0.21\System.Memory.dll
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd
File	\Device\Afd

SystemEater.exe:5920 Properties

Threads | TCP/IP | Security | Environment | Job | Strings

Image | Performance | Performance Graph | GPU Graph

Image File

SystemEater

SystemEater

Version: 1.0.0.0

Build Time: Thu Jul 13 15:00:10 2023

Path:

C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\E | Explore

Command line:

"C:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Releas

Current directory:

c:\Users\afish\Desktop\msp_windowsinternals\SystemEater\bin\Release

Autostart Location:

n/a | Explore

Parent: TOTALCMD.EXE(892)

User: DESKTOP-EIHJ7RK\afish

Started: 3:35:51 AM 8/20/2024 Image: 64-bit

Comment:

VirusTotal: | Submit

Verify | Bring to Front | Kill Process

Data Execution Prevention (DEP) Status: DEP (permanent)

Address Space Load Randomization: High Entropy

OK | Cancel

CPU Usage: 23.50% | Commit Charge: 42.43% | Processes: 175 | Physical Usage: 45.30%

Communication

Fiddler
- Fiddler Classic is still free to download and use

Wireshark

Network Monitor (NetMon, deprecated)

Message Analyzer (deprecated)

Winpcap

TCPView

Spy++

RPCMon

Pipe Monitor

Mailslot Monitor

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Process]	0	TCP	desktop-eihj7rk	64139	20.189.173.22	https	TIME_WAIT				
jhi_service.exe	4932	TCPV6	[0:0:0:0:0:0:0:1]	49670	desktop-eihj7rk	0	LISTENING				
lsass.exe	956	TCP	DESKTOP-EIHJ7...	49664	DESKTOP-EIHJ7...	0	LISTENING				
lsass.exe	956	TCPV6	desktop-eihj7rk	49664	desktop-eihj7rk	0	LISTENING				
msedge.exe	3516	TCP	desktop-eihj7rk	64138	204.79.197.239	https	ESTABLISHED				
SearchApp.exe	8768	TCP	desktop-eihj7rk	64119	a92-123-104-29.d...	https	CLOSE_WAIT				
SearchApp.exe	8768	TCP	desktop-eihj7rk	64120	a104-126-37-184....	https	CLOSE_WAIT				
services.exe	932	TCP	DESKTOP-EIHJ7...	49674	DESKTOP-EIHJ7...	0	LISTENING				
services.exe	932	TCPV6	desktop-eihj7rk	49674	desktop-eihj7rk	0	LISTENING				
spoolsv.exe	4364	TCP	DESKTOP-EIHJ7...	49669	DESKTOP-EIHJ7...	0	LISTENING				
spoolsv.exe	4364	TCPV6	desktop-eihj7rk	49669	desktop-eihj7rk	0	LISTENING				
svchost.exe	1076	TCP	DESKTOP-EIHJ7...	epmap	DESKTOP-EIHJ7...	0	LISTENING				
svchost.exe	1208	TCP	DESKTOP-EIHJ7...	ms-wbt-server	DESKTOP-EIHJ7...	0	LISTENING				
svchost.exe	4092	TCP	DESKTOP-EIHJ7...	5040	DESKTOP-EIHJ7...	0	LISTENING				
svchost.exe	1304	TCP	DESKTOP-EIHJ7...	49666	DESKTOP-EIHJ7...	0	LISTENING				
svchost.exe	2220	TCP	DESKTOP-EIHJ7...	49667	DESKTOP-EIHJ7...	0	LISTENING				
svchost.exe	1872	TCP	DESKTOP-EIHJ7...	49668	DESKTOP-EIHJ7...	0	LISTENING				
svchost.exe	5300	TCP	desktop-eihj7rk	63982	40.113.110.67	https	ESTABLISHED				
svchost.exe	6436	TCP	DESKTOP-EIHJ7...	ms-do	DESKTOP-EIHJ7...	0	LISTENING				
svchost.exe	1356	UDP	DESKTOP-EIHJ7...	ntp	*	*					
svchost.exe	7748	UDP	DESKTOP-EIHJ7...	ssdp	*	*					
svchost.exe	7748	UDP	desktop-eihj7rk	ssdp	*	*					
svchost.exe	1208	UDP	DESKTOP-EIHJ7...	ms-wbt-server	*	*					
svchost.exe	4092	UDP	DESKTOP-EIHJ7...	5050	*	*					
svchost.exe	4072	UDP	DESKTOP-EIHJ7...	5353	*	*					
svchost.exe	4072	UDP	DESKTOP-EIHJ7...	llmnr	*	*					
svchost.exe	4628	UDP	DESKTOP-EIHJ7...	63875	*	*					
svchost.exe	7748	UDP	desktop-eihj7rk	64262	*	*					
svchost.exe	7748	UDP	DESKTOP-EIHJ7...	64263	*	*					
svchost.exe	1076	TCPV6	[0:0:0:0:0:0:0:0]	epmap	[0:0:0:0:0:0:0:0]	0	LISTENING				
svchost.exe	1208	TCPV6	desktop-eihj7rk	ms-wbt-server	desktop-eihj7rk	0	LISTENING				
svchost.exe	6436	TCPV6	desktop-eihj7rk	ms-do	desktop-eihj7rk	0	LISTENING				
svchost.exe	1304	TCPV6	desktop-eihj7rk	49666	desktop-eihj7rk	0	LISTENING				
svchost.exe	2220	TCPV6	desktop-eihj7rk	49667	desktop-eihj7rk	0	LISTENING				
svchost.exe	1872	TCPV6	desktop-eihj7rk	49668	desktop-eihj7rk	0	LISTENING				
svchost.exe	1356	UDPV6	desktop-eihj7rk	123	*	*					
svchost.exe	7748	UDPV6	[0:0:0:0:0:0:0:1]	1900	*	*					
svchost.exe	1208	UDPV6	desktop-eihj7rk	ms-wbt-server	*	*					
svchost.exe	7748	UDPV6	[0:0:0:0:0:0:0:1]	64261	*	*					
System	4	TCP	desktop-eihj7rk	netbios-ssn	DESKTOP-EIHJ7...	0	LISTENING				
System	4	TCP	DESKTOP-EIHJ7...	microsoft-ds	DESKTOP-EIHJ7...	0	LISTENING				
System	4	UDP	desktop-eihj7rk	netbios-ns	*	*					
System	4	UDP	desktop-eihj7rk	netbios-dgm	*	*					
System	4	TCPV6	desktop-eihj7rk	microsoft-ds	desktop-eihj7rk	0	LISTENING				
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	58226	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	58462	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59177	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59178	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59179	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59180	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59181	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59182	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59183	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59184	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59185	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59186	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59187	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59188	*	*					
SystemEater.exe	7864	UDP	DESKTOP-EIHJ7...	59189	*	*					
wininit.exe	788	TCP	DESKTOP-EIHJ7...	49665	DESKTOP-EIHJ7...	0	LISTENING				
wininit.exe	788	TCPV6	desktop-eihj7rk	49665	desktop-eihj7rk	0	LISTENING				

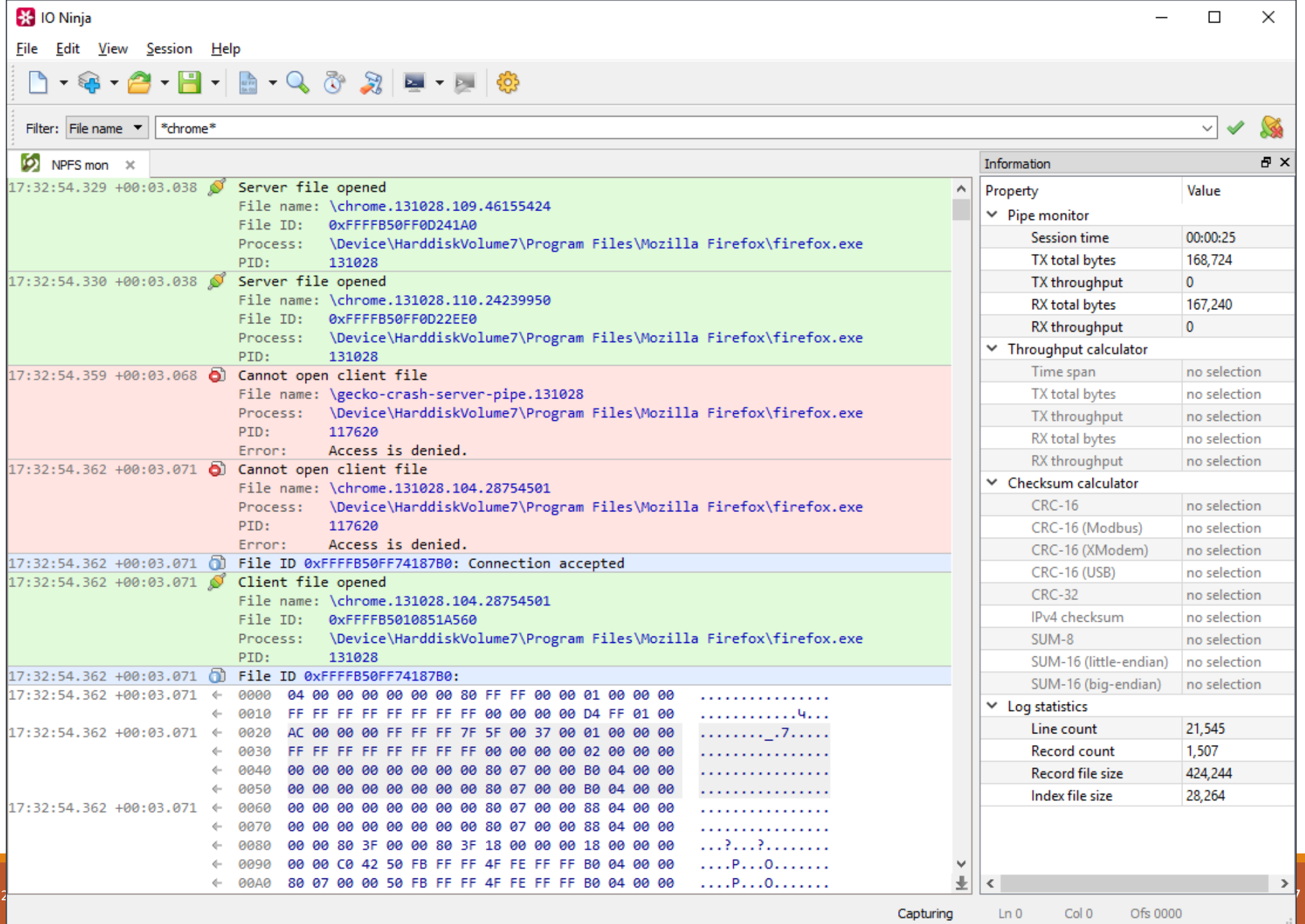
Endpoints: 46 | Established: 2 | Listening: 25 | Time Wait: 1 | Close Wait: 2

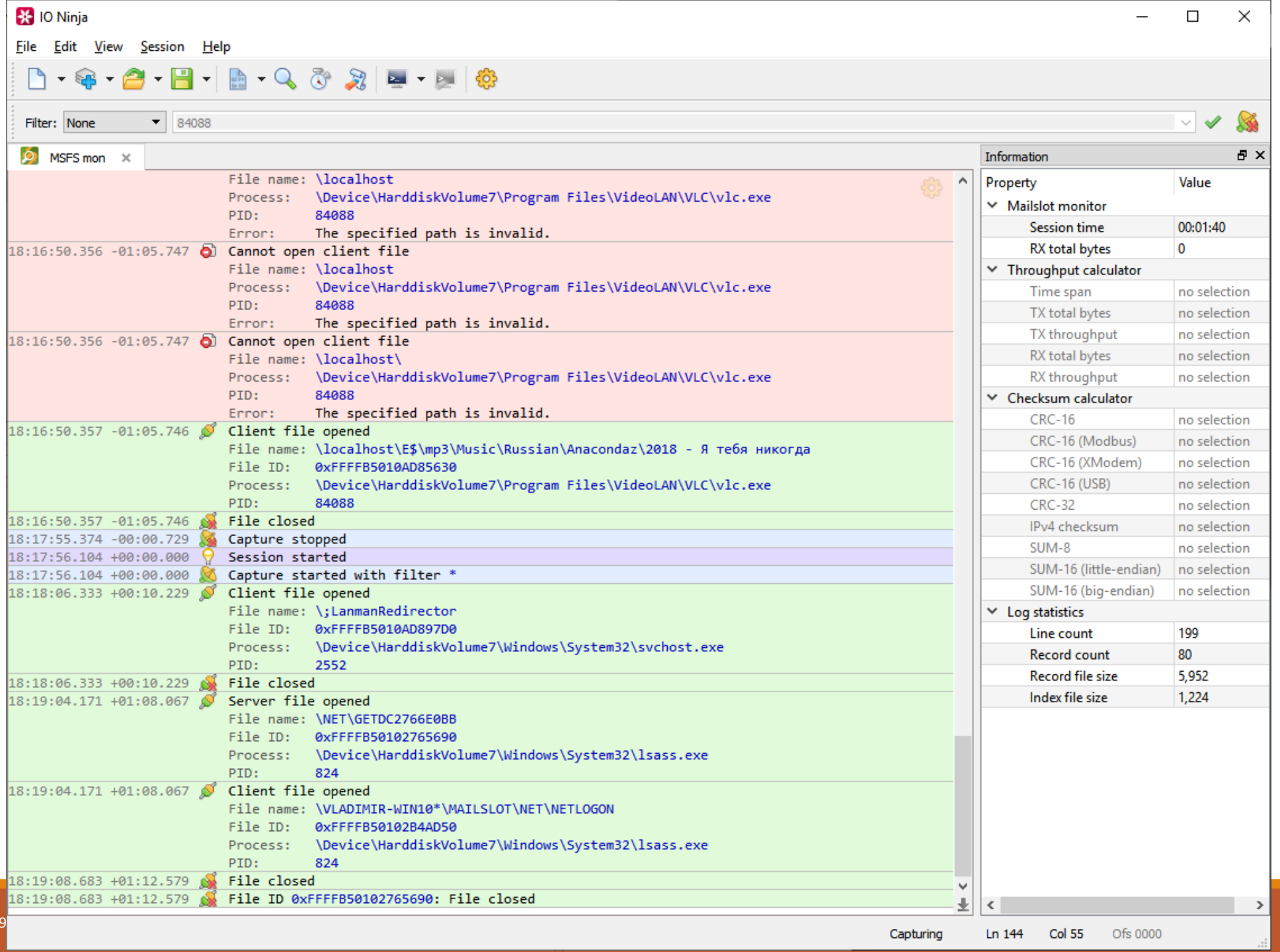
Microsoft Spy++ - [Messages (Window 00670A34)]

Spy Messages Search View Window Help

<000086> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000087> 00670A34 S WM_SETCURSOR hwnd:00140AD6 nHittest:HTCLIENT wMouseMsg:WM_MOUSEMOVE
<000088> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000089> 00670A34 S WM_SETCURSOR hwnd:00140AD6 nHittest:HTCLIENT wMouseMsg:WM_MOUSEMOVE
<000090> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000091> 00670A34 S WM_SETCURSOR hwnd:00140AD6 nHittest:HTCLIENT wMouseMsg:WM_MOUSEMOVE
<000092> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000093> 00670A34 S WM_SETCURSOR hwnd:00140AD6 nHittest:HTCLIENT wMouseMsg:WM_MOUSEMOVE
<000094> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000095> 00670A34 S WM_SETCURSOR hwnd:00140AD6 nHittest:HTCLIENT wMouseMsg:WM_MOUSEMOVE
<000096> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000097> 00670A34 S WM_SETCURSOR hwnd:00140AD6 nHittest:HTCLIENT wMouseMsg:WM_MOUSEMOVE
<000098> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000099> 00670A34 S WM_PARENTNOTIFY fwEvent:WM_LBUTTONDOWN xPos:470 yPos:117
<000100> 00670A34 R WM_PARENTNOTIFY
<000101> 00670A34 S WM_MOUSEACTIVATE hwndTopLevel:00670A34 nHittest:HTCLIENT uMsg:WM_LBUTTONDOWN
<000102> 00670A34 R WM_MOUSEACTIVATE fuActivate:MA_ACTIVATE
<000103> 00670A34 S WM_WINDOWPOSCHANGING lpwp:000000185E8DF9F0
<000104> 00670A34 R WM_WINDOWPOSCHANGING
<000105> 00670A34 S WM_WINDOWPOSCHANGED lpwp:000000185E8DF9F0
<000106> 00670A34 S message:0x0093 [Unknown] wParam:00000000 lParam:000000185E8DEE10
<000107> 00670A34 R message:0x0093 [Unknown] lResult:00000001
<000108> 00670A34 R WM_WINDOWPOSCHANGED
<000109> 00670A34 S WM_ACTIVATEAPP fActive:True dwThreadID:00000000
<000110> 00670A34 R WM_ACTIVATEAPP
<000111> 00670A34 S WM_NCACTIVATE fActive:True
<000112> 00670A34 S message:0x0093 [Unknown] wParam:00000000 lParam:000000185E8DE8C0
<000113> 00670A34 R message:0x0093 [Unknown] lResult:00000001
<000114> 00670A34 S message:0x0093 [Unknown] wParam:00000000 lParam:000000185E8DEFC0
<000115> 00670A34 R message:0x0093 [Unknown] lResult:00000001
<000116> 00670A34 S message:0x0091 [Unknown] wParam:00000000 lParam:000000185E8DEFC0
<000117> 00670A34 R message:0x0091 [Unknown] lResult:00000000
<000118> 00670A34 S message:0x0092 [Unknown] wParam:00000000 lParam:000000185E8DEF40
<000119> 00670A34 R message:0x0092 [Unknown] lResult:00000000
<000120> 00670A34 S message:0x0092 [Unknown] wParam:00000000 lParam:000000185E8DEF40
<000121> 00670A34 R message:0x0092 [Unknown] lResult:00000000
<000122> 00670A34 S message:0x0092 [Unknown] wParam:00000000 lParam:000000185E8DEF40
<000123> 00670A34 R message:0x0092 [Unknown] lResult:00000000
<000124> 00670A34 S message:0x0092 [Unknown] wParam:00000000 lParam:000000185E8DEF40
<000125> 00670A34 R message:0x0092 [Unknown] lResult:00000000
<000126> 00670A34 S message:0x0092 [Unknown] wParam:00000000 lParam:000000185E8DEF40
<000127> 00670A34 R message:0x0092 [Unknown] lResult:00000000
<000128> 00670A34 R WM_NCACTIVATE
<000129> 00670A34 S WM_ACTIVATE fActive:WA_CLICKACTIVE fMinimized:False hwndPrevious:(null)
<000130> 00670A34 S WM_IME_SETCONTEXT fSet:1 iShow:C000000F
<000131> 00670A34 S WM_IME_NOTIFY dwCommand:IMN_SETCOMPOSITIONWINDOW dwCommand:0000000B dwData:00000000
<000132> 00670A34 S WM_IME_NOTIFY dwCommand:000F dwCommand:0000000F dwData:01300D3D
<000133> 00670A34 R WM_IME_NOTIFY
<000134> 00670A34 R WM_IME_NOTIFY
<000135> 00670A34 S WM_IME_NOTIFY dwCommand:IMN_OPENSTATUSWINDOW dwCommand:00000002 dwData:00000000
<000136> 00670A34 R WM_IME_NOTIFY
<000137> 00670A34 R WM_IME_SETCONTEXT
<000138> 00670A34 S WM_GETOBJECT dwFlags:FFFFFFFF dwObjId:FFFFFFFC
<000139> 00670A34 R WM_GETOBJECT dwRet:FFFFFFFF
<000140> 00670A34 S WM_GETOBJECT dwFlags:00000000 dwObjId:FFFFFFF4
<000141> 00670A34 R WM_GETOBJECT dwRet:00000000
<000142> 00670A34 S WM_SETFOCUS hwndLoseFocus:(null)
<000143> 00670A34 S WM_KILLFOCUS hwndGetFocus:00140AD6
<000144> 00670A34 S WM_COMMAND wNotifyCode:EN_KILLFOCUS wID:15 hwndCtl:00140AD6
<000145> 00670A34 R WM_COMMAND
<000146> 00670A34 R WM_KILLFOCUS
<000147> 00670A34 S WM_IME_SETCONTEXT fSet:0 iShow:C000000F
<000148> 00670A34 R WM_IME_SETCONTEXT
<000149> 00670A34 S WM_COMMAND wNotifyCode:EN_SETFOCUS wID:15 hwndCtl:00140AD6
<000150> 00670A34 R WM_COMMAND
<000151> 00670A34 R WM_SETFOCUS
<000152> 00670A34 R WM_ACTIVATE
<000153> 00670A34 S WM_SETCURSOR hwnd:00140AD6 nHittest:HTCLIENT wMouseMsg:WM_LBUTTONDOWN
<000154> 00670A34 R WM_SETCURSOR fHaltProcessing:False
<000155> 00670A34 S WM_CTLCOLOREDIT hdcEdit:14011654 hwndEdit:00140AD6
<000156> 00670A34 R WM_CTLCOLOREDIT hBrush:001000FB
<000157> 00670A34 S WM_CTLCOLOREDIT hdcEdit:14011654 hwndEdit:00140AD6
<000158> 00670A34 R WM_CTLCOLOREDIT hBrush:001000FB

For Help, press F1 NUM


IO Ninja
File Edit View Session Help
Filter: File name *chrome*
NPFS mon
17:32:54.329 +00:03.038 Server file opened
File name: \chrome.131028.109.46155424
File ID: 0xFFFFB50FF0D241A0
Process: \Device\HarddiskVolume7\Program Files\Mozilla Firefox\firefox.exe
PID: 131028
17:32:54.330 +00:03.038 Server file opened
File name: \chrome.131028.110.24239950
File ID: 0xFFFFB50FF0D22EE0
Process: \Device\HarddiskVolume7\Program Files\Mozilla Firefox\firefox.exe
PID: 131028
17:32:54.359 +00:03.068 Cannot open client file
File name: \gecko-crash-server-pipe.131028
Process: \Device\HarddiskVolume7\Program Files\Mozilla Firefox\firefox.exe
PID: 117620
Error: Access is denied.
17:32:54.362 +00:03.071 Cannot open client file
File name: \chrome.131028.104.28754501
Process: \Device\HarddiskVolume7\Program Files\Mozilla Firefox\firefox.exe
PID: 117620
Error: Access is denied.
17:32:54.362 +00:03.071 File ID 0xFFFFB50FF74187B0: Connection accepted
17:32:54.362 +00:03.071 Client file opened
File name: \chrome.131028.104.28754501
File ID: 0xFFFFB5010851A560
Process: \Device\HarddiskVolume7\Program Files\Mozilla Firefox\firefox.exe
PID: 131028
17:32:54.362 +00:03.071 File ID 0xFFFFB50FF74187B0:
17:32:54.362 +00:03.071 0000 04 00 00 00 00 00 00 80 FF FF 00 00 01 00 00 00
0010 FF FF FF FF FF FF FF FF 00 00 00 00 D4 FF 01 00
17:32:54.362 +00:03.071 0020 AC 00 00 00 FF FF FF 7F 5F 00 37 00 01 00 00 00
0030 FF FF FF FF FF FF FF FF 00 00 00 00 02 00 00 00
0040 00 00 00 00 00 00 00 00 80 07 00 00 B0 04 00 00
0050 00 00 00 00 00 00 00 00 80 07 00 00 B0 04 00 00
17:32:54.362 +00:03.071 0060 00 00 00 00 00 00 00 00 80 07 00 00 88 04 00 00
0070 00 00 00 00 00 00 00 00 80 07 00 00 88 04 00 00
0080 00 00 80 3F 00 00 80 3F 18 00 00 00 18 00 00 00
0090 00 00 C0 42 50 FB FF FF 4F FE FF FF B0 04 00 00
00A0 80 07 00 00 50 FB FF FF 4F FE FF FF B0 04 00 00
Information
Property Value
Pipe monitor
Session time 00:00:25
TX total bytes 168,724
TX throughput 0
RX total bytes 167,240
RX throughput 0
Throughput calculator
Time span no selection
TX total bytes no selection
TX throughput no selection
RX total bytes no selection
RX throughput no selection
Checksum calculator
CRC-16 no selection
CRC-16 (Modbus) no selection
CRC-16 (XModem) no selection
CRC-16 (USB) no selection
CRC-32 no selection
IPv4 checksum no selection
SUM-8 no selection
SUM-16 (little-endian) no selection
SUM-16 (big-endian) no selection
Log statistics
Line count 21,545
Record count 1,507
Record file size 424,244
Index file size 28,264
Capturing
Ln 0
Col 0
Ofs 0000


IO Ninja
File Edit View Session Help
Filter: None
84088
MSFS mon
File name: \localhost
Process: \Device\HarddiskVolume7\Program Files\VideoLAN\VLC\vlc.exe
PID: 84088
Error: The specified path is invalid.
18:16:50.356 -01:05.747 Cannot open client file
File name: \localhost
Process: \Device\HarddiskVolume7\Program Files\VideoLAN\VLC\vlc.exe
PID: 84088
Error: The specified path is invalid.
18:16:50.356 -01:05.747 Cannot open client file
File name: \localhost\
Process: \Device\HarddiskVolume7\Program Files\VideoLAN\VLC\vlc.exe
PID: 84088
Error: The specified path is invalid.
18:16:50.357 -01:05.746 Client file opened
File name: \localhost\E$\mp3\Music\Russian\Anacondaz\2018 - Я тебя никогда
File ID: 0xFFFFB5010AD85630
Process: \Device\HarddiskVolume7\Program Files\VideoLAN\VLC\vlc.exe
PID: 84088
18:16:50.357 -01:05.746 File closed
18:17:55.374 -00:00.729 Capture stopped
18:17:56.104 +00:00.000 Session started
18:17:56.104 +00:00.000 Capture started with filter *
18:18:06.333 +00:10.229 Client file opened
File name: \;LanmanRedirector
File ID: 0xFFFFB5010AD897D0
Process: \Device\HarddiskVolume7\Windows\System32\svchost.exe
PID: 2552
18:18:06.333 +00:10.229 File closed
18:19:04.171 +01:08.067 Server file opened
File name: \NET\GETDC2766E0BB
File ID: 0xFFFFB50102765690
Process: \Device\HarddiskVolume7\Windows\System32\lsass.exe
PID: 824
18:19:04.171 +01:08.067 Client file opened
File name: \VLADIMIR-WIN10*\MAILSLOT\NET\NETLOGON
File ID: 0xFFFFB50102B4AD50
Process: \Device\HarddiskVolume7\Windows\System32\lsass.exe
PID: 824
18:19:08.683 +01:12.579 File closed
18:19:08.683 +01:12.579 File ID 0xFFFFB50102765690: File closed
Information
Property Value
Mailslot monitor
Session time 00:01:40
RX total bytes 0
Throughput calculator
Time span no selection
TX total bytes no selection
TX throughput no selection
RX total bytes no selection
RX throughput no selection
Checksum calculator
CRC-16 no selection
CRC-16 (Modbus) no selection
CRC-16 (XModem) no selection
CRC-16 (USB) no selection
CRC-32 no selection
IPv4 checksum no selection
SUM-8 no selection
SUM-16 (little-endian) no selection
SUM-16 (big-endian) no selection
Log statistics
Line count 199
Record count 80
Record file size 5,952
Index file size 1,224
Capturing
Ln 144
Col 55
Ofs 0000

RPCMon - RPC Monitor Based Windows Events (Administrator)

File DB Options Help

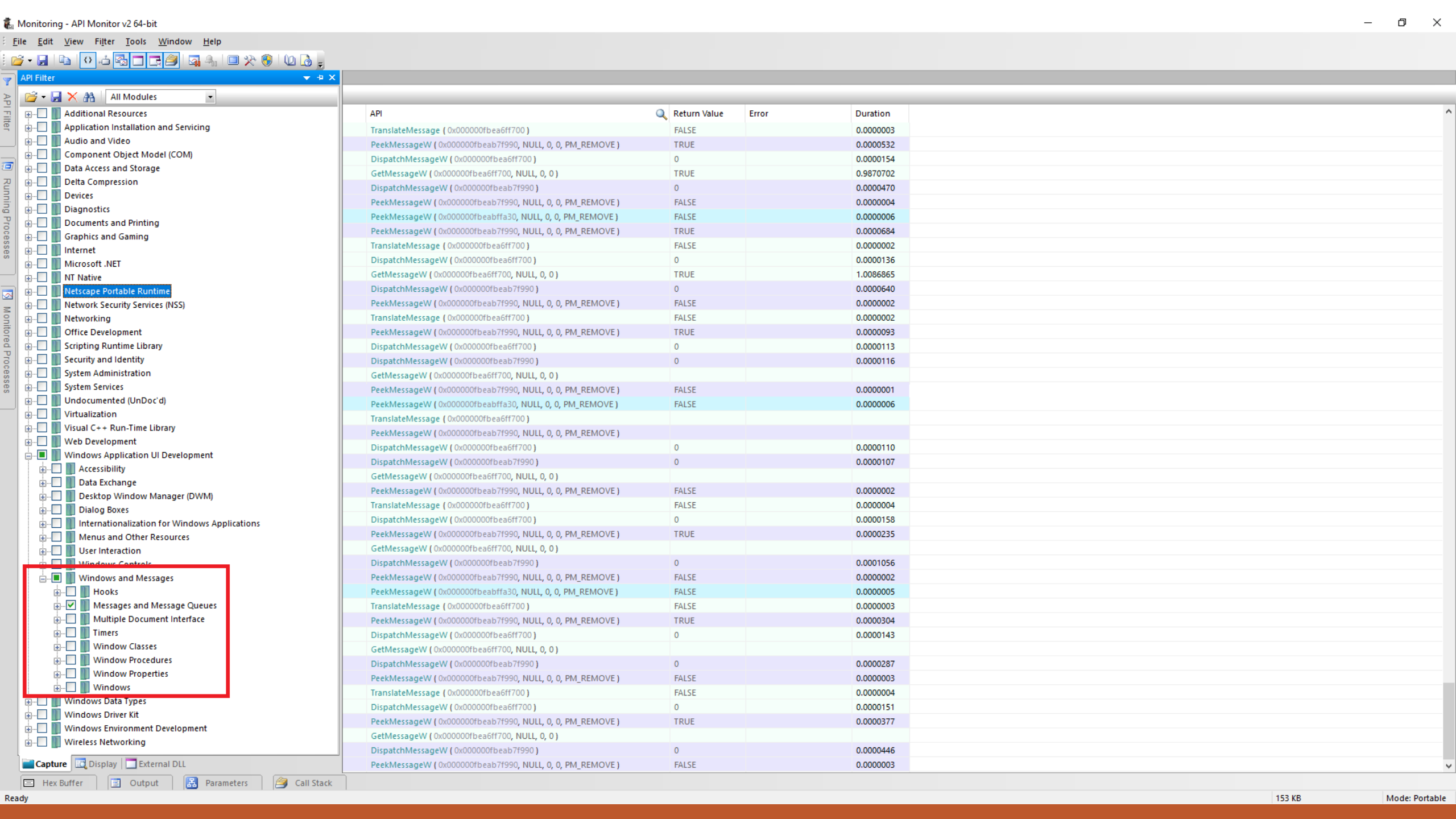
PID	TID	ProcessName	UUID	Module	Service	Function	Protocol	Endpoint	ImpersonationLevel	TaskName
5216	3484	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
1524	1976	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Default	RpcServerCallStart
1076	8456	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Impersonate	RpcClientCallStart
1524	8064	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Default	RpcServerCallStart
1524	8064	svchost	e60c73e6-88f9-11cf-9af1-0020af6e72f4	rpcss.dll	RpcSs	ServerAllocateOIDs	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	5708	svchost	e60c73e6-88f9-11cf-9af1-0020af6e72f4	rpcss.dll	RpcSs	ServerAllocateOIDs	LRPC	epmapper	Default	RpcServerCallStart
5216	3952	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
5216	11148	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
1524	1976	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Default	RpcServerCallStart
1076	8456	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Impersonate	RpcClientCallStart
1524	8064	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Default	RpcServerCallStart
3504	2872	RPCMon	4f32adc8-6052-4a04-8701-293ccf2096f0	sspicli.dll		SspiClientCallback	LRPC	lsasspirpc	Default	RpcClientCallStart
956	8788	lsass	4f32adc8-6052-4a04-8701-293ccf2096f0	sspicli.dll		SspiClientCallback	LRPC	lsasspirpc	Default	RpcServerCallStart
3504	2872	RPCMon	4f32adc8-6052-4a04-8701-293ccf2096f0	sspicli.dll		N\A	LRPC	lsasspirpc	Default	RpcClientCallStart
956	8788	lsass	4f32adc8-6052-4a04-8701-293ccf2096f0	sspicli.dll		N\A	LRPC	lsasspirpc	Default	RpcServerCallStart
5216	9328	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
5216	7964	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
1524	1976	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Default	RpcServerCallStart
1076	8456	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Impersonate	RpcClientCallStart
1524	8064	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Default	RpcServerCallStart
2264	1892	explorer	e60c73e6-88f9-11cf-9af1-0020af6e72f4	rpcss.dll	RpcSs	_ServerFreeOXIDAndOIDs	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	e60c73e6-88f9-11cf-9af1-0020af6e72f4	rpcss.dll	RpcSs	_ServerFreeOXIDAndOIDs	LRPC	epmapper	Default	RpcServerCallStart
5216	5800	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
5216	7464	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
1524	1976	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Default	RpcServerCallStart
1076	8456	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Impersonate	RpcClientCallStart
1524	8064	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Default	RpcServerCallStart
5216	7780	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
5216	10252	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
1524	1976	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Default	RpcServerCallStart
1076	8456	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Impersonate	RpcClientCallStart
1524	8064	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Default	RpcServerCallStart
5216	6060	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
3672	10528	RuntimeBroker	412f241e-c12a-11ce-abff-0020af6e7a17	rpcss.dll	RpcSs	ServerRevokeClsid	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	412f241e-c12a-11ce-abff-0020af6e7a17	rpcss.dll	RpcSs	ServerRevokeClsid	LRPC	epmapper	Default	RpcServerCallStart
7712	11236	taskhostw	9d420415-b8fb-4f4a-8c53-4502ead30ca9	PlaySndSrv.dll		I_PlaySoundkPostMessage	LRPC	PlaySoundKRpc2	Default	RpcServerCallStart
5216	4192	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart
1128	4380	svchost	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Default	RpcServerCallStart
1524	1976	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Impersonate	RpcClientCallStart
1076	8456	svchost	00000136-0000-0000-c000-000000000046	rpcss.dll	RpcSs	SCMActivatorCreateInstance	LRPC	epmapper	Default	RpcServerCallStart
1076	8456	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Impersonate	RpcClientCallStart
1524	8064	svchost	00000132-0000-0000-c000-000000000046	N\A	N\A	N\A	LRPC	OLE951E60D9F86E61D184DC8C7AF8AE	Default	RpcServerCallStart
5216	3496	SECOMN64	11f25515-c879-400a-989e-b074d5f092fe	lsm.dll	LSM	RpcGetUserToken	LRPC	LSMApi	Impersonate	RpcClientCallStart

Shown events: 265/265 | Selected events: 1 DB File: RPC_UUID_Map_Windows10_1909_18363.1977.rpcdb.json

Debugging

CTRL+ALT+HOME activates the connection bar. Please change that to a different combination.

HTTPS://LEARN.MICROSOFT.COM/EN-US/WINDOWS/WIN32/TERMSERV/TERMINAL-SERVICES-SHORTCUT-KEYS


Monitoring - API Monitor v2 64-bit
File Edit View Filter Tools Window Help
API Filter
All Modules
Additional Resources
Application Installation and Servicing
Audio and Video
Component Object Model (COM)
Data Access and Storage
Delta Compression
Devices
Diagnostics
Documents and Printing
Graphics and Gaming
Internet
Microsoft .NET
NT Native
Netscape Portable Runtime
Network Security Services (NSS)
Networking
Office Development
Scripting Runtime Library
Security and Identity
System Administration
System Services
Undocumented (UnDoc'd)
Virtualization
Visual C++ Run-Time Library
Web Development
Windows Application UI Development
Accessibility
Data Exchange
Desktop Window Manager (DWM)
Dialog Boxes
Internationalization for Windows Applications
Menus and Other Resources
User Interaction
Windows and Messages
Hooks
Messages and Message Queues
Multiple Document Interface
Timers
Window Classes
Window Procedures
Window Properties
Windows
Windows Data Types
Windows Driver Kit
Windows Environment Development
Wireless Networking
Capture
Display
External DLL
Hex Buffer
Output
Parameters
Call Stack
API
Return Value
Error
Duration
TranslateMessage (0x000000fbea6ff700) FALSE 0.0000003
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) TRUE 0.0000532
DispatchMessageW (0x000000fbea6ff700) 0 0.0000154
GetMessageW (0x000000fbea6ff700, NULL, 0, 0) TRUE 0.9870702
DispatchMessageW (0x000000fbeab7f990) 0 0.0000470
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) FALSE 0.0000004
PeekMessageW (0x000000fbeabffa30, NULL, 0, 0, PM_REMOVE) FALSE 0.0000006
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) TRUE 0.0000684
TranslateMessage (0x000000fbea6ff700) FALSE 0.0000002
DispatchMessageW (0x000000fbea6ff700) 0 0.0000136
GetMessageW (0x000000fbea6ff700, NULL, 0, 0) TRUE 1.0086865
DispatchMessageW (0x000000fbeab7f990) 0 0.0000640
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) FALSE 0.0000002
TranslateMessage (0x000000fbea6ff700) FALSE 0.0000002
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) TRUE 0.0000093
DispatchMessageW (0x000000fbea6ff700) 0 0.0000113
DispatchMessageW (0x000000fbeab7f990) 0 0.0000116
GetMessageW (0x000000fbea6ff700, NULL, 0, 0)
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) FALSE 0.0000001
PeekMessageW (0x000000fbeabffa30, NULL, 0, 0, PM_REMOVE) FALSE 0.0000006
TranslateMessage (0x000000fbea6ff700)
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE)
DispatchMessageW (0x000000fbea6ff700) 0 0.0000110
DispatchMessageW (0x000000fbeab7f990) 0 0.0000107
GetMessageW (0x000000fbea6ff700, NULL, 0, 0)
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) FALSE 0.0000002
TranslateMessage (0x000000fbea6ff700) FALSE 0.0000004
DispatchMessageW (0x000000fbea6ff700) 0 0.0000158
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) TRUE 0.0000235
GetMessageW (0x000000fbea6ff700, NULL, 0, 0)
DispatchMessageW (0x000000fbeab7f990) 0 0.0001056
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) FALSE 0.0000002
PeekMessageW (0x000000fbeabffa30, NULL, 0, 0, PM_REMOVE) FALSE 0.0000005
TranslateMessage (0x000000fbea6ff700) FALSE 0.0000003
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) TRUE 0.0000304
DispatchMessageW (0x000000fbea6ff700) 0 0.0000143
GetMessageW (0x000000fbea6ff700, NULL, 0, 0)
DispatchMessageW (0x000000fbeab7f990) 0 0.0000287
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) FALSE 0.0000003
TranslateMessage (0x000000fbea6ff700) FALSE 0.0000004
DispatchMessageW (0x000000fbea6ff700) 0 0.0000151
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) TRUE 0.0000377
GetMessageW (0x000000fbea6ff700, NULL, 0, 0)
DispatchMessageW (0x000000fbeab7f990) 0 0.0000446
PeekMessageW (0x000000fbeab7f990, NULL, 0, 0, PM_REMOVE) FALSE 0.0000003
Ready
153 KB
Mode: Portable

Monitoring - API Monitor v2 64-bit

File Edit View Filter Tools Window Help

API Filter

All Modules

- Messages and Message Queues
  - User32.dll
    - BroadcastSystemMessage
    - BroadcastSystemMessageExA
    - BroadcastSystemMessageExW
    - DispatchMessageA
    - DispatchMessageW
    - GetInputState
    - GetMessageA
    - GetMessageExtraInfo
    - GetMessagePos
    - GetMessageTime
    - GetMessageW
    - GetQueueStatus
    - InSendMessage
    - InSendMessageEx
    - PeekMessageA
    - PeekMessageW
    - PostMessageA
    - PostMessageW
    - PostQuitMessage
    - PostThreadMessageA
    - PostThreadMessageW
    - RegisterWindowMessageA
    - RegisterWindowMessageW
    - ReplyMessage
    - SendMessageA
    - SendMessageCallbackA
    - SendMessageCallbackW
    - SendMessageTimeoutA
    - SendMessageTimeoutW
    - SendMessageW
    - SendNotifyMessageA
    - SendNotifyMessageW
    - SetMessageExtraInfo
    - TranslateMessage
    - WaitMessage
  - Multiple Document Interface
  - Timers
  - Window Classes
  - Window Procedures
  - Window Properties
  - Windows
- Windows Data Types
- Windows Driver Kit
- Windows Environment Development
- Wireless Networking

Capture | Display | External DLL

Summary | 194 calls | 75 KB used | mstsc.exe

#	Time of Day	Thread	Module	API	Return Value	Error	Du
43	8:41:25.627 AM	6	IMM32.DLL	SendMessageW (0x000000000009051c, WM_IME_SETCONTEXT, 1, 3221225487)	0		0.(
44	8:41:25.629 AM	6	IMM32.DLL	SendMessageW (0x000000000009051c, WM_IME_SETCONTEXT, 0, 3221225487)	0		0.(
45	8:41:31.926 AM	1	IMM32.DLL	SendMessageW (0x00000000000d0652, WM_IME_SETCONTEXT, 1, 3221225487)	0		0.(
46	8:41:31.926 AM	1	IMM32.DLL	SendMessageW (0x00000000000d0652, WM_IME_SETCONTEXT, 0, 3221225487)	0		0.(
47	8:41:31.926 AM	1	IMM32.DLL	SendMessageW (0x00000000000805fe, WM_IME_SETCONTEXT, 1, 3221225487)	0		0.(
48	8:41:31.926 AM	1	IMM32.DLL	SendMessageW (0x00000000000805fe, WM_IME_SETCONTEXT, 0, 3221225487)	0		0.(
49	8:41:31.926 AM	1	IMM32.DLL	SendMessageW (0x00000000000f0484, WM_IME_SETCONTEXT, 1, 3221225487)	0		0.(
50	8:41:31.926 AM	1	IMM32.DLL	SendMessageW (0x00000000000f0484, WM_IME_SETCONTEXT, 0, 3221225487)	0		0.(
51	8:41:31.927 AM	6	IMM32.DLL	SendMessageW (0x000000000009051c, WM_IME_SETCONTEXT, 1, 3221225487)	0		0.(
52	8:41:33.498 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYDOWN, 162, 1900545)	TRUE		0.(
53	8:41:33.604 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYDOWN, 164, 3670017)	TRUE		0.(
54	8:41:33.679 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYDOWN, 45, 22151169)	TRUE		0.(
55	8:41:33.814 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYUP, 45, -2125332479)	TRUE		0.(
56	8:41:33.846 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYUP, 164, -2143813631)	TRUE		0.(
57	8:41:33.873 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYUP, 162, -2145583103)	TRUE		0.(
58	8:41:34.052 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYDOWN, 162, 1900545)	TRUE		0.(
59	8:41:34.078 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYDOWN, 164, 3670017)	TRUE		0.(
60	8:41:34.218 AM	6	mstscax.dll	PostMessageW (0x000000000009051c, WM_KEYDOWN, 36, 21430273)	TRUE		0.(
61	8:41:34.218 AM	6	mstscax.dll	PostMessageW (0x00000000000d0740, WM_USER+19, 140710098758112, 1952893682784)	TRUE		0.(
62	8:42:07.623 AM	6	IMM32.DLL	SendMessageW (0x000000000009051c, WM_IME_SETCONTEXT, 0, 3221225487)	0		0.(
63	8:42:07.623 AM	1	IMM32.DLL	SendMessageW (0x0000000000090398, WM_IME_SETCONTEXT, 1, 3221225487)	0		0.(
64	8:42:07.623 AM	1	IMM32.DLL	SendMessageW (0x0000000000090398, WM_IME_SETCONTEXT, 0, 3221225487)	0		0.(
65	8:42:07.623 AM	1	IMM32.DLL	SendMessageW (0x0000000000080524, WM_IME_SETCONTEXT, 1, 3221225487)	0		0.(
66	8:42:07.623 AM	1	mstscax.dll	SendMessageW (0x00000000001601ee, WM_NOTIFY, 590744, 385610150128)	1		0.(
67	8:42:07.624 AM	1	mstscax.dll	SendMessageW (0x0000000000080524, WM_USER+12, 3, 0)	0		0.(
68	8:42:07.624 AM	1	mstscax.dll	SendMessageW (0x0000000000080524, WM_USER+12, 4, 0)	0		0.(
69	8:42:07.624 AM	1	mstscax.dll	SendMessageW (0x0000000000080524, WM_USER+94, 1, 16)	0		0.(
70	8:42:07.624 AM	1	COMCTL32.dll	SendMessageW (0x0000000000090398, WM_NOTIFY, 0, 385610146752)	1		0.(
71	8:42:07.624 AM	1	mstscax.dll	SendMessageW (0x0000000000080524, WM_USER+94, 4294967295, 33)	1		0.(
72	8:42:07.624 AM	1	COMCTL32.dll	SendMessageW (0x0000000000090398, WM_NOTIFY, 0, 385610145584)	0		0.(
73	8:42:07.624 AM	1	COMCTL32.dll	SendMessageW (0x000000000009053c, WM_USER+53, 0, 385610145440)	1		0.(
74	8:42:07.624 AM	1	COMCTL32.dll	SendMessageW (0x000000000009053c, WM_USER+17, 0, 385610145440)	1		0.(
75	8:42:07.624 AM	1	COMCTL32.dll	SendMessageW (0x000000000009053c, WM_USER+54, 0, 385610145440)	0		0.(

API PostMessageW
Module User32.dll
Category Messages and Message Queues

PostMessageW (
0x000000000009051c,
WM_KEYDOWN,
36,
21430273
);

Call Stack: PostMessageW (User32.dll)

#	Module	Address	Offset	Location
1	mstscax.dll	0x00007ff99f4e707f	0xb707f	
2	mstscax.dll	0x00007ff99f4557b1	0x257b1	
3	mstscax.dll	0x00007ff99f453fd2	0x23fd2	
4	mstscax.dll	0x00007ff99f4e2fc2	0xb2fc2	

Hex Buffer | Output | Parameters: PostMessageW (User32.dll)

Ready | 75 KB | Mode: Portable

Pid 7352 - WinDbg:10.0.22621.1778 AMD64

File Edit View Debug Window Help

Command

```
ModLoad: 00007ff9`d2630000 00007ff9`d2642000   C:\Windows\system32\cscapi.dll
ModLoad: 00007ff9`e9380000 00007ff9`e9421000   C:\windows\SYSTEM32\policymanager.dll
ModLoad: 00007ff9`bfa60000 00007ff9`bfb05000   C:\Windows\system32\WINSPOOL.DRV
ModLoad: 00007ff9`ea7b0000 00007ff9`ea7ef000   C:\windows\System32\netprofm.dll
ModLoad: 00007ff9`dd010000 00007ff9`dd020000   C:\windows\System32\npmproxy.dll
ModLoad: 00007ff9`e40e0000 00007ff9`e40f7000   C:\windows\SYSTEM32\dhcpcsvc6.DLL
ModLoad: 00007ff9`e6620000 00007ff9`e663d000   C:\windows\SYSTEM32\dhcpcsvc.DLL
ModLoad: 00007ff9`a00f0000 00007ff9`a04a5000   C:\Windows\System32\DriverStore\FileRepository\prnms003.inf_amd64_ddecfc8d679b6224\Amd64\PrintConfig.dll
ModLoad: 00007ff9`f2e20000 00007ff9`f2e4e000   C:\windows\SYSTEM32\USERENV.dll
ModLoad: 00007ff9`cbe20000 00007ff9`cbe52000   C:\windows\SYSTEM32\prntvpt.dll
ModLoad: 00007ff9`d7330000 00007ff9`d751d000   C:\windows\SYSTEM32\urlmon.dll
ModLoad: 00007ff9`de6c0000 00007ff9`de97c000   C:\Windows\System32\iertutil.dll
ModLoad: 00007ff9`a9c30000 00007ff9`a9d06000   C:\Windows\System32\jscript.dll
ModLoad: 00007ff9`dae60000 00007ff9`daee1000   C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24070.5-0\MpOav.dll
ModLoad: 00007ff9`f2d30000 00007ff9`f2dd2000   C:\windows\SYSTEM32\sxs.dll
ModLoad: 00007ff9`d90d0000 00007ff9`d912b000   C:\Windows\system32\Bcp47Langs.dll
ModLoad: 00007ff9`d8a70000 00007ff9`d8a9d000   C:\Windows\system32\bcp47mrm.dll
ModLoad: 00007ff9`c7530000 00007ff9`c755a000   C:\windows\system32\spool\DRIVERS\x64\3\FXSUI.DLL
ModLoad: 00007ff9`bd200000 00007ff9`bd229000   C:\windows\system32\spool\DRIVERS\x64\3\FXSWZRD.dll
ModLoad: 00007ff9`a94f0000 00007ff9`a955b000   C:\windows\system32\spool\DRIVERS\x64\3\FXSTIFF.dll
ModLoad: 00007ff9`bcba0000 00007ff9`bcbe2000   C:\windows\SYSTEM32\TAPI32.dll
ModLoad: 000001c6`d0410000 000001c6`d0ac3000   C:\windows\system32\spool\DRIVERS\x64\3\FXSRES.DLL
ModLoad: 00007ff9`a94a0000 00007ff9`a94ed000   C:\windows\system32\spool\DRIVERS\x64\3\FXSAPI.DLL
ModLoad: 00007ff9`eac40000 00007ff9`eac4d000   C:\windows\system32\spool\DRIVERS\x64\3\FXSDRV.DLL
(1cb8.2264): Break instruction exception - code 80000003 (first chance)
ntdll!DbgBreakPoint:
00007ff9`f58f0b10 cc              int     3
0:025> bu bu 0x00007ff99f4e707f
*** Bp expression 'bu ' contains symbols not qualified with module name.
                    ^ Range error in 'bu bu 0x00007ff99f4e707f'
0:025> bu 0x00007ff99f4e707f
*** Unable to resolve unqualified symbol in Bp expression 'bu '.
0:025> g
Breakpoint 1 hit
mstscax!PAL_System_ThreadSignalPulse+0x2b:
00007ff9`9f4e707f 0f1f440000      nop     dword ptr [rax+rax]
0:002> kb
 # RetAddr               : Args to Child                                                 : Call Site
00 00007ff9`9f4557b1     : 49470b2b`ae785134 0000eedd`98a034a2 0000533d`00e1a6e5 000001c6`b42d6bc0 : mstscax!PAL_System_ThreadSignalPulse+0x2b
01 00007ff9`9f453fd2     : 00000000`00000000 00000059`c84fef68 00000000`00000000 00000000`00000000 : mstscax!CTSThread::SignalEventQueue+0x71
02 00007ff9`9f4e2fc2     : 000001c6`b188d540 000001c6`b4266740 00000000`00000000 00000059`00000001 : mstscax!CTSThread::AddCallback+0x392
03 00007ff9`9f487635     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000024 : mstscax!CTSCoreEventSource::InternalFireAsyncNotification+0xca
04 00007ff9`9f486285     : 00000000`00000100 00000000`00000000 00000000`00000000 00000024 000001c6`b3e6b828 : mstscax!CTSInput::IHPostMessageToMainWindow+0x1c5
05 00007ff9`9f4861a8     : 00000000`00000001 00000000`01470001 00000000`01af054d 00000000`0009051c : mstscax!CTSInput::IHInputCaptureWndProc+0x85
*** Unable to resolve unqualified symbol in Bp expression 'bu '.
06 00007ff9`f3fbe858     : 00000000`00000001 00000059`c84ff540 00000000`00000000 00000000`80000022 : mstscax!CTSInput::IHStaticInputCaptureWndProc+0x58
07 00007ff9`f3fbe299     : 00000000`00003dff 00007ff9`9f486150 00000000`0009051c 000001c6`00000100 : USER32!UserCallWinProcCheckWow+0x2f8
*** Unable to resolve unqualified symbol in Bp expression 'bu '.
08 00007ff9`eac5ab32     : 00007ff9`9f486150 00000000`00000000 00007ff9`9f430000 00000000`00000000 : USER32!DispatchMessageWorker+0x249
09 00007ff9`eac53cdc     : 000001c6`b56097e0 00007ff9`f58747b1 000001c6`0000008e 00007ff9`00000000 : apimonitor_drv_x64+0xab32
0a 000001c6`b3f1350f     : 000001c6`b387da6a 00000000`00000001 00000000`00000001 00000000`00000001 : apimonitor_drv_x64+0x3cdc
0b 000001c6`b387da6a     : 00000000`00000001 00000000`00000001 00000000`00000001 000001c6`b4271a90 : 0x000001c6`b3f1350f
0c 00000000`00000001     : 00000000`00000001 00000000`00000001 000001c6`b4271a90 00007ff9`9f4375fc : 0x000001c6`b387da6a
0d 00000000`00000001     : 00000000`00000001 000001c6`b4271a90 00007ff9`9f4375fc 00000059`c84ff6f0 : 0x1
0e 00000000`00000001     : 000001c6`b4271a90 00007ff9`9f4375fc 00000059`c84ff6f0 00000000`00000000 : 0x1
0f 000001c6`b4271a90     : 00007ff9`9f4375fc 00000059`c84ff6f0 00000000`00000000 00000059`c84ff318 : 0x1
10 00007ff9`9f4375fc     : 00000059`c84ff6f0 00000000`00000000 00000059`c84ff318 00000000`00000001 : 0x000001c6`b4271a90
11 00007ff9`9f437424     : 00000000`00000000 49470b2b`ae785134 00000000`00001790 0000533d`0019259f : mstscax!PAL_System_CondWait+0x1cc
12 00007ff9`9f450f55     : 00000000`00000400 00000000`00000000 00000059`c84ffb30 000001c6`b42c38e0 : mstscax!CTSThreadInternal::ThreadSignalWait+0x34
13 00007ff9`9f451f6d     : 00000000`00000000 00000000`00000000 000001c6`b42c38e0 00000000`00000400 : mstscax!CTSThread::internalMsgPump+0x6d
14 00007ff9`9f4e691c     : 00000000`00000000 00007ff9`9f44e20d 000001c6`b4266d90 00007ff9`9f73f960 : mstscax!CTSThread::internalThreadMsgLoop+0x14d
15 00007ff9`9f888ad0     : 00007ff9`9fbd5808 00000059`c84ffb30 00000000`00000000 000001c6`b4272ab0 : mstscax!CTSThread::ThreadMsgLoop+0x1c
16 00007ff9`9f73f218     : 000001c6`b42c38e0 000001c6`b4272ab0 000001c6`b42c38e0 000001c6`b427a988 : mstscax!CSND::SND_Main+0x148
17 00007ff9`9f747932     : 000001c6`b42c5ec0 000001c6`b42c38e0 00000059`c827e430 00000000`00000000 : mstscax!CTSThread::TSStaticThreadEntry+0x258
*** Unable to resolve unqualified symbol in Bp expression 'bu '.
18 00007ff9`f4c47344     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : mstscax!PAL_System_Win32_ThreadProcWrapper+0x32
19 00007ff9`f58a26b1     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14
1a 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21
```

0:002>

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:1cb8 | Thrd 002:1790 | ASM | OVR | CAPS | NUM

IDA - mstscax.dll C:\Windows\System32\mstscax.dll

File Edit Jump Search View Debugger Options Windows Help

Local Windows debugger

Library function | Regular function | Instruction | Data | Unexplored | External symbol | Lumina function

Functions

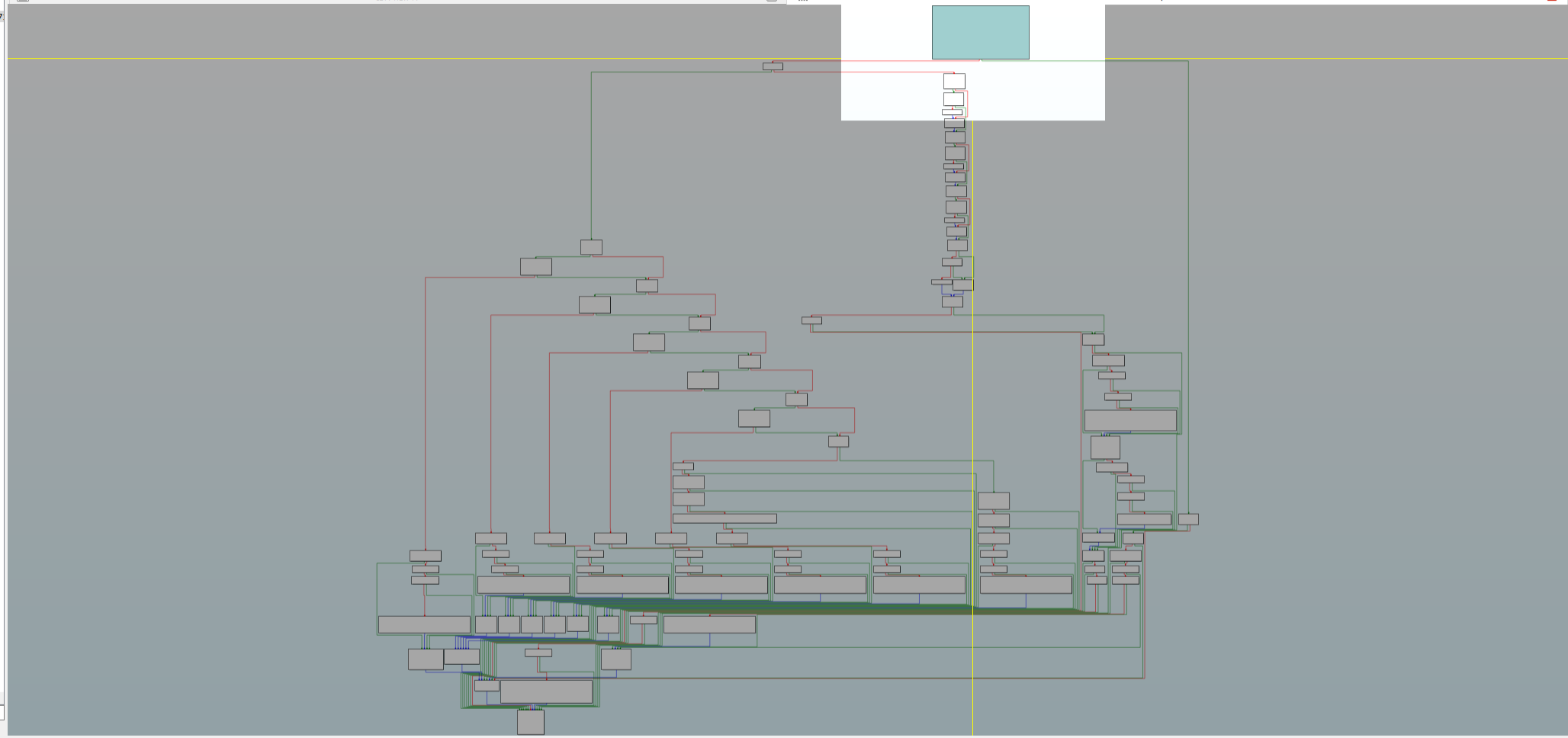
Function name	Segment	Start
CTSInput::IHPostMessageToMainWindow(uint,unsigned _...	.text	000000016A657

IHPostMessageToMainWind

Line 1 of 1, /?IHPostMessageToMainWindow@CTSInput@@AEAAHI_K_J@Z

IDA View-A, Graph overview | Hex View-1 | Local Types | Imports | Exports

IDA View-A | Graph overview



Output

```
16AA4EF30: propagate_stkargs: function is already typed
16AAADF40: propagate_stkargs: function is already typed
16A607490: propagate_stkargs: function is already typed
16A7F9750: propagate_stkargs: function is already typed
16A7F97B0: propagate_stkargs: function is already typed
16AA4ED90: propagate_stkargs: function is already typed
16AAADFF0: propagate_stkargs: function is already typed
16A747430: propagate_stkargs: function is already typed
16AA00C00: propagate_stkargs: function is already typed
Function argument information has been propagated
The initial autoanalysis has been finished.
WindowStateChange Graph overview
Command "JumpEnterNew" failed
```


IDC

AU: idle | Down | Disk: 8GB

Pid 7352 - WinDbg:10.0.22621.1778 AMD64

File Edit View Debug Window Help

Command

```
00007ff9`9f48751e 415e            pop     r14
00007ff9`9f487520 5f              pop     rdi
00007ff9`9f487521 c3              ret
00007ff9`9f487522 cc              int     3
00007ff9`9f487523 81fe13010000    cmp     esi,113h
00007ff9`9f487529 0f851f010000    jne     mstscax!CTSInput::IHPostMessageToMainWindow+0x1de (00007ff9`9f48764e)
00007ff9`9f48752f bb01000000      mov     ebx,1
00007ff9`9f487534 ebd1            jmp     mstscax!CTSInput::IHPostMessageToMainWindow+0x97 (00007ff9`9f487507)
00007ff9`9f487536 8b8128030000    mov     eax,dword ptr [rcx+328h]
00007ff9`9f48753c be00800000      mov     esi,8000h
00007ff9`9f487541 483be8          cmp     rbp,rax
00007ff9`9f487544 0f8470010000    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x24a (00007ff9`9f4876ba)
00007ff9`9f48754a 8b8744030000    mov     eax,dword ptr [rdi+344h]
00007ff9`9f487550 483be8          cmp     rbp,rax
00007ff9`9f487553 0f84dc010000    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x2c5 (00007ff9`9f487735)
00007ff9`9f487559 8b8748030000    mov     eax,dword ptr [rdi+348h]
00007ff9`9f48755f 483be8          cmp     rbp,rax
00007ff9`9f487562 0f8440020000    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x338 (00007ff9`9f4877a8)
00007ff9`9f487568 8b874c030000    mov     eax,dword ptr [rdi+34Ch]
00007ff9`9f48756e 483be8          cmp     rbp,rax
00007ff9`9f487571 0f84a4020000    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x3ab (00007ff9`9f48781b)
00007ff9`9f487577 8b8750030000    mov     eax,dword ptr [rdi+350h]
00007ff9`9f48757d 483be8          cmp     rbp,rax
00007ff9`9f487580 0f8408030000    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x41e (00007ff9`9f48788e)
00007ff9`9f487586 4883fd24        cmp     rbp,24h
00007ff9`9f48758a 0f8471030000    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x491 (00007ff9`9f487901)
00007ff9`9f487590 4883fd2d        cmp     rbp,2Dh
00007ff9`9f487594 0f856dffffff    jne     mstscax!CTSInput::IHPostMessageToMainWindow+0x97 (00007ff9`9f487507)
00007ff9`9f48759a 8d4de5          lea     ecx,[rbp-1Bh]
00007ff9`9f48759d 48ff15bcec5b00  call    qword ptr [mstscax!_imp_GetKeyState (00007ff9`9fa46260)]
00007ff9`9f4875a4 0f1f440000      nop     dword ptr [rax+rax]
00007ff9`9f4875a9 6685c6          test    si,ax
00007ff9`9f4875ac 0f8455ffffff    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x97 (00007ff9`9f487507)
00007ff9`9f4875b2 8d4de4          lea     ecx,[rbp-1Ch]
00007ff9`9f4875b5 48ff15a4ec5b00  call    qword ptr [mstscax!_imp_GetKeyState (00007ff9`9fa46260)]
00007ff9`9f4875bc 0f1f440000      nop     dword ptr [rax+rax]
00007ff9`9f4875c1 6685c6          test    si,ax
00007ff9`9f4875c4 0f843dffffff    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x97 (00007ff9`9f487507)
00007ff9`9f4875ca e8c581fcff      call    mstscax!CClientUtilsWin32::UT_IsRunningInAppContainer (00007ff9`9f44f794)
00007ff9`9f4875cf 85c0            test    eax,eax
00007ff9`9f4875d1 0f8430ffffff    je      mstscax!CTSInput::IHPostMessageToMainWindow+0x97 (00007ff9`9f487507)
00007ff9`9f4875d7 488b052ae27400  mov     rax,qword ptr [mstscax!WPP_GLOBAL_Control (00007ff9`9fbd5808)]
00007ff9`9f4875de 4c8d3d23e27400  lea     r15,[mstscax!WPP_GLOBAL_Control (00007ff9`9fbd5808)]
00007ff9`9f4875e5 493bc7          cmp     rax,r15
00007ff9`9f4875e8 7430            je      mstscax!CTSInput::IHPostMessageToMainWindow+0x1aa (00007ff9`9f48761a)
00007ff9`9f4875ea f6401c01        test    byte ptr [rax+1Ch],1
00007ff9`9f4875ee 742a            je      mstscax!CTSInput::IHPostMessageToMainWindow+0x1aa (00007ff9`9f48761a)
00007ff9`9f4875f0 80781904        cmp     byte ptr [rax+19h],4
00007ff9`9f4875f4 7224            jb      mstscax!CTSInput::IHPostMessageToMainWindow+0x1aa (00007ff9`9f48761a)
00007ff9`9f4875f6 e82de60000      call    mstscax!RdpWppGetCurrentThreadActivityIdPrefix (00007ff9`9f495c28)
00007ff9`9f4875fb 488b0d06e27400  mov     rcx,qword ptr [mstscax!WPP_GLOBAL_Control (00007ff9`9fbd5808)]
00007ff9`9f487602 4c8d0567ca5c00  lea     r8,[mstscax!WPP_f5f71bb7bac236b27f26969128cc1e12_Traceguids (00007ff9`9fa54070)]
00007ff9`9f487609 448bc8          mov     r9d,eax
00007ff9`9f48760c bafd000000      mov     edx,0FDh
00007ff9`9f487611 488b4910        mov     rcx,qword ptr [rcx+10h]
```

BUSY Debuggee is running...

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:1cb8 | Thrd 002:1790 | ASM | OVR | CAPS | NUM

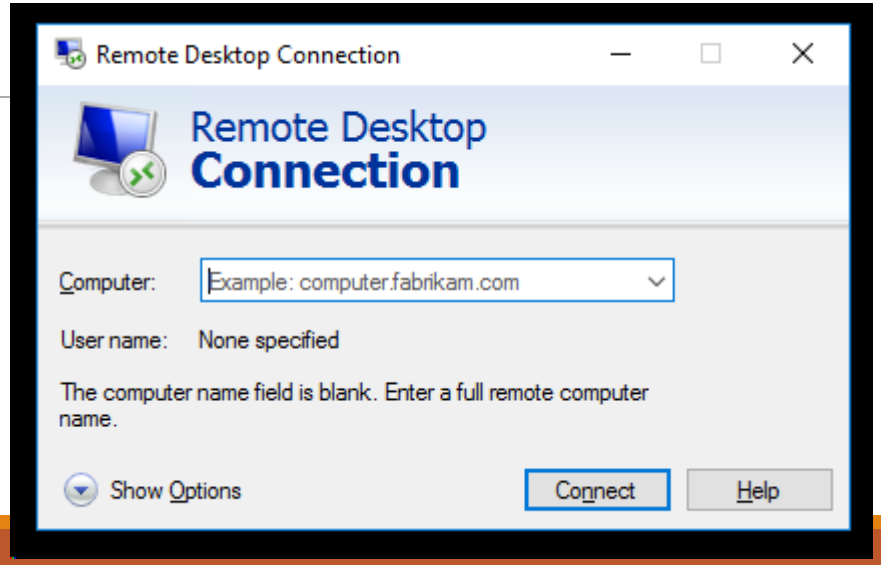
Recap

We found the keyboard event handler.

We modified the *if-else* conditions to check a different key combination.

Audio is lagging behind in *mstsc.exe*.

FIX IT PLEASE



Audio and Video

We don’t have access to the ***mstsc.exe*** source code.

We are on our own (nobody’s going to help us).

We can use only publicly available materials.

We know nothing about ***mstsc.exe***:

- What programming language it’s written in
- How it downloads, stores, and plays audio and video
- Why it’s getting out of sync

Audio and Video

We can reproduce the problem.

We notice that the sound gets delayed after our computer is overloaded.

We know RDP defines virtual data channels.

- https://www.cyberark.com/resources/threat-research-blog/explain-like-i-m-5-remote-desktop-protocol-rdp
- https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-rdsod/072543f9-4bd4-4dc6-ab97-9a04bf9d2c6a
- https://github.com/MicrosoftDocs/SupportArticles-docs/blob/main/support/windows-server/remote/understanding-remote-desktop-protocol.md

We may suspect that audio and video are sent via different channels with no timestamps or time markers.

Approach 1: Implement timestamping

Difficult, as we have no access to source code.

However, RDP implements virtual data channels, so we can implement plugins.

There are applications doing that, for instance ***Sound For Remote Desktop***: https://www.sound-over-rdp.com/

Approach 2: Decrease the buffer length

The incoming audio must be buffered somewhere.

If we find the buffer, we can shorten it.

Hard to do because:

- The buffer is probably initialized at the application startup
- We don’t know how the buffer length is determined – it could be a constant integer, determined based on allocation metadata, or determined automatically
- We don’t know if there is one buffer or many
- It’s hard to find the buffer without knowing its content

Approach 3: Empty the buffer periodically

Hard to do because:

- We don’t know where the pointer to the current position in the buffer is
- We need to avoid race conditions
- And we still can’t find the buffer easily

Approach 4: Find the call site and cut the buffer in half

Let’s find where the audio is played.

Let’s patch the call site.

Let’s shorten the buffer by half based on some random sampling.

Monitoring | ApiMonitorTrace_mstsc_exe_single_sound.apmx64 - API Monitor v2 64-bit

File Edit View Filter Tools Window Help

API Filter

All Modules

- Additional Resources
- Application Installation and Servicing
- Audio and Video
- Component Object Model (COM)
- Data Access and Storage
- Delta Compression
- Devices
- Diagnostics
- Documents and Printing
- Graphics and Gaming
- Internet
- Microsoft .NET
- NT Native
- Netscape Portable Runtime
- Network Security Services (NSS)
- Networking
- Office Development
- Scripting Runtime Library
- Security and Identity
- System Administration
- System Services
- Undocumented (UnDoc'd)
- Virtualization
- Visual C++ Run-Time Library
- Web Development
- Windows Application UI Development
- Windows Data Types
- Windows Driver Kit
- Windows Environment Development
- Wireless Networking

Capture | Display | External DLL

Running Processes

Process	PID
dllhost.exe	10832
explorer.exe	8904
GitExtensions.exe	9660
msedge.exe	2680
msedge.exe	10644
msedge.exe	4884
msedge.exe	4856
msedge.exe	11236
mstsc.exe	6512
PhoneExperienceHost....	10764
rdpclip.exe	8032
RtkAudUService64.exe	2224
RuntimeBroker.exe	9644
RuntimeBroker.exe	10032
RuntimeBroker.exe	11060
SearchApp.exe	9876
SecurityHealthSystray....	10756
sihost.exe	7692
StartMenuExperience...	9416
svchost.exe	8204
svchost.exe	8228
svchost.exe	8464
svchost.exe	3824
SynTPEnh.exe	7448

Processes | Services

Monitored Processes

C:\windows\system32\mstsc.exe - PID: 6512

Summary | 9,834 calls | 3.37 MB used | mstsc.exe

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
9771	7:17:48.519 AM	11	mstscax.dll	IMFSample::RemoveAllBuffers ( )	S_OK		0.0000035
9772	7:17:48.519 AM	11	mstscax.dll	IMFMediaBuffer::Release ( )	0		0.0000032
9773	7:17:48.519 AM	11	mstscax.dll	IMFSample::SetSampleFlags (0)	S_OK		0.0000001
9774	7:17:48.519 AM	11	mstscax.dll	IMFSample::DeleteAllItems ( )	S_OK		0.0000006
9775	7:17:48.519 AM	11	mstscax.dll	IMFMediaBuffer::Release ( )	1		0.0000001
9776	7:17:48.519 AM	11	mstscax.dll	IMFSample::Release ( )	0		0.0000012
9777	7:17:48.519 AM	11	mstscax.dll	IMFSample::RemoveAllBuffers ( )	S_OK		0.0000005
9778	7:17:48.519 AM	11	mstscax.dll	IMFMediaBuffer::Release ( )	0		0.0000003
9779	7:17:48.519 AM	11	mstscax.dll	IMFSample::SetSampleFlags (0)	S_OK		0.0000000
9780	7:17:48.519 AM	11	mstscax.dll	IMFSample::DeleteAllItems ( )	S_OK		0.0000001
9781	7:17:48.519 AM	11	mstscax.dll	waveOutGetPosition (0x0000019ed6e7cab0, 0x000000466d2fe8f0, 12)	MMSYSERR_NO...		0.0001340
9782	7:17:48.519 AM	56	mstscax.dll	IAudioClock::GetPosition (0x000000466d2fe300, NULL)	S_OK		0.0000029
9783	7:17:48.521 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff5d0)	S_OK		0.0000025
9784	7:17:48.521 AM	56	mstscax.dll	IAudioRenderClient::GetBuffer (393, 0x000000466ceff568)	S_OK		0.0000014
9785	7:17:48.521 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff1d0)	S_OK		0.0000001
9786	7:17:48.521 AM	56	mstscax.dll	IAudioRenderClient::ReleaseBuffer (0, 0)	S_OK		0.0000019
9787	7:17:48.521 AM	56	mstscax.dll	IAudioClock::GetPosition (0x000000466ceff648, NULL)	S_OK		0.0000009
9788	7:17:48.521 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff630)	S_OK		0.0000039
9789	7:17:48.521 AM	56	mstscax.dll	IAudioRenderClient::GetBuffer (834, 0x000000466ceff5c8)	S_OK		0.0000011
9790	7:17:48.521 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff230)	S_OK		0.0000005
9791	7:17:48.521 AM	56	mstscax.dll	IAudioRenderClient::ReleaseBuffer (0, 0)	S_OK		0.0000013
9792	7:17:48.521 AM	56	mstscax.dll	IAudioClock::GetPosition (0x000000466ceff6a8, NULL)	S_OK		0.0000007
9793	7:17:48.528 AM	55	mstscax.dll	waveOutPrepareHeader (0x0000019ed6e7cab0, 0x0000019eebebe310, 48)	MMSYSERR_NO...		0.0002624
9794	7:17:48.528 AM	55	mstscax.dll	waveOutWrite (0x0000019ed6e7cab0, 0x0000019eebebe310, 48)	MMSYSERR_NO...		0.0000667
9795	7:17:48.529 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff630)	S_OK		0.0000074
9796	7:17:48.529 AM	56	mstscax.dll	IAudioRenderClient::GetBuffer (1275, 0x000000466ceff5c8)	S_OK		0.0000016
9797	7:17:48.529 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff230)	S_OK		0.0000001
9798	7:17:48.529 AM	56	mstscax.dll	IAudioRenderClient::ReleaseBuffer (1024, 0)	S_OK		0.0000039
9799	7:17:48.529 AM	56	mstscax.dll	IAudioClock::GetPosition (0x000000466ceff6a8, NULL)	S_OK		0.0000015
9800	7:17:48.536 AM	13	mstscax.dll	waveOutUnprepareHeader (0x0000019ed6e7cab0, 0x0000019eebebd910, 4..	MMSYSERR_NO...		0.0002413
9801	7:17:48.539 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff630)	S_OK		0.0000159
9802	7:17:48.539 AM	56	mstscax.dll	IAudioRenderClient::GetBuffer (692, 0x000000466ceff5c8)	S_OK		0.0000051
9803	7:17:48.539 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff230)	S_OK		0.0000005
9804	7:17:48.539 AM	56	mstscax.dll	IAudioRenderClient::ReleaseBuffer (0, 0)	S_OK		0.0000042
9805	7:17:48.539 AM	56	mstscax.dll	IAudioClock::GetPosition (0x000000466ceff6a8, NULL)	S_OK		0.0000030
9806	7:17:48.549 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff630)	S_OK		0.0000068
9807	7:17:48.549 AM	56	mstscax.dll	IAudioRenderClient::GetBuffer (1133, 0x000000466ceff5c8)	S_OK		0.0000023
9808	7:17:48.549 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff230)	S_OK		0.0000002
9809	7:17:48.549 AM	56	mstscax.dll	IAudioRenderClient::ReleaseBuffer (0, 0)	S_OK		0.0000021
9810	7:17:48.549 AM	56	mstscax.dll	IAudioClock::GetPosition (0x000000466ceff6a8, NULL)	S_OK		0.0000021
9811	7:17:48.560 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff630)	S_OK		0.0000048
9812	7:17:48.560 AM	56	mstscax.dll	IAudioRenderClient::GetBuffer (1574, 0x000000466ceff5c8)	S_OK		0.0000021
9813	7:17:48.560 AM	56	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000466ceff230)	S_OK		0.0000001
9814	7:17:48.560 AM	56	mstscax.dll	IAudioRenderClient::ReleaseBuffer (0, 0)	S_OK		0.0000011

Parameters: waveOutPrepareHeader (Winmm.dll)

#	Type	Name	Pre-Call Value	Post-Call Value
1	HWAVEOUT	hwo	0x0000019ed6e7cab0	0x0000019ed6e7cab0
2	LPWAVEHDR	pwh	0x0000019eebebe310 = { lpData = ...	0x0000019eebebe310 = { lpData = ...
3	UINT	cbwh	48	48
	MMRESULT	Return		MMSYSERR_NOERROR

Hex Buffer

Call Stack: waveOutPrepareHeader (Winmm.dll)

#	Module	Address	Offset	Location
1	mstscax.dll	0x00007ffb364...	0x52d29	
2	mstscax.dll	0x00007ffb364...	0x50d74	
3	mstscax.dll	0x00007ffb364...	0x67bf8	
4	mstscax.dll	0x00007ffb365...	0x1670cf	DllUnregisterServer + 0xa60bf

Output

```
------ Loading Files from C:\Users\afish\Desktop\Tools\API Monitor\API ------
------ Finished Loading 2119 Files ------
Categories:      835
Variables:       19678
DLLs:            222
APIs:            15885
COM Interfaces:  1826
COM Methods:     22262
```

API Loader | Monitoring | Output

Ready | 3.37 MB | Mode: Portable

https://learn.microsoft.com/en-us/windows/win32/api/mmeapi/nf-mmeapi-waveoutprepareheader

waveOutPrepareHeader function (mmeapi.h)

Article • 04/02/2021 Feedback

In this article

The **waveOutPrepareHeader** function prepares a waveform-audio data block for playback.

Syntax

C++ Copy

```
MMRESULT waveOutPrepareHeader(
  HWAVEOUT  hwo,
  LPWAVEHDR pwh,
  UINT      cbwh
);
```

Parameters

`hwo`

Handle to the waveform-audio output device.

`pwh`

Pointer to a WAVEHDR structure that identifies the data block to be prepared.

`cbwh`

Size, in bytes, of the WAVEHDR structure.

WAVEHDR structure

Article • 06/06/2016

In this article

The **WAVEHDR** structure defines the header used to identify a waveform-audio buffer.

Syntax

c++

```
typedef struct wavehdr_tag {
  LPSTR              lpData;
  DWORD              dwBufferLength;
  DWORD              dwBytesRecorded;
  DWORD_PTR          dwUser;
  DWORD              dwFlags;
  DWORD              dwLoops;
  struct wavehdr_tag  *lpNext;
  DWORD_PTR          reserved;
} WAVEHDR, *LPWAVEHDR;
```

Monitoring - API Monitor v2 64-bit

File Edit View Filter Tools Window Help

API Filter

All Modules

- Additional Resources
- Application Installation and Servicing
- Audio and Video
- Component Object Model (COM)
- Data Access and Storage
- Delta Compression
- Devices
- Diagnostics
- Documents and Printing
- Graphics and Gaming
- Internet
- Microsoft .NET
- NT Native
- Netscape Portable Runtime
- Network Security Services (NSS)
- Networking
- Office Development
- Scripting Runtime Library
- Security and Identity
- System Administration
- System Services
- Undocumented (UnDoc'd)
- Virtualization
- Visual C++ Run-Time Library
- Web Development
- Windows Application UI Development
- Windows Data Types
- Windows Driver Kit
- Windows Environment Development
- Wireless Networking

Capture | Display | External DLL

Hex Buffer | Output

Summary | 44,855 calls | 15.02 MB used | mstsc.exe

#	Time of Day	Thread	Module	API	Return Value	Error	Du
36516	11:56:34.171 AM	53	mstscax.dll	IAudioClock::GetPosition (0x000000bbd7dfe760, NULL)	S_OK		0.(
36517	11:56:34.173 AM	53	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000bbd8b7f690)	S_OK		0.(
36518	11:56:34.173 AM	53	mstscax.dll	IAudioClock::GetPosition (0x000000bbd8b7f708, NULL)	S_OK		0.(
36519	11:56:34.175 AM	52	mstscax.dll	waveOutPrepareHeader (0x00000214d2ea62e0, 0x00000214f28d8bb0, 48)	MMSYSERR_NO...		0.(
36520	11:56:34.175 AM	52	mstscax.dll	waveOutWrite (0x00000214d2ea62e0, 0x00000214f28d8bb0, 48)	MMSYSERR_NO...		0.(
36521	11:56:34.179 AM	53	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000bbd8b7f6f0)	S_OK		0.(
36522	11:56:34.179 AM	53	mstscax.dll	IAudioRenderClient::GetBuffer (441, 0x000000bbd8b7f688)	S_OK		0.(
36523	11:56:34.179 AM	53	mstscax.dll	└IAudioClient::GetCurrentPadding (0x000000bbd8b7f2f0)	S_OK		0.(
36524	11:56:34.179 AM	53	mstscax.dll	IAudioRenderClient::ReleaseBuffer (441, 0)	S_OK		0.(
36525	11:56:34.179 AM	53	mstscax.dll	IAudioClock::GetPosition (0x000000bbd8b7f768, NULL)	S_OK		0.(
36526	11:56:34.189 AM	53	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000bbd8b7f6f0)	S_OK		0.(
36527	11:56:34.189 AM	53	mstscax.dll	IAudioRenderClient::GetBuffer (441, 0x000000bbd8b7f688)	S_OK		0.(
36528	11:56:34.189 AM	53	mstscax.dll	└IAudioClient::GetCurrentPadding (0x000000bbd8b7f2f0)	S_OK		0.(
36529	11:56:34.189 AM	53	mstscax.dll	IAudioRenderClient::ReleaseBuffer (441, 0)	S_OK		0.(
36530	11:56:34.189 AM	53	mstscax.dll	IAudioClock::GetPosition (0x000000bbd8b7f768, NULL)	S_OK		0.(
36531	11:56:34.189 AM	9	mstscax.dll	waveOutUnprepareHeader (0x00000214d2ea62e0, 0x00000214f28d8970, 48)	MMSYSERR_NO...		0.(
36532	11:56:34.199 AM	53	mstscax.dll	IAudioClient::GetCurrentPadding (0x000000bbd8b7f6f0)	S_OK		0.(
36533	11:56:34.199 AM	53	mstscax.dll	IAudioRenderClient::GetBuffer (441, 0x000000bbd8b7f688)	S_OK		0.(
36534	11:56:34.199 AM	53	mstscax.dll	└IAudioClient::GetCurrentPadding (0x000000bbd8b7f2f0)	S_OK		0.(

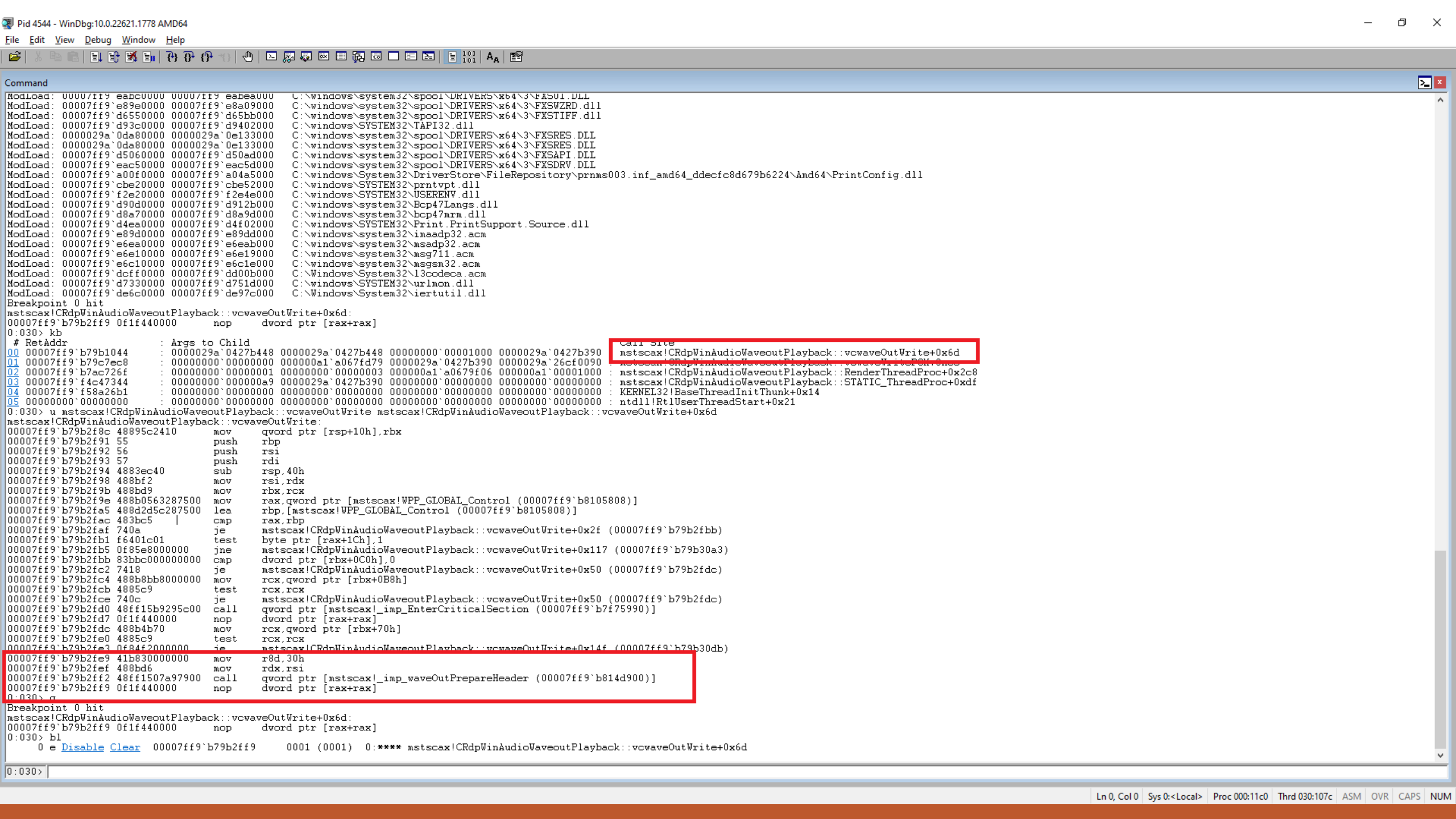
Parameters: waveOutPrepareHeader (Winmm.dll)

#	Type	Name	Pre-Call Value	Post-Call Value
1	HWAVEOUT	hwo	0x00000214d2ea62e0	0x00000214d2ea62e0
2	LPWAVEHDR	pwh	0x00000214f28d8bb0 = { lpData = ...	0x00000214f28d8bb0 = { lpData = ...
3	UINT	cbwh	48	48
	MMRESULT	Return		MMSYSERR_NOERROR

Call Stack: waveOutPrepareHeader (Winmm.dll)

#	Module	Address	Offset	Location
1	mstscax.dll	0x00007ff9b79b2ff9	0x52ff9	
2	mstscax.dll	0x00007ff9b79b1044	0x51044	
3	mstscax.dll	0x00007ff9b79c7ec8	0x67ec8	
4	mstscax.dll	0x00007ff9b7ac726f	0x16726f	DllUnregisterServer + 0xa5f9f

Ready | 15.02 MB | Mode: Portable


Pid 4544 - WinDbg:10.0.22621.1778 AMD64
File Edit View Debug Window Help
Command
ModLoad: 00007ff9`e89e0000 00007ff9`e8a09000 C:\windows\system32\spool\DRIVERS\x64\3\FXSWZRD.dll
ModLoad: 00007ff9`d6550000 00007ff9`d65bb000 C:\windows\system32\spool\DRIVERS\x64\3\FXSTIFF.dll
ModLoad: 00007ff9`d93c0000 00007ff9`d9402000 C:\windows\SYSTEM32\TAPI32.dll
ModLoad: 0000029a`0da80000 0000029a`0e133000 C:\windows\system32\spool\DRIVERS\x64\3\FXSRES.DLL
ModLoad: 0000029a`0da80000 0000029a`0e133000 C:\windows\system32\spool\DRIVERS\x64\3\FXSRES.DLL
ModLoad: 00007ff9`d5060000 00007ff9`d50ad000 C:\windows\system32\spool\DRIVERS\x64\3\FXSAPI.DLL
ModLoad: 00007ff9`eac50000 00007ff9`eac5d000 C:\windows\system32\spool\DRIVERS\x64\3\FXSDRV.DLL
ModLoad: 00007ff9`a00f0000 00007ff9`a04a5000 C:\windows\System32\DriverStore\FileRepository\prnms003.inf_amd64_ddecfc8d679b6224\Amd64\PrintConfig.dll
ModLoad: 00007ff9`cbe20000 00007ff9`cbe52000 C:\windows\SYSTEM32\prntvpt.dll
ModLoad: 00007ff9`f2e20000 00007ff9`f2e4e000 C:\windows\SYSTEM32\USERENV.dll
ModLoad: 00007ff9`d90d0000 00007ff9`d912b000 C:\windows\system32\Bcp47Langs.dll
ModLoad: 00007ff9`d8a70000 00007ff9`d8a9d000 C:\windows\system32\bcp47mrm.dll
ModLoad: 00007ff9`d4ea0000 00007ff9`d4f02000 C:\windows\SYSTEM32\Print.PrintSupport.Source.dll
ModLoad: 00007ff9`e89d0000 00007ff9`e89dd000 C:\windows\system32\imaadp32.acm
ModLoad: 00007ff9`e6ea0000 00007ff9`e6eab000 C:\windows\system32\msadp32.acm
ModLoad: 00007ff9`e6e10000 00007ff9`e6e19000 C:\windows\system32\msg711.acm
ModLoad: 00007ff9`e6c10000 00007ff9`e6c1e000 C:\windows\system32\msgsm32.acm
ModLoad: 00007ff9`dcff0000 00007ff9`dd00b000 C:\Windows\System32\l3codeca.acm
ModLoad: 00007ff9`d7330000 00007ff9`d751d000 C:\windows\SYSTEM32\urlmon.dll
ModLoad: 00007ff9`de6c0000 00007ff9`de97c000 C:\Windows\System32\iertutil.dll
Breakpoint 0 hit
mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d:
00007ff9`b79b2ff9 0f1f440000 nop dword ptr [rax+rax]
0:030> kb
RetAddr : Args to Child : Call Site
00 00007ff9`b79b1044 : 0000029a`0427b448 0000029a`0427b448 00000000`00001000 0000029a`0427b390 : mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d
01 00007ff9`b79c7ec8 : 00000000`00000000 000000a1`a067fd79 0000029a`0427b390 0000029a`26cf0090 : mstscax!CRdpWinAudioWaveoutPlayback::vcwaveWritePCM+0xa4
02 00007ff9`b7ac726f : 00000000`00000001 00000000`00000003 000000a1`a0679f06 000000a1`00001000 : mstscax!CRdpWinAudioWaveoutPlayback::RenderThreadProc+0x2c8
03 00007ff9`f4c47344 : 00000000`000000a9 0000029a`0427b390 00000000`00000000 00000000`00000000 : mstscax!CRdpWinAudioWaveoutPlayback::STATIC_ThreadProc+0xdf
04 00007ff9`f58a26b1 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14
05 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21
0:030> u mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d
mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite:
00007ff9`b79b2f8c 48895c2410 mov qword ptr [rsp+10h],rbx
00007ff9`b79b2f91 55 push rbp
00007ff9`b79b2f92 56 push rsi
00007ff9`b79b2f93 57 push rdi
00007ff9`b79b2f94 4883ec40 sub rsp,40h
00007ff9`b79b2f98 488bf2 mov rsi,rdx
00007ff9`b79b2f9b 488bd9 mov rbx,rcx
00007ff9`b79b2f9e 488b0563287500 mov rax,qword ptr [mstscax!WPP_GLOBAL_Control (00007ff9`b8105808)]
00007ff9`b79b2fa5 488d2d5c287500 lea rbp,[mstscax!WPP_GLOBAL_Control (00007ff9`b8105808)]
00007ff9`b79b2fac 483bc5 cmp rax,rbp
00007ff9`b79b2faf 740a je mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x2f (00007ff9`b79b2fbb)
00007ff9`b79b2fb1 f6401c01 test byte ptr [rax+1Ch],1
00007ff9`b79b2fb5 0f85e8000000 jne mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x117 (00007ff9`b79b30a3)
00007ff9`b79b2fbb 83bbc000000000 cmp dword ptr [rbx+0C0h],0
00007ff9`b79b2fc2 7418 je mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x50 (00007ff9`b79b2fdc)
00007ff9`b79b2fc4 488b8bb8000000 mov rcx,qword ptr [rbx+0B8h]
00007ff9`b79b2fcb 4885c9 test rcx,rcx
00007ff9`b79b2fce 740c je mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x50 (00007ff9`b79b2fdc)
00007ff9`b79b2fd0 48ff15b9295c00 call qword ptr [mstscax!_imp_EnterCriticalSection (00007ff9`b7f75990)]
00007ff9`b79b2fd7 0f1f440000 nop dword ptr [rax+rax]
00007ff9`b79b2fdc 488b4b70 mov rcx,qword ptr [rbx+70h]
00007ff9`b79b2fe0 4885c9 test rcx,rcx
00007ff9`b79b2fe3 0f84f2000000 je mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x14f (00007ff9`b79b30db)
00007ff9`b79b2fe9 41b830000000 mov r8d,30h
00007ff9`b79b2fef 488bd6 mov rdx,rsi
00007ff9`b79b2ff2 48ff1507a97900 call qword ptr [mstscax!_imp_waveOutPrepareHeader (00007ff9`b814d900)]
00007ff9`b79b2ff9 0f1f440000 nop dword ptr [rax+rax]
0:030> g
Breakpoint 0 hit
mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d:
00007ff9`b79b2ff9 0f1f440000 nop dword ptr [rax+rax]
0:030> bl
0 e Disable Clear 00007ff9`b79b2ff9 0001 (0001) 0:**** mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d
0:030>
Ln 0, Col 0
Sys 0:<Local>
Proc 000:11c0
Thrd 030:107c
ASM
OVR
CAPS
NUM

Pid 4544 - WinDbg:10.0.22621.1778 AMD64

File Edit View Debug Window Help

Command

```
ModLoad: 00007ff9`e89d0000 00007ff9`e89dd000   C:\windows\system32\imaadp32.acm
ModLoad: 00007ff9`e6ea0000 00007ff9`e6eab000   C:\windows\system32\msadp32.acm
ModLoad: 00007ff9`e6e10000 00007ff9`e6e19000   C:\windows\system32\msg711.acm
ModLoad: 00007ff9`e6c10000 00007ff9`e6c1e000   C:\windows\system32\msgsm32.acm
ModLoad: 00007ff9`dcff0000 00007ff9`dd00b000   C:\Windows\System32\l3codeca.acm
ModLoad: 00007ff9`d7330000 00007ff9`d751d000   C:\windows\SYSTEM32\urlmon.dll
ModLoad: 00007ff9`de6c0000 00007ff9`de97c000   C:\Windows\System32\iertutil.dll
Breakpoint 0 hit
mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d:
00007ff9`b79b2ff9 0f1f440000      nop     dword ptr [rax+rax]
0:030> kb
 # RetAddr               : Args to Child                                                   : Call Site
00 00007ff9`b79b1044     : 0000029a`0427b448 0000029a`0427b448 00000000`00001000 0000029a`0427b390 : mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d
01 00007ff9`b79c7ec8     : 00000000`00000000 000000a1`a067fd79 0000029a`0427b390 0000029a`26cf0090 : mstscax!CRdpWinAudioWaveoutPlayback::vcwaveWritePCM+0xec
02 00007ff9`b7ac726f     : 00000000`00000001 00000000`00000003 000000a1`a0679f06 000000a1`00001000 : mstscax!CRdpWinAudioWaveoutPlayback::RenderThreadProc+0x2c8
03 00007ff9`f4c47344     : 00000000`000000a9 0000029a`0427b390 00000000`00000000 00000000`00000000 : mstscax!CRdpWinAudioWaveoutPlayback::STATIC_ThreadProc+0xdf
04 00007ff9`f58a26b1     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14
05 00000000`00000000     : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21
0:030> u mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d
mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite:
00007ff9`b79b2f8c 48895c2410      mov     qword ptr [rsp+10h],rbx
00007ff9`b79b2f91 55              push    rbp
00007ff9`b79b2f92 56              push    rsi
00007ff9`b79b2f93 57              push    rdi
00007ff9`b79b2f94 4883ec40        sub     rsp,40h
00007ff9`b79b2f98 488bf2          mov     rsi,rdx
00007ff9`b79b2f9b 488bd9          mov     rbx,rcx
00007ff9`b79b2f9e 488b0563287500  mov     rax,qword ptr [mstscax!WPP_GLOBAL_Control (00007ff9`b8105808)]
00007ff9`b79b2fa5 488d2d5c287500  lea     rbp,[mstscax!WPP_GLOBAL_Control (00007ff9`b8105808)]
00007ff9`b79b2fac 483bc5          cmp     rax,rbp
00007ff9`b79b2faf 740a            je      mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x2f (00007ff9`b79b2fbb)
00007ff9`b79b2fb1 f6401c01        test    byte ptr [rax+1Ch],1
00007ff9`b79b2fb5 0f85e8000000    jne     mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x117 (00007ff9`b79b30a3)
00007ff9`b79b2fbb 83bbc000000000  cmp     dword ptr [rbx+0C0h],0
00007ff9`b79b2fc2 7418            je      mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x50 (00007ff9`b79b2fdc)
00007ff9`b79b2fc4 488b8bb8000000  mov     rcx,qword ptr [rbx+0B8h]
00007ff9`b79b2fcb 4885c9          test    rcx,rcx
00007ff9`b79b2fce 740c            je      mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x50 (00007ff9`b79b2fdc)
00007ff9`b79b2fd0 48ff15b9295c00  call    qword ptr [mstscax!_imp_EnterCriticalSection (00007ff9`b7f75990)]
00007ff9`b79b2fd7 0f1f440000      nop     dword ptr [rax+rax]
00007ff9`b79b2fdc 488b4b70        mov     rcx,qword ptr [rbx+70h]
00007ff9`b79b2fe0 4885c9          test    rcx,rcx
00007ff9`b79b2fe3 0f84f2000000    je      mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x14f (00007ff9`b79b30db)
00007ff9`b79b2fe9 41b830000000    mov     r8d,30h
00007ff9`b79b2fef 488bd6          mov     rdx,rsi
00007ff9`b79b2ff2 48ff1507a97900  call    qword ptr [mstscax!_imp_waveOutPrepareHeader (00007ff9`b814d900)]
00007ff9`b79b2ff9 0f1f440000      nop     dword ptr [rax+rax]
0:030> g
Breakpoint 0 hit
mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d:
00007ff9`b79b2ff9 0f1f440000      nop     dword ptr [rax+rax]
0:030> bl
     0 e Disable Clear  00007ff9`b79b2ff9     0001 (0001)  0:**** mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d
0:030> .dvalloc 1000
Allocated 1000 bytes starting at 0000029a`0e200000
0:030> e  00007ff9`b79b2fe9  0x48 0xB8 0x00 0x00 0x20 0x0E 0x9A 0x02 0x00 0x00 0x50 0xC3 0x90 0x90 0x90 0x90
0:030> e 0x0000029a0e200000 0x41 0xB8 0x30 0x00 0x00 0x00 0x48 0x89 0xF2 0x48 0x8B 0x42 0x08 0x48 0xD1 0xE8 0x48 0x89 0x42 0x08 0x48 0xB8 0xF9 0x2F 0x9B 0xB7 0xF9 0x7F 0x00 0x00 0x50 0x53 0x48 0xBB 0x00 0xD9 0x14 0xB8 0xF9 0x7F 0x00 0x
0:030> g
Breakpoint 0 hit
mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d:
00007ff9`b79b2ff9 0f1f440000      nop     dword ptr [rax+rax]
0:030> bl
     0 e Disable Clear  00007ff9`b79b2ff9     0001 (0001)  0:**** mstscax!CRdpWinAudioWaveoutPlayback::vcwaveOutWrite+0x6d
0:030> bd 0
0:030> g
```

BUSY Debuggee is running...

Ln 0, Col 0 | Sys 0:<Local> | Proc 000:11c0 | Thrd 030:107c | ASM | OVR | CAPS | NUM

Recap

We found the call site of the audio WinAPI method.

We patched the call site to jump to our custom payload.

We sampled the audio packets based on the address of user data.

We modified the length of the packets before they were delivered to WinAPI.

Summary

Debugging is neither harder nor easier than coding. It’s different.

It’s a completely different skill for which we need new tools.

Great minds think alike. We need to know how others do things.

Ultimately, it’s just a bunch of bytes.

Q&A

References

https://learn.microsoft.com/en-us/windows/win32/procthread/multimedia-class-scheduler-service - MMCSS

https://www.reddit.com/r/ProgrammerHumor/comments/f6csjp/so_both_these_tools_copied_from_the_same_wrong/ - single instance bug

https://devblogs.microsoft.com/oldnewthing/20140905-00/?p=63 – lock based on byte-ranges

https://blog.adamfurmanek.pl/2018/05/05/concurrency-part-2/ - file lock

https://blog.adamfurmanek.pl/2019/10/19/concurrency-part-8/ - memory mapped file lock

http://emulators.com/docs/abc_arm64ec_explained.htm - WoW64 and AMR64EC

https://brooker.co.za/blog/2024/05/09/nagle.html - TCP_NODELAY

https://stackoverflow.com/questions/11227809/why-is-processing-a-sorted-array-faster-than-processing-an-unsorted-array - sorted array is faster

https://learn.microsoft.com/en-us/windows/win32/ipc/interprocess-communications - IPC

https://stackoverflow.com/questions/78028901/does-async-await-use-windows-messages-to-return-control-to-the-ui-thread - async and message loop

References

Jeffrey Richter - „CLR via C#”

https://github.com/dotnet/coreclr/blob/master/Documentation/botr/README.md — „Book of the Runtime”

Adam Furmanek – „.NET Internals Cookbook”

Jeffrey Richter, Christophe Nasarre - „Windows via C/C++”

W. Richard Stevens, Stephen A. Rago – „Advanced Programming in the UNIX Environment”

Mark Russinovich, David A. Solomon, Alex Ionescu - „Windows Internals”

Daniel P Bovet, Marco Cesati Ph.D. – „Understanding the Linux Kernel: From I/O Ports to Process”

Richard Mcdougall, Jim Mauro – „Solaris Internals: Solaris 10 and Opensolaris Kernel Architecture”

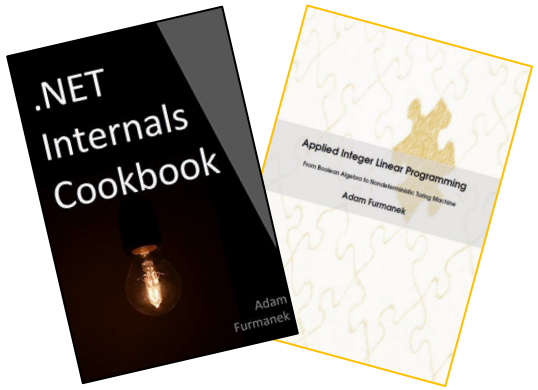
Joe Duffy - „Concurrent Programming on Windows”

Brendan Gregg – „Systems Performance: Enterprise and the Cloud”

Mario Hewardt, Daniel Pravat - „Advanced Windows Debugging”

Mario Hewardt - „Advanced .NET Debugging”

https://blogs.msdn.microsoft.com/oldnewthing/ — Raymond Chen „The Old New Thing”



Random IT Utensils

IT, operating systems, maths, and more.

Thanks!

CONTACT@ADAMFURMANEK.PL

HTTP://BLOG.ADAMFURMANEK.PL

FURMANEKADAM