

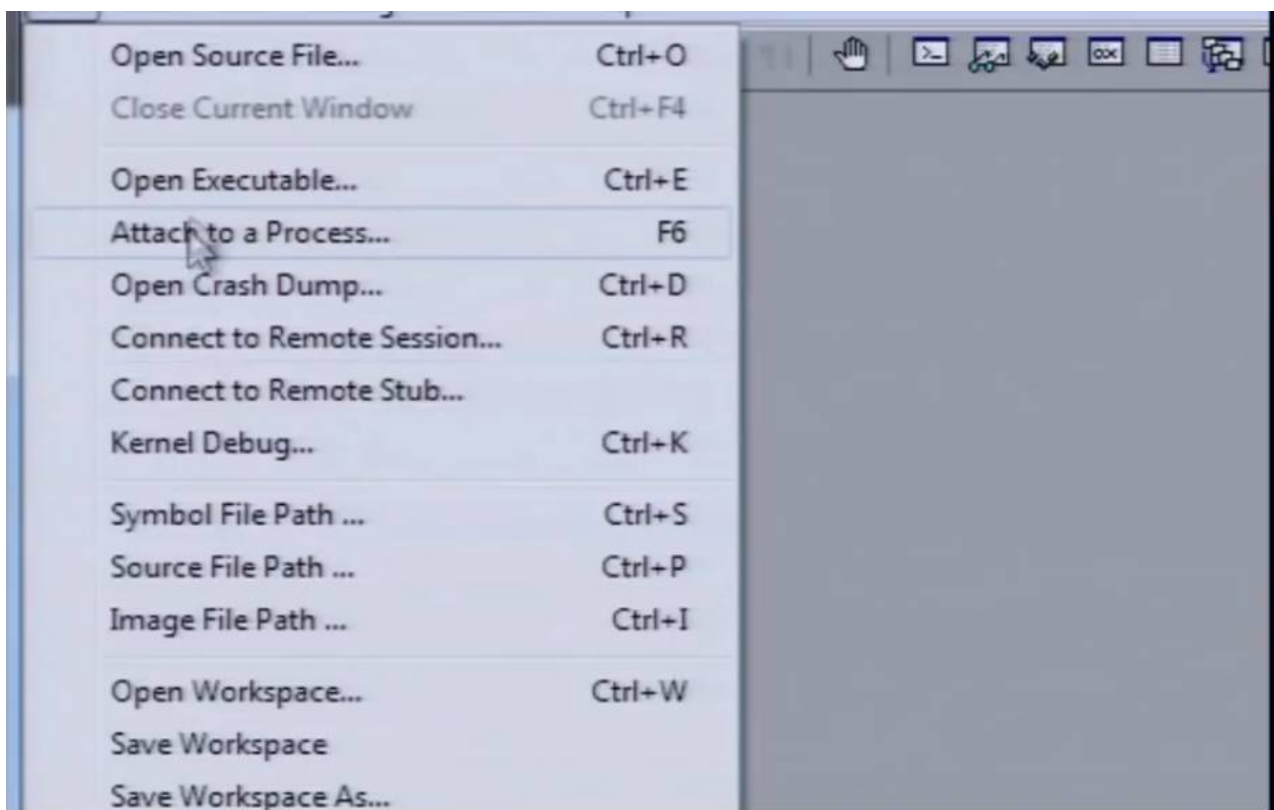
All commands can be insert in a script and can strated when the debugger starts.

Number which is shown left in the Windbg-GUI means the number of thread which has the exception (error)

Attach to a process with WinDBG in a physical machine to show what is going on in there.

Press the folder symbol in the left corner and press the attach to a process menu entree

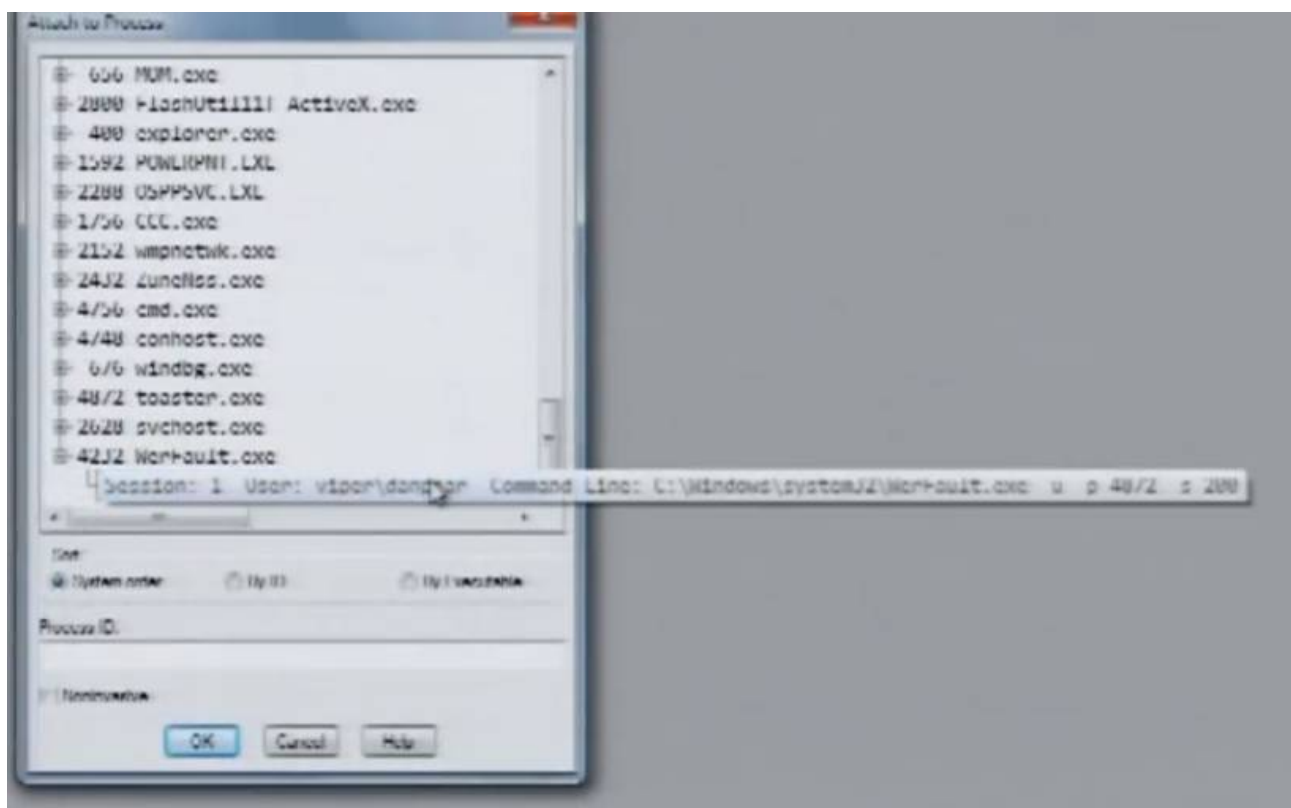
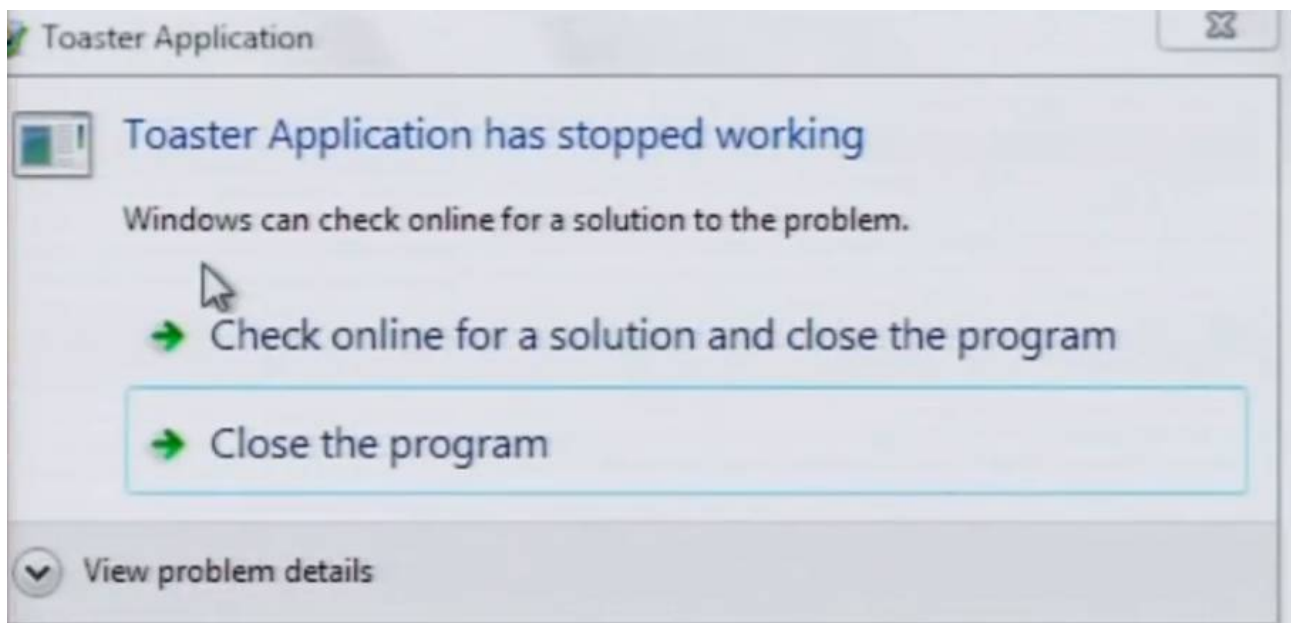
You can short this steps if you press windbg and the program name into the cmd or powershell.



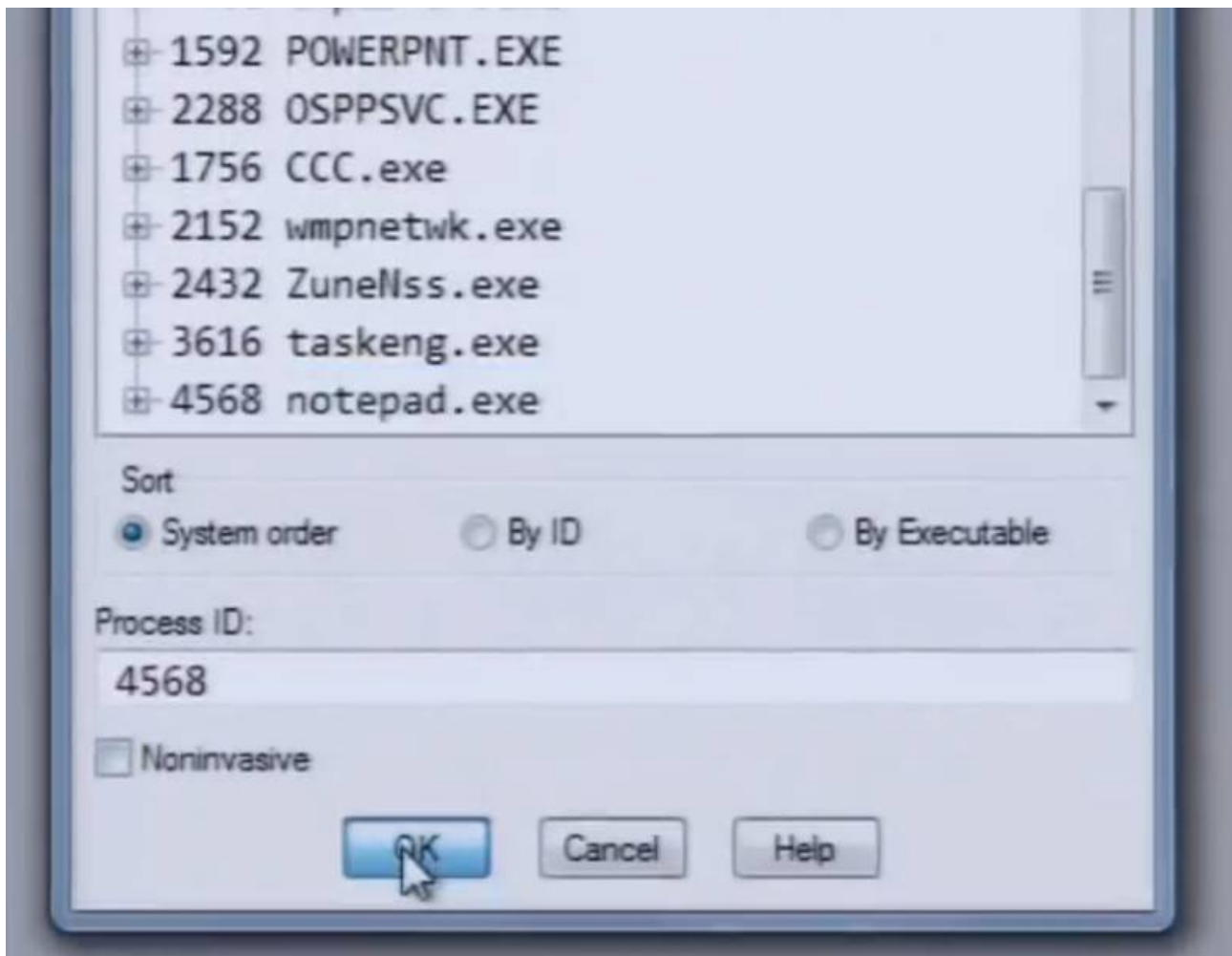
Select the program to which you want to be attached

Additional information:

If a program crashed and the application shows the crash windows leave it open to show on the WerFault.exe process which captured the process ID of the crashed application



In the next Step attach to the crashed process and search for the captured process ID.



At this moment a direct access to the program is not possible until you enter the **g**-command in the debugging tool.

Important: If you close the debugging tool and the process you be attached is running, it will be closed instantly as the debugging tool is closed !

To prevent this issue press the **qd**-command into the debugging tool, so the program continue where the debugging tool is deattached and closed.

To see more debugging details of a process or crashdump file you can use the following commands for different information:

Press the **db** command with the memory space address to see what is inside include Hex and ASCII values you want to see more details

```
ModLoad: 000007fe`fe030000 000007fe`fe0f9000 C:\Windows\sys
ModLoad: 000007fe`fdc80000 000007fe`fdd17000 C:\Windows\sys
ModLoad: 000007fe`ff350000 000007fe`ff3c1000 C:\Windows\sys
ModLoad: 000007fe`fc450000 000007fe`fc644000 C:\Windows\Win
ModLoad: 000007fe`fe100000 000007fe`fee88000 C:\Windows\sys
ModLoad: 000007fe`f8300000 000007fe`f8371000 C:\Windows\sys
ModLoad: 000007fe`ff090000 000007fe`ff293000 C:\Windows\sys
ModLoad: 000007fe`ff680000 000007fe`ff757000 C:\Windows\sys
ModLoad: 000007fe`fc9c0000 000007fe`fc9cc000 C:\Windows\sys
ModLoad: 000007fe`ff2a0000 000007fe`ff2ce000 C:\Windows\sys
ModLoad: 000007fe`ff3d0000 000007fe`ff4d9000 C:\Windows\sys
0:001> db 00000000`ffba0000
```

```
0:001> db 00000000`ffba0000
00000000`ffba0000  4d 5a 90 00 03 00 00 00-04 00 00 00 ff
00000000`ffba0010  b8 00 00 00 00 00 00 00-40 00 00 00 00
00000000`ffba0020  00 00 00 00 00 00 00 00-00 00 00 00 00
00000000`ffba0030  00 00 00 00 00 00 00 00-00 00 00 00 e8
00000000`ffba0040  0e 1f ba 0e 00 b4 09 cd-21 b8 01 4c cd
00000000`ffba0050  69 73 20 70 72 6f 67 72-61 6d 20 63 61
00000000`ffba0060  74 20 62 65 20 72 75 6e-20 69 6e 20 44
00000000`ffba0070  6d 6f 64 65 2e 0d 0d 0a-24 00 00 00 00
```

Press the **dc** command with the memory space address to see what is inside as Hex as Oktal and ASCII values

```

00000000`774a0530 cc int 3
0:001> db 00000000`ffba0000
00000000`ffba0000 4d 5a 90 00 03 00 00 00-04 00 00 00 ff
00000000`ffba0010 b8 00 00 00 00 00 00 00-40 00 00 00 00
00000000`ffba0020 00 00 00 00 00 00 00 00-00 00 00 00 00
00000000`ffba0030 00 00 00 00 00 00 00 00-00 00 00 00 e8
00000000`ffba0040 0e 1f ba 0e 00 b4 09 cd-21 b8 01 4c cd
00000000`ffba0050 69 73 20 70 72 6f 67 72-61 6d 20 63 61
00000000`ffba0060 74 20 62 65 20 72 75 6e-20 69 6e 20 44
00000000`ffba0070 6d 6f 64 65 2e 0d 0d 0a-24 00 00 00 00

0:001> dc 00000000`ffba0000

```

```

00000000`ffba0000 00905a4d 00000003 00000004 0000ffff MZ...
00000000`ffba0010 000000b8 00000000 00000040 00000000 ....
00000000`ffba0020 00000000 00000000 00000000 00000000 ....
00000000`ffba0030 00000000 00000000 00000000 000000e8 ....
00000000`ffba0040 0eba1f0e cd09b400 4c01b821 685421cd ....
00000000`ffba0050 70207369 72676f72 63206d61 6f6e6e61 is pr
00000000`ffba0060 65622074 6e757220 206e6920 20534f44 t be
00000000`ffba0070 65646f6d 0a0d0d2e 00000024 00000000 mode

```

You can use the Tilde ~ command to see which Threads (with numbers) is inside this memory address space

```

0:001> ~

```

```

0:001> ~
 0 Id: 1240.12c0 Suspend: 1 Teb: 000007ff`ffffde000 Unfrozen
. 1 Id: 1240.f30 Suspend: 1 Teb: 000007ff`ffffdc000 Unfrozen

```

First value is the Threads Number, Second is the Process ID and third is the Thread ID

The Thread ID is a hex code. If you want to know the decimal number of the process in task manager you have to convert this value with the ?-command

```
0:001> ~
  0 Id: 1240.12c0 Suspend: 1 Teb: 000007ff`ffffde000
. 1 Id: 1240.f30 Suspend: 1 Teb: 000007ff`ffffdc000
0:001> ?12c0
```

```
0:001> ~
  0 Id: 1240.12c0 Suspend: 1 Teb: 000007ff`ffffde000
. 1 Id: 1240.f30 Suspend: 1 Teb: 000007ff`ffffdc000
0:001> ?12c0
Evaluate expression: 4800 = 00000000`000012c0
0:001> I
```

Debugging Steps of a Crashed Application or Process

Press the „attach to a process“ menu entree

show for the captured crashed process id looking on the WerFault.exe process

Attache the crashed application

Show on the left side the number displayed on the command promp which shows the thread where the error or expection occurs.

```
0:005> ~
```

Add the Tilde ~ command into the debugging tool to display open Threads

Add the k-command to display the stack and whats inside the stack of one thread or at the Tilde / Star ~* command to display stack and whats inside the stack for each thread.

```

ntdll!DbgBreakPoint:
00000000`774a0530 cc int 3
0:002> ~
 0 Id: 1308.f10 Suspend: 2 Teb: 000007ff`ffffde000 Unfrozer
 1 Id: 1308.2e0 Suspend: 1 Teb: 000007ff`ffffda000 Unfrozer
. 2 Id: 1308.6e8 Suspend: 1 Teb: 000007ff`ffffd8000 Unfrozer
0:002> k
Child-SP RetAddr Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin-
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart-

```

```

# 2 Id: 1308.6e8 Suspend: 1 Teb: 000007ff`ffffd8000 Unfrozer
Child-SP RetAddr Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin-
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart-

```

Now looking for e.g exceptions ... to find the module which occurs the crash

```

00000000`774a1278 ntdll!RtlDispatchException+0x45a
000007fe`fc441178 ntdll!KiUserExceptionDispatcher+0x2e
bad completed but symbols could not be loaded for C:\Windows\sys
000007fe`fc441196 malware+0x1178
00000000`7724652d malware+0x1196
00000000`7747c521 kernel32!BaseThreadInitThunk+0xd
00000000`00000000 ntdll!RtlUserThreadStart+0x1d

```

If you find something press the **lm v m** command combination include the module name you found. This means list modules(lm) in verbose mode (v / show as much information you find) and match (m) it

```

0:002> lm v m malware

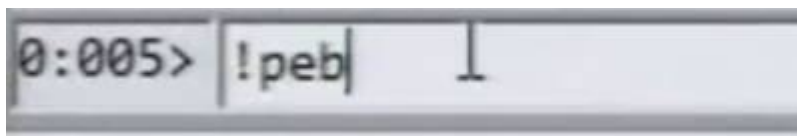
```

```
Image path: C:\Windows\system32\malware.dll
Image name: malware.dll
Timestamp:      Mon Feb 13 22:44:16 2012 (4F397620)
Checksum:       000073B8
ImageSize:      00007000
File version:   1.0.326.0
Product version: 1.0.326.0
File flags:     8 (Mask 3F) Private
File OS:        40004 NT Win32
File type:      2.0 Dll
File date:      00000000.00000000
Translations:   0409.04b0
CompanyName:    Malware Industries
ProductName:     Malware DLL
InternalName:    malware.dll
OriginalFilename: malware.dll
ProductVersion:  1.0.326.0
FileVersion:     1.0.326.0
```

Debugging Steps to analyze a Dump file

Open the dump file with the „open dump file“ menu entree

Add bang peb `!peb` into the command prompt which displays the process environment block which shows a lot of system information include corrupted process



```
0:005> !peb
```



```
CommandLine: 'C:\WINDOWS\System32\svchost.exe -k netsvc
DllPath:      'C:\WINDOWS\System32;C:\WINDOWS\system32;C:
Environment:  00010000
    ALLUSERSPROFILE=C:\Documents and Settings\All Users
    AVENGINE=C:\PROGRA~1\CA\SHARED~1\SCANEN~1
    BAB_HOME=C:\Program Files\CA\BrightStor ARCserve Back
    ClusterLog=C:\WINDOWS\Cluster\cluster.log
    CommonProgramFiles=C:\Program Files\Common Files
    COMPUTERNAME=EDITED
    ComSpec=C:\WINDOWS\system32\cmd.exe
    FP_NO_HOST_CHECK=NO
    IGW_LOC=C:\Program Files\CA\SharedComponents\iTechno
    NUMBER_OF_PROCESSORS=2
    OS=Windows_NT
    Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System
    PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.
```

```
NUMBER_OF_PROCESSORS=2
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 8
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0f08
ProgramFiles=C:\Program Files
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Default User
windir=C:\WINDOWS
```

Show on the left side the number displayed on the command prompt which shows the thread where the error or exception occurs.



Add the Tilde ~ command into the debugging tool to display open Threads

Add the k-command to display the stack and whats inside the stack of one thread or at the Tilde / Star ~* command to display stack and whats inside the stack for each thread.

```
ntdll!DbgBreakPoint:
00000000`774a0530 cc          int      3
0:002> ~
  0  Id: 1308.f10 Suspend: 2 Teb: 000007ff`ffffde000 Unfrozer
  1  Id: 1308.2e0 Suspend: 1 Teb: 000007ff`ffffda000 Unfrozer
.  2  Id: 1308.6e8 Suspend: 1 Teb: 000007ff`ffffd8000 Unfrozer
0:002> k
Child-SP          RetAddr          Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin-
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart-
```

```
# 2  Id: 1308.6e8 Suspend: 1 Teb: 000007ff`ffffd8000 Unfrozer
Child-SP          RetAddr          Call Site
00000000`0207fbd8 00000000`77547ef8 ntdll!DbgBreakPoint
00000000`0207fbe0 00000000`7724652d ntdll!DbgUiRemoteBreakin-
00000000`0207fc10 00000000`7747c521 kernel32!BaseThreadInitTh
00000000`0207fc40 00000000`00000000 ntdll!RtlUserThreadStart-
```

Now looking for e.g excpetions ... to find the module which occures the crash

```
00000000`774a1278 ntdll!RtlDispatchException+0x45a
000007fe`fc441178 ntdll!KiUserExceptionDispatcher+0x2e
ad completed but symbols could not be loaded for C:\Windows\sys
000007fe`fc441196 malware+0x1178
00000000`7724652d malware+0x1196
00000000`7747c521 kernel32!BaseThreadInitThunk+0xd
00000000`00000000 ntdll!RtlUserThreadStart+0x1d
```

IT is possible that you can't finde the exception directly rather show continuing Hex-Code

```

d7ee54 77e7650f faultrep!ReportFault+0x3d2
d7f0b0 77e792a3 kernel32!UnhandledExceptionFilter+0x494
d7f0b8 77e61ac1 kernel32!BaseThreadStart+0x4a
d7f0e0 7c828752 kernel32!_except_handler3+0x61
d7f104 7c828723 ntdll!ExecuteHandler2+0x26
d7f1ac 7c82855e ntdll!ExecuteHandler+0x24
d7f1ac 78040065 ntdll!KiUserExceptionDispatcher+0xe
WARNING: Frame IP not in any known module. Following frames may
d7f4a8 00d7f555 0x78040065
d7f4ac 00d7f5c8 0xd7f555
d7f555 00000000 0xd7f5c8

```

In this case you have to convert the Hex code using **dc** command with the memory space address to see what is inside as Hex as Oktal and ASCII values

```

d7f4a8 00d7f555 0x78040065
d7f4ac 00d7f5c8 0xd7f555
d7f555 00000000 0xd7f5c8

```

005> dc 78040065

If the converted entree shows ??? the Hex code before has handle the last executions before the exception or error occurs and the system crashed. Repeat the last step with the **dc** command using the Hex code before this process handling.

```

005> dc 78040065
040065  ???????? ???????? ???????? ???????? ??????????????????
040075  ???????? ???????? ???????? ???????? ??????????????????
040085  ???????? ???????? ???????? ???????? ??????????????????
040095  ???????? ???????? ???????? ???????? ??????????????????
0400a5  ???????? ???????? ???????? ???????? ??????????????????
0400b5  ???????? ???????? ???????? ???????? ??????????????????
0400c5  ???????? ???????? ???????? ???????? ??????????????????
0400d5  ???????? ???????? ???????? ???????? ??????????????????

```

005> | I

So the general process handling steps are different lines showing below. The Hex code in the upper line is handling the command showing in the next line and so on.

```

00d79ac0 77e61d1e ntdll!NtWaitForSingleObject+0xc
00d79b30 77e61c8d kernel32!WaitForSingleObjectEx+0xac
00d79b44 6951163f kernel32!WaitForSingleObject+0x12
00d79bac 69506136 faultrep!MyCallNamedPipe+0x15b
00d7e008 69508b5c faultrep!StartManifestReport+0x1d5
00d7ee54 77e7650f faultrep!ReportFault+0x3d2
00d7f0b0 77e792a3 kernel32!UnhandledExceptionFilter+0x494
00d7f0b8 77e61ac1 kernel32!BaseThreadStart+0x4a
00d7f0e0 7c828752 kernel32!_except_handler3+0x61
00d7f104 7c828723 ntdll!ExecuteHandler2+0x26
00d7f1ac 7c82855e ntdll!ExecuteHandler+0x24
00d7f1ac 78040065 ntdll!KiUserExceptionDispatcher+0xe
WARNING: Frame IP not in any known module. Following frames n
00d7f4a8 00d7f555 0x78040065
00d7f4ac 00d7f5c8 0xd7f555
00d7f555 00000000 0xd7f5c8
0:005> dc 78040065
78040065  ???????? ???????? ???????? ???????? ??????????????

```

```

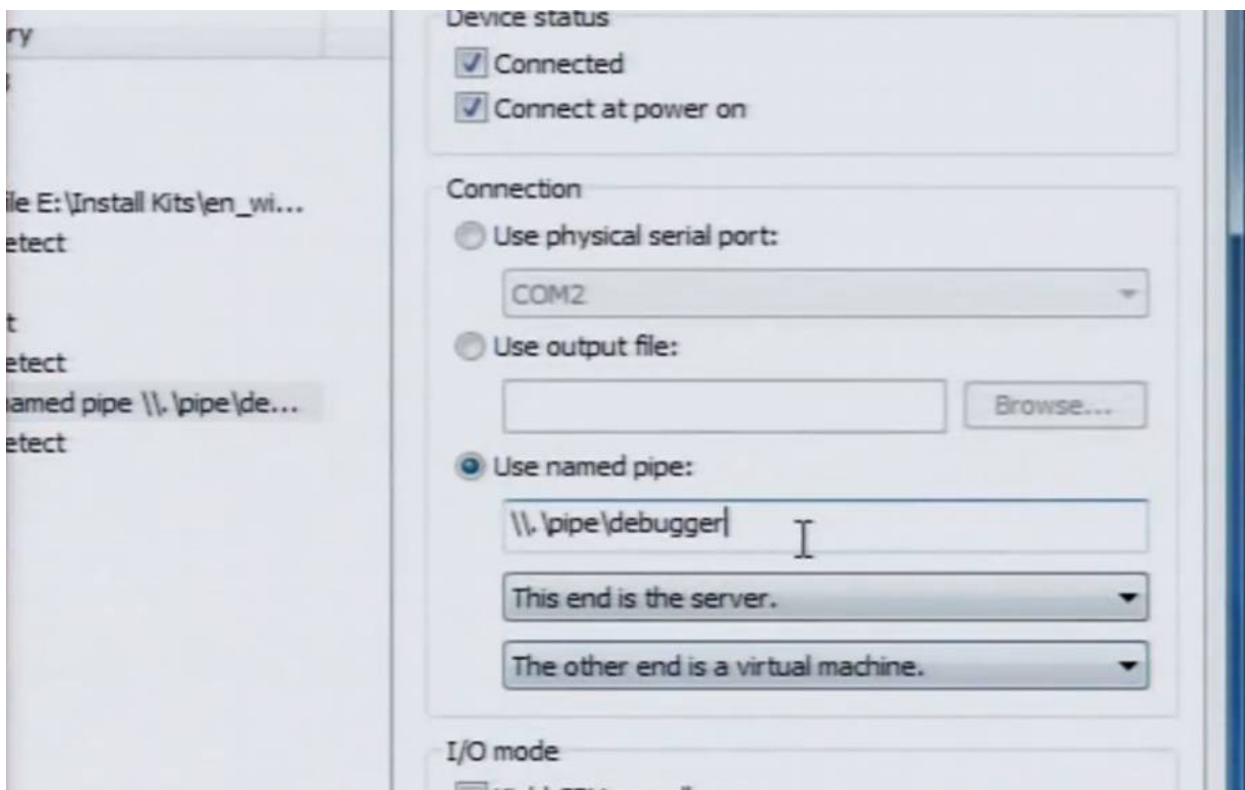
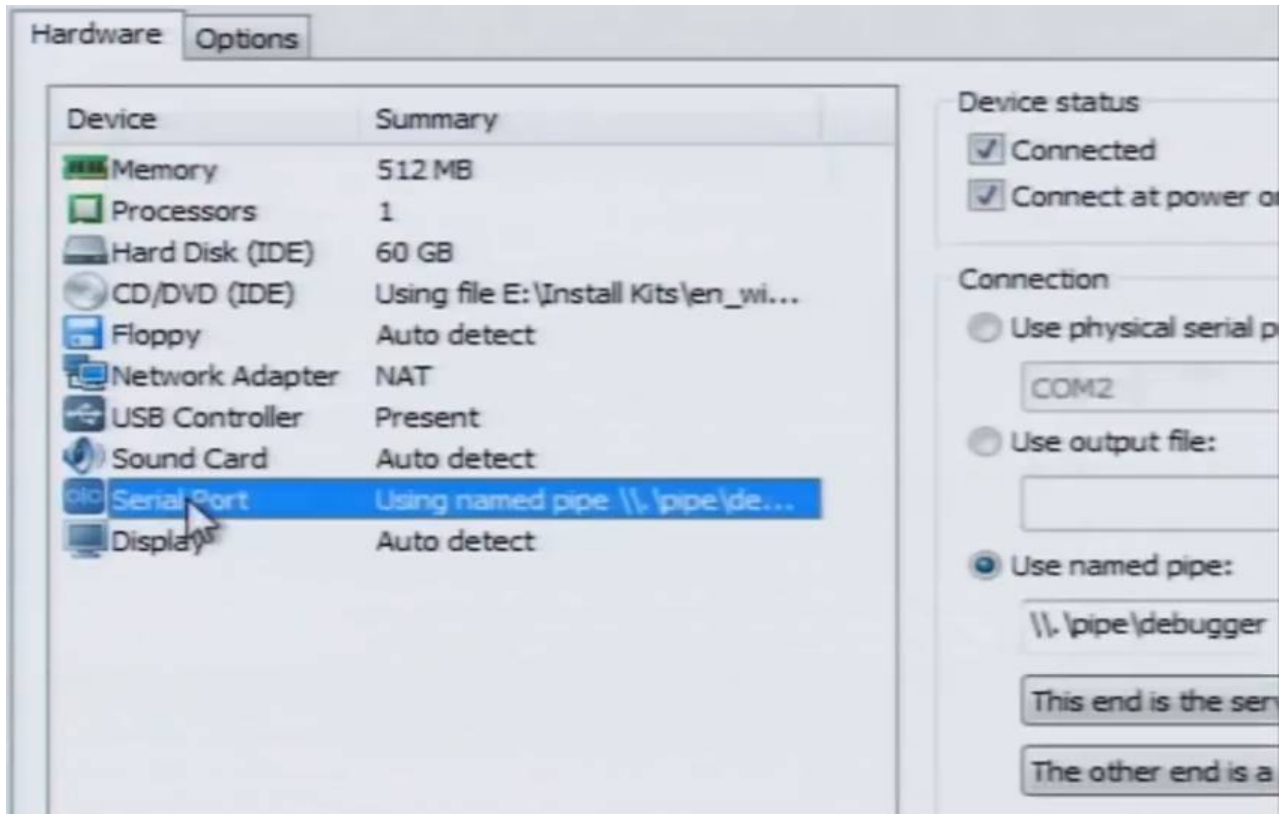
0:005> dc d7f5c8
00d7f5c8 6d6c7275 99006e6f 68d95d23 3a707474 urlmon..#].htt
00d7f5d8 30312f2f 312e322e 362e3331 31383a30 //10.2.113.60:
00d7f5e8 632f3539 69637572 534d007a 4d514953 95/cruciz.MSSJ
00d7f5f8 754e4453 6453467a 614e726b 51715757 SDNuzFSdkrNawW
00d7f608 70417869 44594d6c 6353626b 504d4c43 ixApIMYDkbScCl
00d7f618 67656c42 5674755a 6e594c62 504e5165 BlegZutVbLYneC
00d7f628 616c667a 71436348 45776d6a 4464647a zflaHcCqjmwEzc
00d7f638 50624149 506d6359 61507364 6b644766 IAbPYcmPdsPafC

```

The last picture shows the last code which was executed and crashed the system. Now further investigating steps are needed also without the WinDbg.

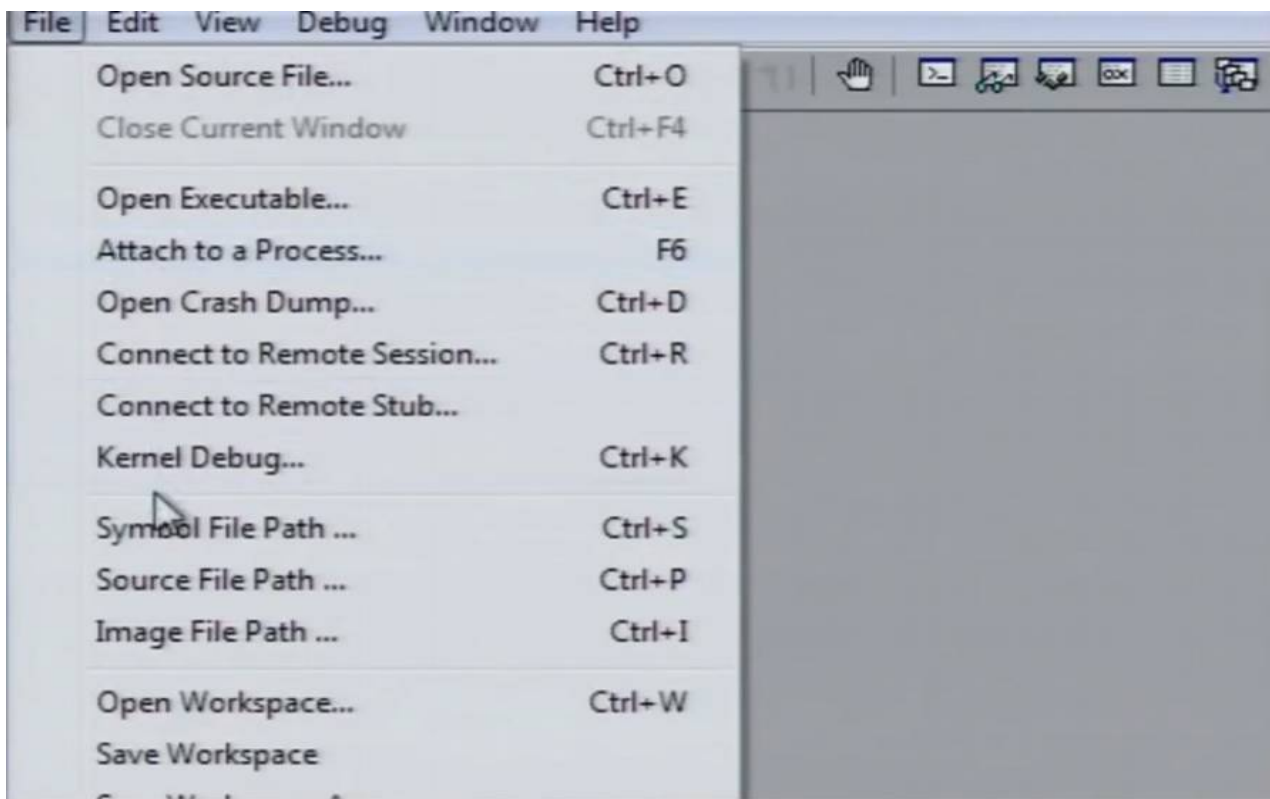
Debugging Steps on Virtual / Remote Machine

To debug a virtual machine or other clients you can add a connection pipe on the virtual machine settings → Hardware → Serial Port to connect with a WinDbg from another machine.

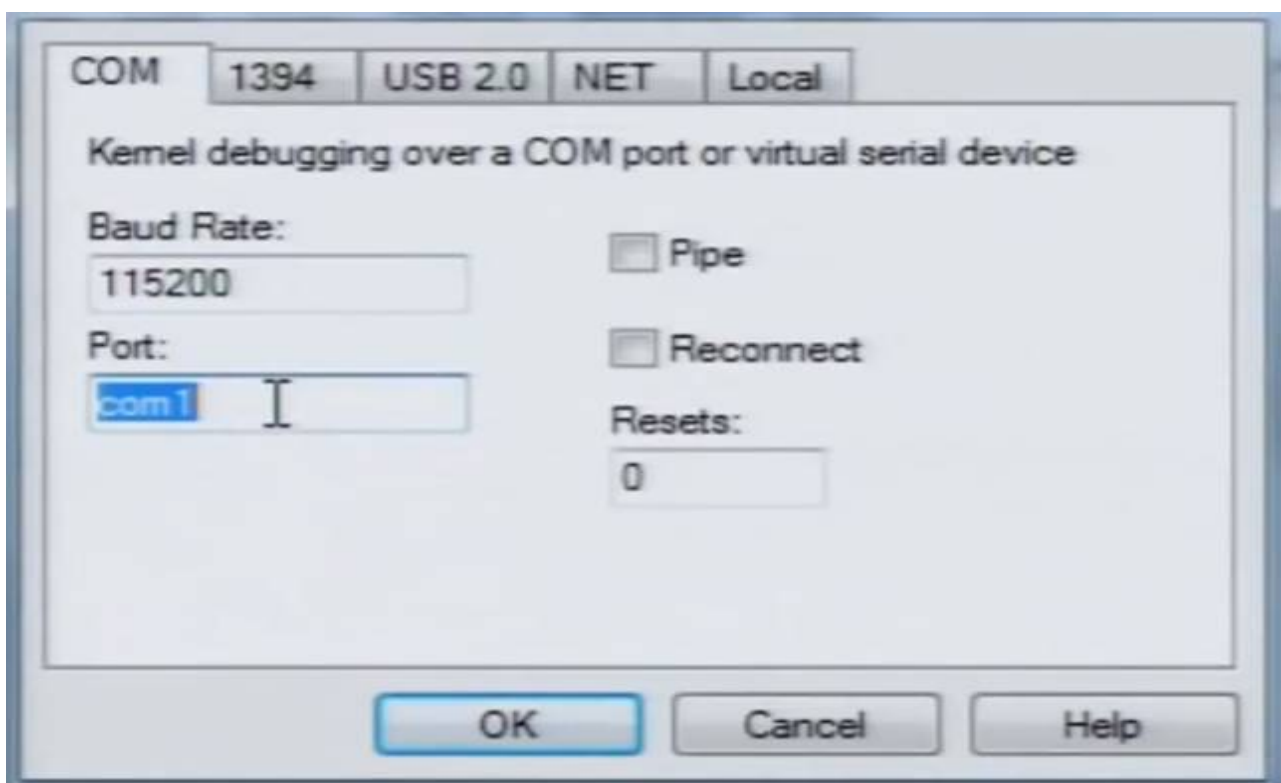


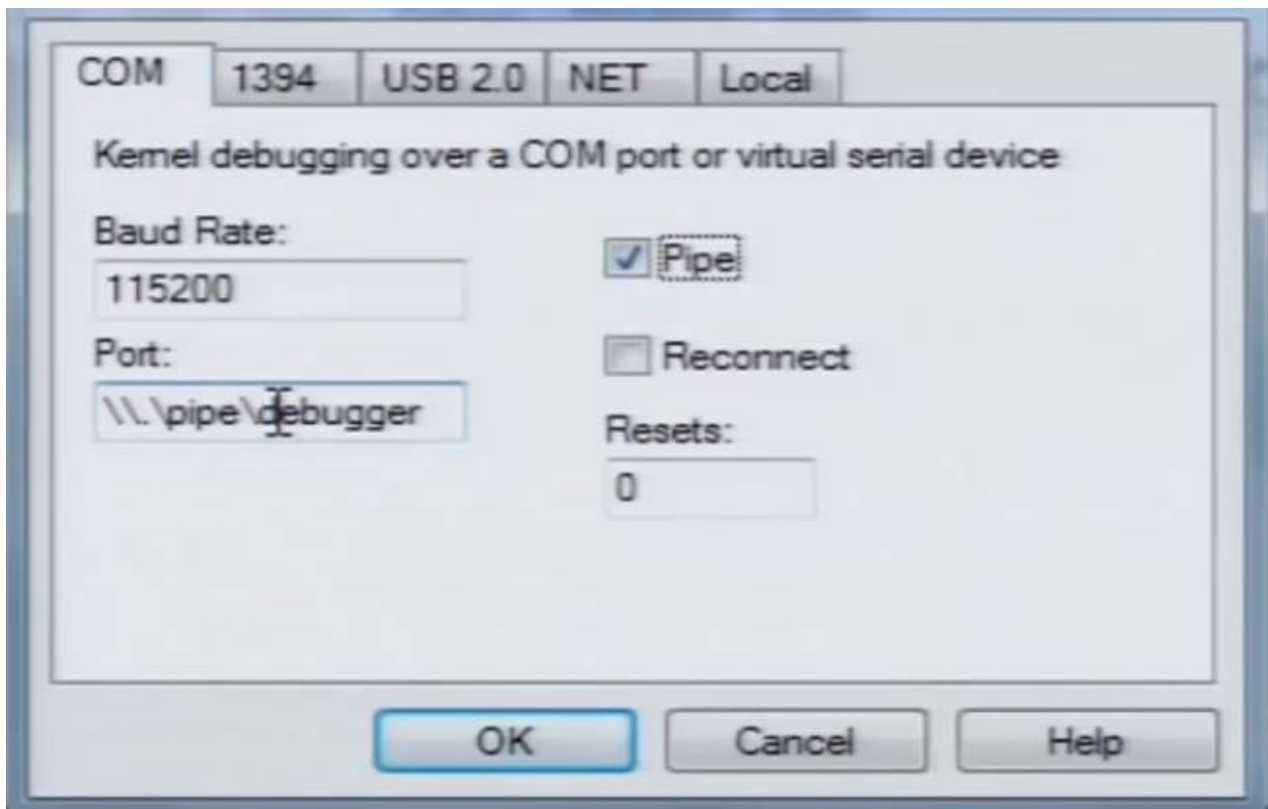
Add a debugging pipe eg. `\\.\pipe\debugger` in the virtual machine menu path.

After that open the WinDbg on the own machine and press the **Kernel Debug** menu option

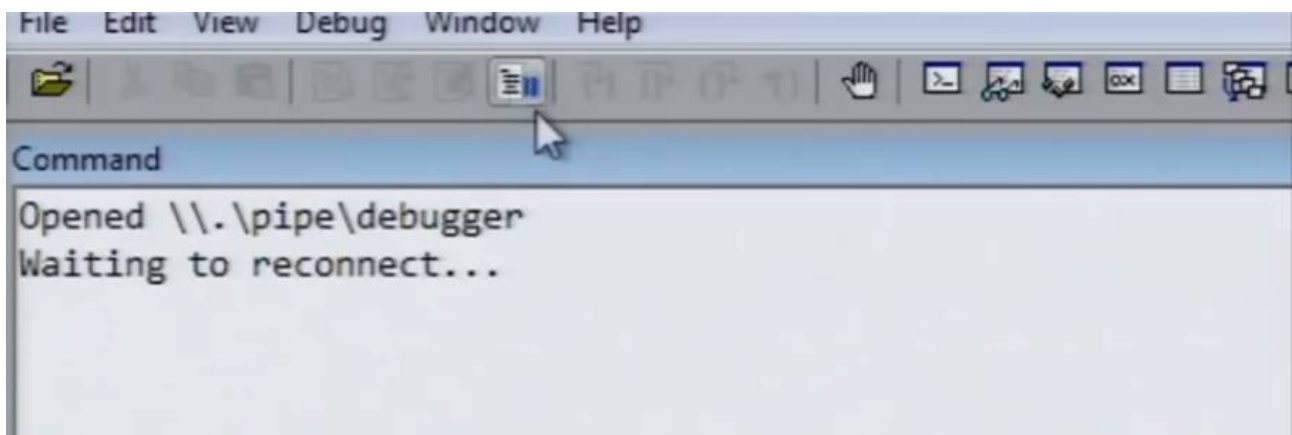


On the open window the default port option is „com1“ enter the pipe from the VM and mark the pipe option

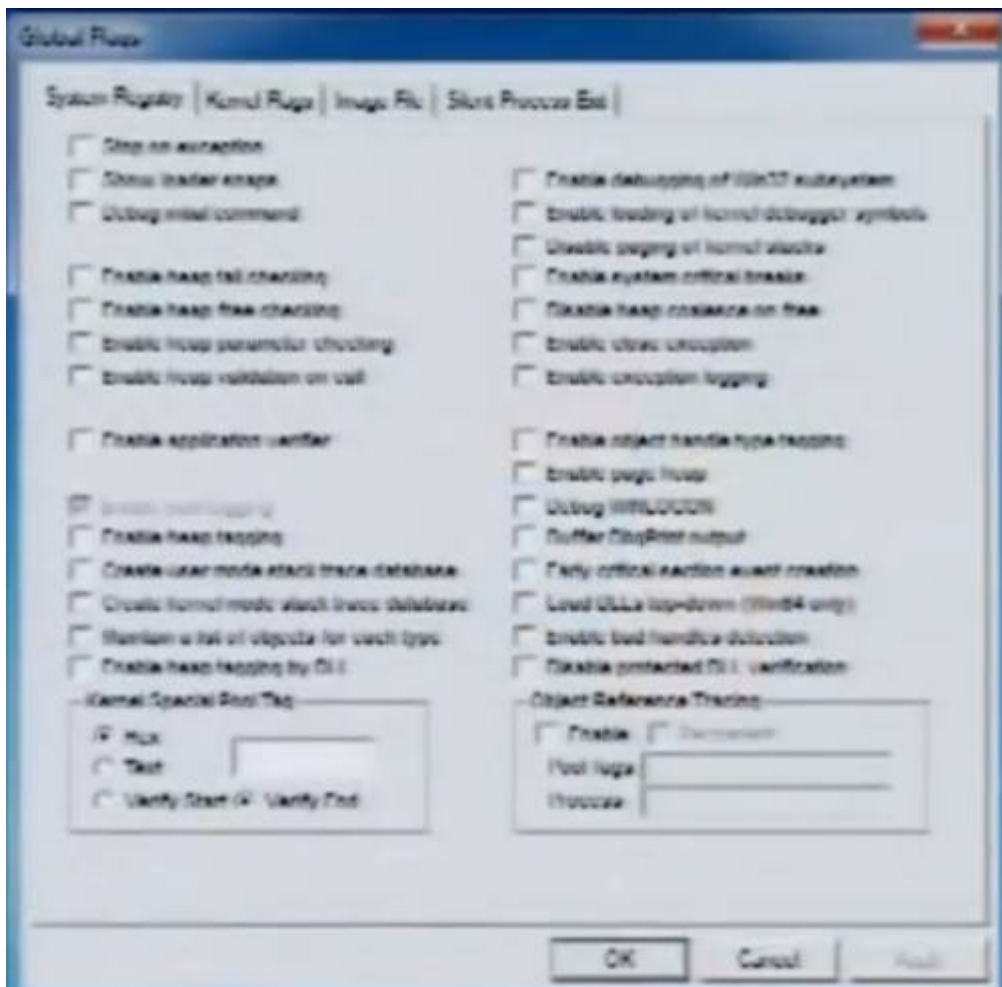




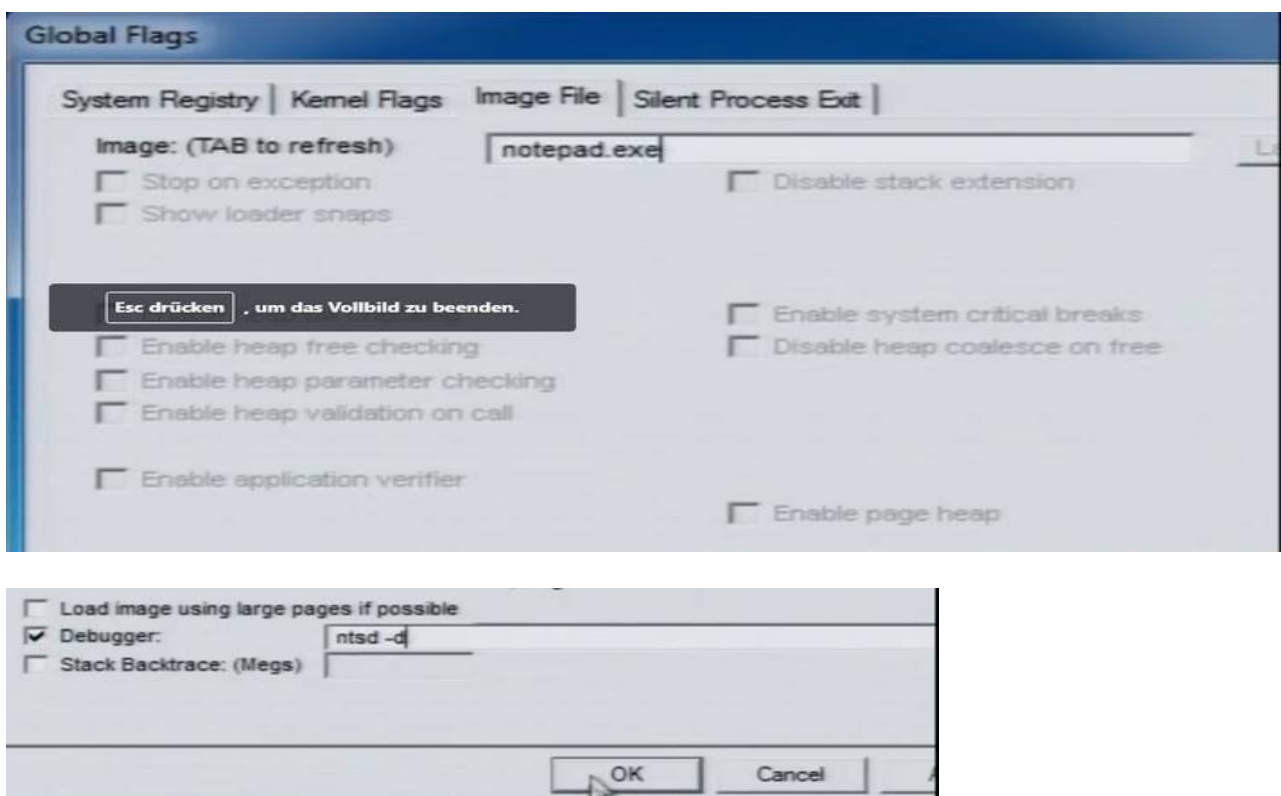
After that press the icon showing in the picture to connect to the machine with the WinDbg. The connected machine is frozen until press the g-command



On the virtual machine install the sysinternal program global flags which provides more debugging options for the virtual machine.



On the option ImageFile it is possible to select the process which you want to debug. On the Debugger field you have also to enter the pipe you choiced

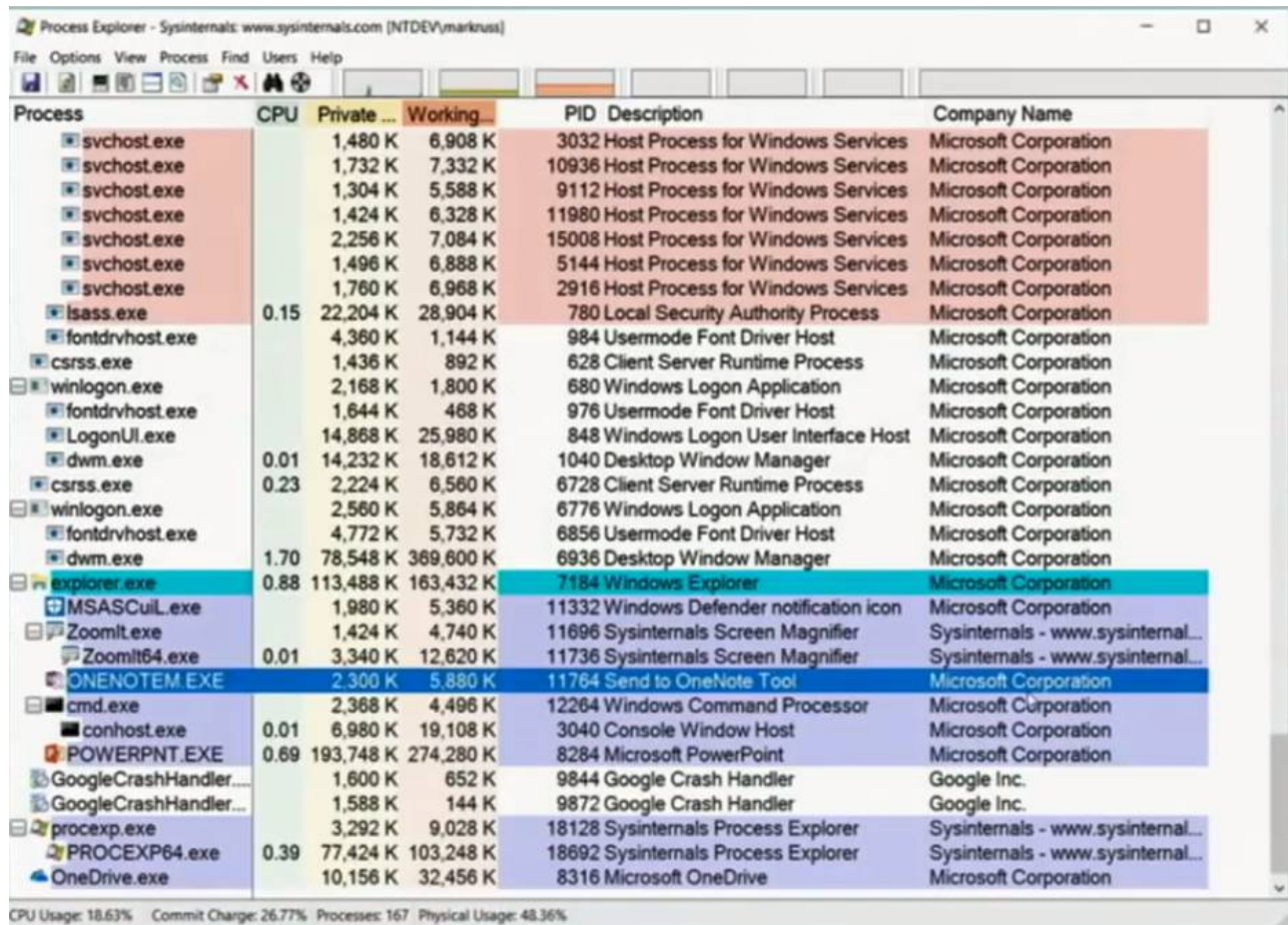


WinDbg – Important Commands in short Overview

g - go	go start the program which is debugged
qd - quite detach	quite detach the debugged programm without close them (important for debugging server)
r – registry values	show register values
db – display bytes	display bytes of specific address include ASCII values
dc - display in bit counter	display in bit counter include ASCII values
~ - Tilde	show number and information of threads
k – kernel thread	show stack information of one kernel thread
~* - Tilde / Star	show stack information of all threads (compare e.g xarg by Linux)
lm - list loaded modules	list loaded modules inside this space
v - verbose	verbose information / most information it can find
m - matching results	matching results into one big output
Machting to one command	example: lm v m malware
!peb – process environment block	displays the information of the process environment block (peb)

Troubelshooting with Process Explorer

Process Explorer is part of the sysinternal tools of windows.



Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\marknuss]

Process	CPU	Private ...	Working...	PID	Description	Company Name
svchost.exe		1,480 K	6,908 K	3032	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,732 K	7,332 K	10936	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,304 K	5,588 K	9112	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,424 K	6,328 K	11980	Host Process for Windows Services	Microsoft Corporation
svchost.exe		2,256 K	7,084 K	15008	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,496 K	6,888 K	5144	Host Process for Windows Services	Microsoft Corporation
svchost.exe		1,760 K	6,968 K	2916	Host Process for Windows Services	Microsoft Corporation
lsass.exe	0.15	22,204 K	28,904 K	780	Local Security Authority Process	Microsoft Corporation
fontdrvhost.exe		4,360 K	1,144 K	984	Usermode Font Driver Host	Microsoft Corporation
csrss.exe		1,436 K	892 K	628	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,168 K	1,800 K	680	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		1,644 K	468 K	976	Usermode Font Driver Host	Microsoft Corporation
LgoinUI.exe		14,868 K	25,980 K	848	Windows Logon User Interface Host	Microsoft Corporation
dwm.exe	0.01	14,232 K	18,612 K	1040	Desktop Window Manager	Microsoft Corporation
csrss.exe	0.23	2,224 K	6,560 K	6728	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,560 K	5,864 K	6776	Windows Logon Application	Microsoft Corporation
fontdrvhost.exe		4,772 K	5,732 K	6856	Usermode Font Driver Host	Microsoft Corporation
dwm.exe	1.70	78,548 K	369,600 K	6936	Desktop Window Manager	Microsoft Corporation
explorer.exe	0.88	113,488 K	163,432 K	7184	Windows Explorer	Microsoft Corporation
MSASCuiL.exe		1,980 K	5,360 K	11332	Windows Defender notification icon	Microsoft Corporation
ZoomIt.exe		1,424 K	4,740 K	11696	Sysinternals Screen Magnifier	Sysinternals - www.sysinternal...
ZoomIt64.exe	0.01	3,340 K	12,620 K	11736	Sysinternals Screen Magnifier	Sysinternals - www.sysinternal...
ONENOTEM.EXE		2,300 K	5,880 K	11764	Send to OneNote Tool	Microsoft Corporation
cmd.exe		2,368 K	4,496 K	12264	Windows Command Processor	Microsoft Corporation
conhost.exe	0.01	6,980 K	19,108 K	3040	Console Window Host	Microsoft Corporation
POWERPNT.EXE	0.69	193,748 K	274,280 K	8284	Microsoft PowerPoint	Microsoft Corporation
GoogleCrashHandler...		1,600 K	652 K	9844	Google Crash Handler	Google Inc.
GoogleCrashHandler...		1,588 K	144 K	9872	Google Crash Handler	Google Inc.
procexp.exe		3,292 K	9,028 K	18128	Sysinternals Process Explorer	Sysinternals - www.sysinternal...
PROCEXP64.exe	0.39	77,424 K	103,248 K	18692	Sysinternals Process Explorer	Sysinternals - www.sysinternal...
OneDrive.exe		10,156 K	32,456 K	8316	Microsoft OneDrive	Microsoft Corporation

CPU Usage: 18.63% Commit Charge: 26.77% Processes: 167 Physical Usage: 48.36%

Process Explorer is called the super taskmanager because he displays very detailed information about currently running processes and futher information. The following Options are of important interest:

By scrolling over a specific process with the mouse it shows the command line command include the name of the program which is running inside them.

File Options View Process Find Users Help

Process	CPU	Private ...	Working...	PID	Description
svchost.exe		11,216 K	12,904 K	11548	Host Process
svchost.exe		2,212 K	4,660 K	13072	Host Process
svchost.exe		7,604 K	17,112 K	13192	Host Process
MsSense.exe	0.60	44,568 K	38,240 K	8516	Windows Defe
svchost.exe		4,056 K	11,964 K	7336	Host Process
svchost.exe		1,680 K	3,568 K	17556	Host Process
svchost.exe		1,884 K	3,500 K	17592	Host Process
svchost.exe		11,212 K	10,932 K	17460	Host Process
SearchIndexer.exe		74,496 K	77,428 K	18284	Microsoft Win
svchost.exe		10,924 K	13,184 K	20036	Host Process
svchost.exe					Host Process
svchost.exe					Host Process
svchost.exe					Host Process
svchost.exe					Host Process
svchost.exe					Host Process
svchost.exe					Host Process
svchost.exe					Host Process

Command Line:
c:\windows\system32\svchost.exe -k netsvcs -s BITS

Path:
c:\Windows\System32\svchost.exe (netsvcs -s BITS)

Services:
Background Intelligent Transfer Service [BITS]

By double clicking to a process a window with detailed overview is open.

svchost.exe:15496 (devicesflow -s DevicesFlowUserSvc) Properties

Image Performance Performance Graph Disk and Network GPU Graph Services Threads TCP/IP Security Environment Job Strings

Image File

Host Process for Windows Services
Microsoft Corporation

Version: 10.0.15063.0
Build Time: Mon Apr 26 07:43:01 1971

Path: c:\Windows\System32\svchost.exe Explore

Command line: c:\windows\system32\svchost.exe -k devicesflow -s DevicesFlowUserSvc

Current directory: C:\Windows\System32\

Autostart Location: HKLM\System\CurrentControlSet\Services\CDPUserSvc_74403 Explore

Parent: services.exe(772)
User: NTDEV\markruss
Started: 3:44:21 PM 9/22/2017 Image: 64-bit

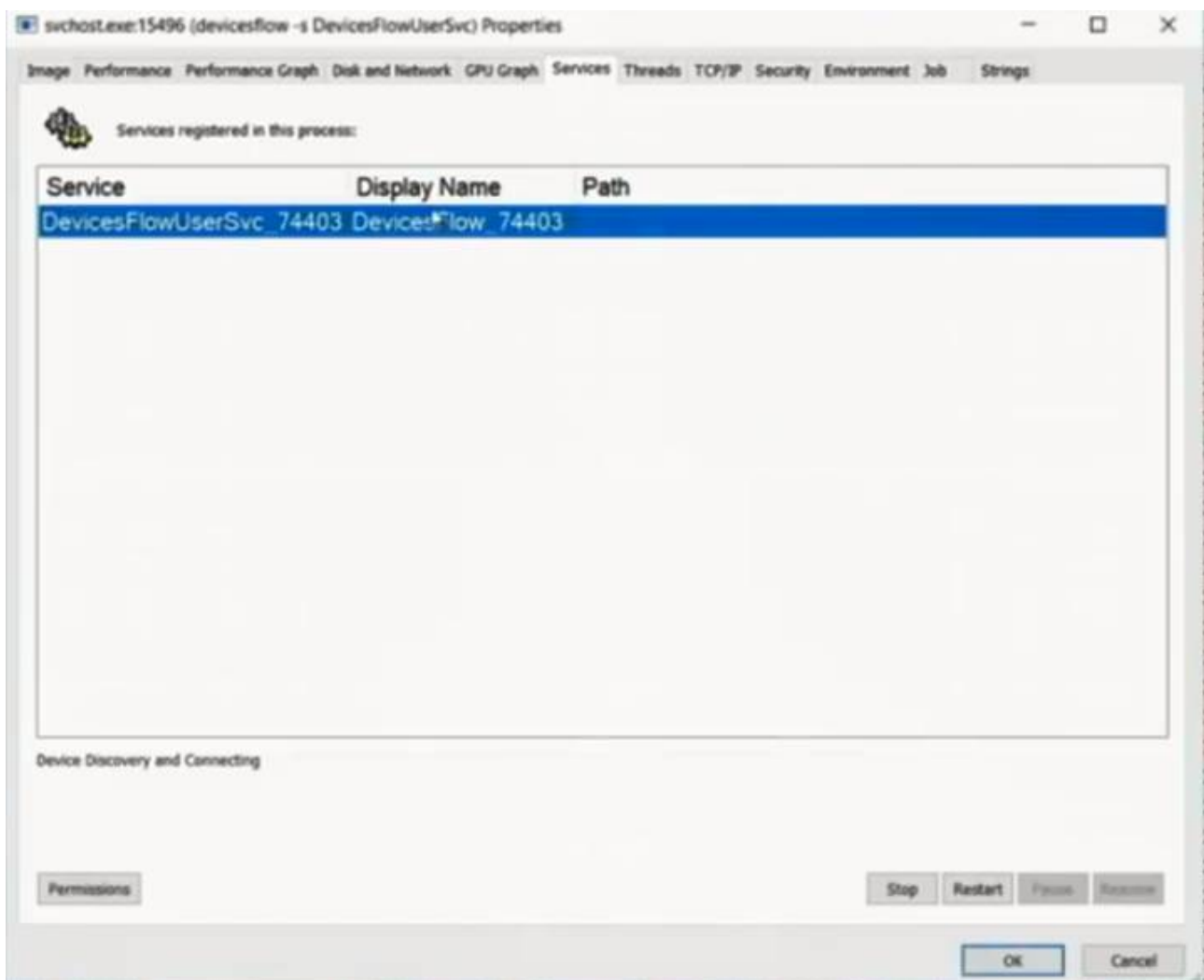
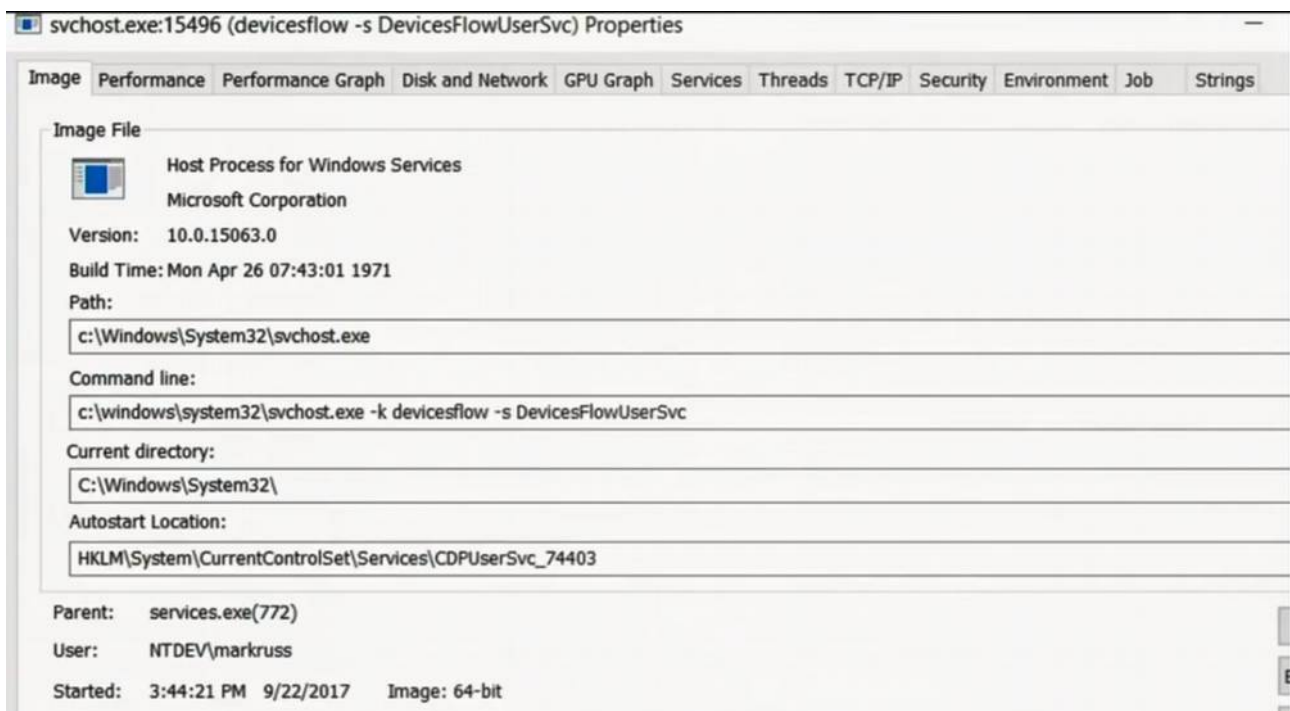
Comment
VirusTotal: Submit

Data Execution Prevention (DEP) Status: Enabled
Address Space Load Randomization: High-Entropy, Bottom-Up
Control Flow Guard: Enabled

Verify
Bring to Front
Kill Process

OK Cancel

The important windows are:



svchost.exe:15496 (devicesflow -s DevicesFlowUserSvc) Properties

Image Performance Performance Graph Disk and Network GPU Graph Services Threads TCP/IP Security Environment Job Strings

Count: 3

TID	CPU	Cycles	Service	Start Address
14320				svchost.exe!wmainCRTSt...
7768			DevicesFlowUserSvc_74403	sechost.dll!ScSvcctrlThre...
12872				ntdll.dll!TppWorkerThread

Thread: 14320

Start: 3:44:21 PM 9/22/2017

State: Wait:UserRequest Base Priority: 8

Kernel: 0:00:00.015 Dynamic Priority: 10

User: 0:00:00.031 I/O Priority: Normal

Context Switches: 43 Memory Priority: 5

Cycles: 49,410,589 Ideal Processor: 3

Stack Module

Permissions Kill Suspend

OK Cancel

svchost.exe:15496 (devicesflow -s DevicesFlowUserSvc) Properties

Image Performance Performance Graph Disk and Network GPU Graph Services Threads TCP/IP Security Environment Job Strings

User: NTDEV\markruss

SID: S-1-5-21-397955417-626881126-188441444-3617895

Session: 2 Logon Session: 5f27

Virtualized: No Protected: No

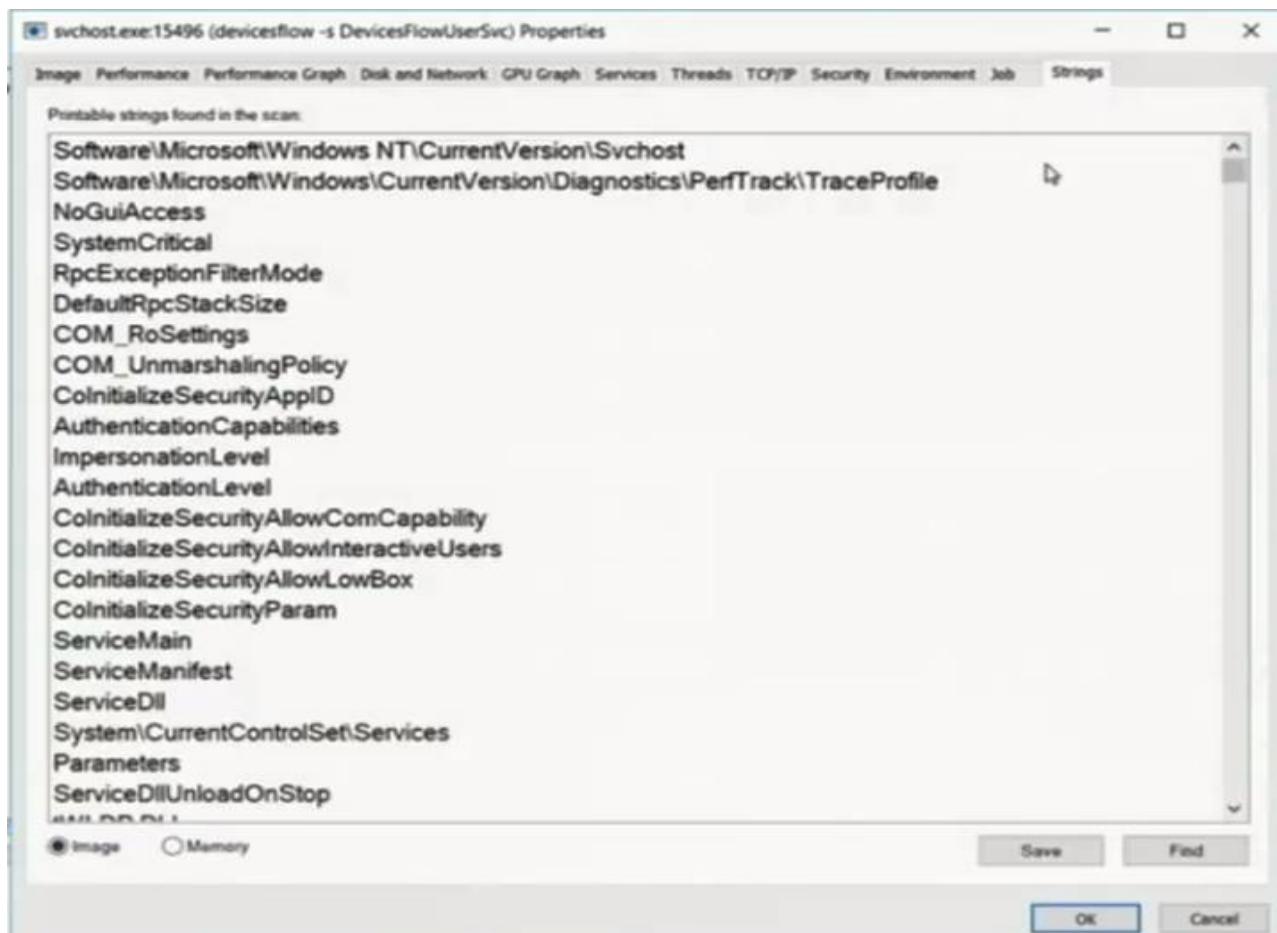
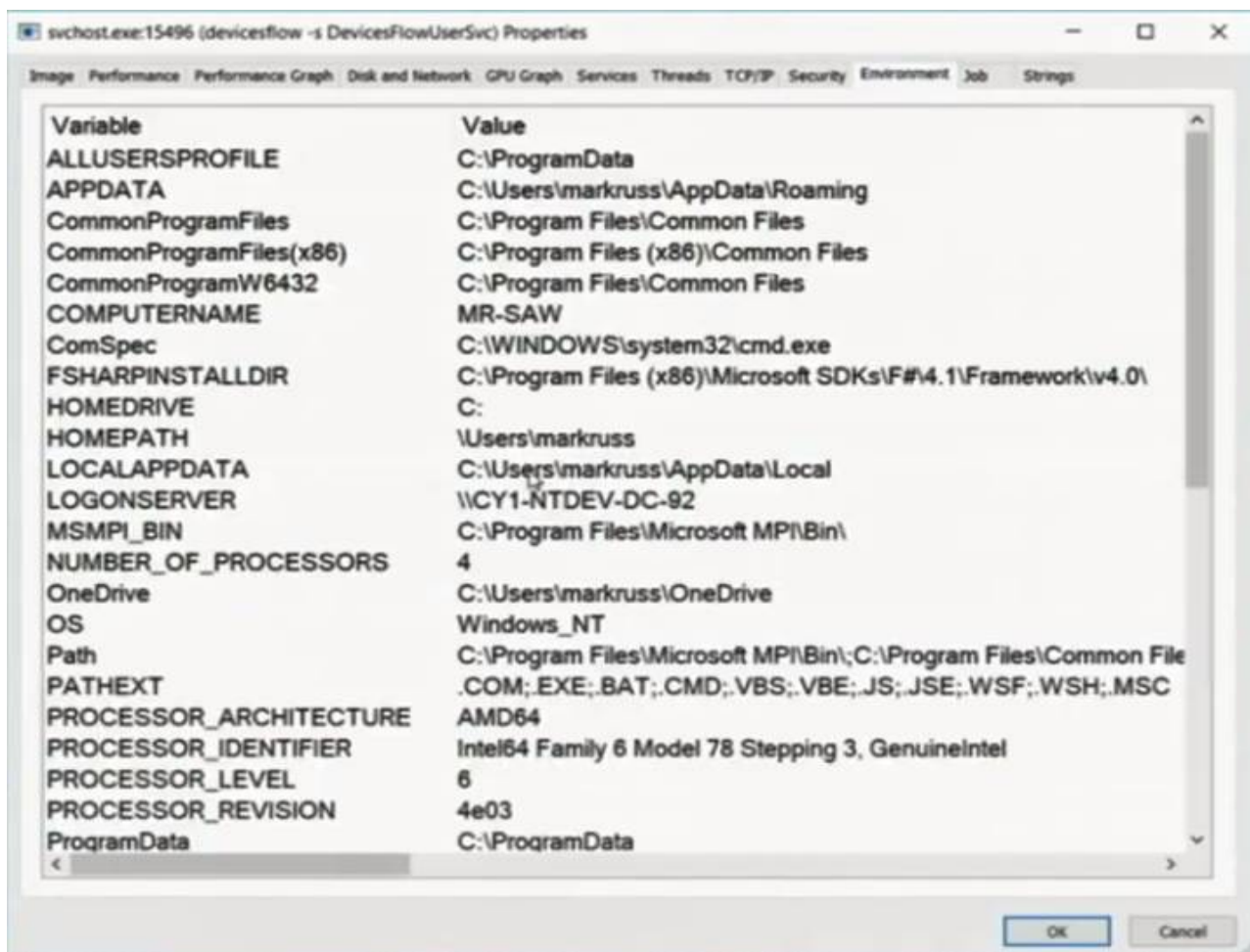
Group	Flags
NT AUTHORITY\LogonSessionId_0_391644	Mandatory
Everyone	Mandatory
Mandatory Label\Medium Mandatory Level	Integrity
Authentication authority asserted identity	Mandatory
LOCAL	Mandatory
NT AUTHORITY\Authenticated Users	Mandatory
NT AUTHORITY\REMOTE INTERACTIVE LOGON	Mandatory
NT AUTHORITY\This Organization	Mandatory
NT AUTHORITY\Claims Valid	Mandatory
S-1-5-21-397955417-626881126-188441444-2931095	Mandatory
S-1-5-21-397955417-626881126-188441444-2931096	Mandatory

Group SID: n/a

Privilege	Flags
SeChangeNotifyPrivilege	Default Enabled
SeIncreaseWorkingSetPrivilege	Disabled
SeShutdownPrivilege	Disabled
SeTimeZonePrivilege	Disabled
SeUndockPrivilege	Disabled

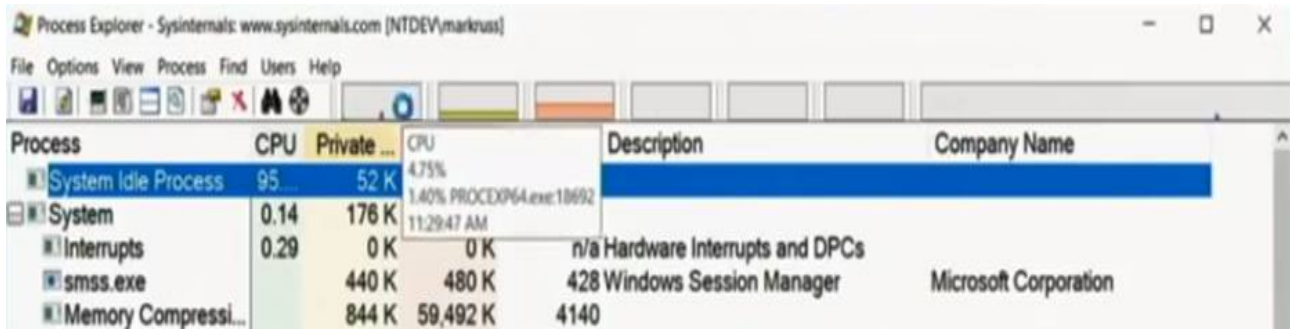
Permissions

OK Cancel

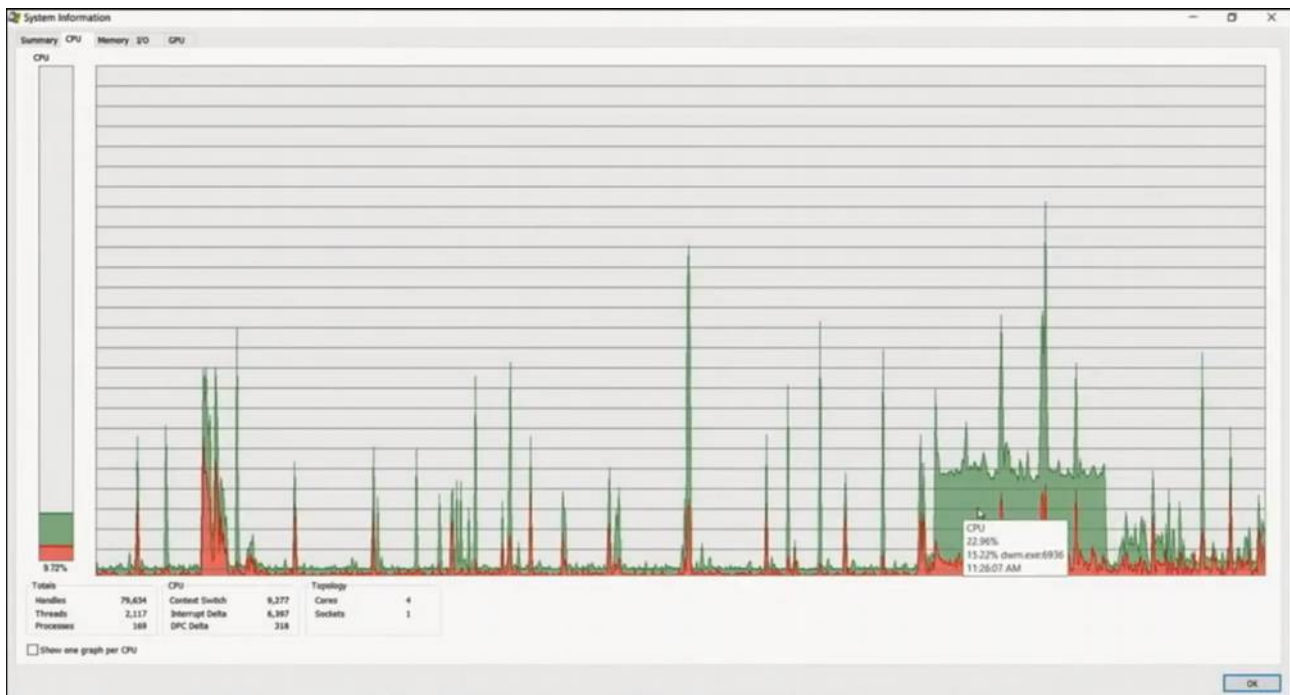


So the important windows of interest are Image, Services, Threads, Security, Environment Variables and Strings.

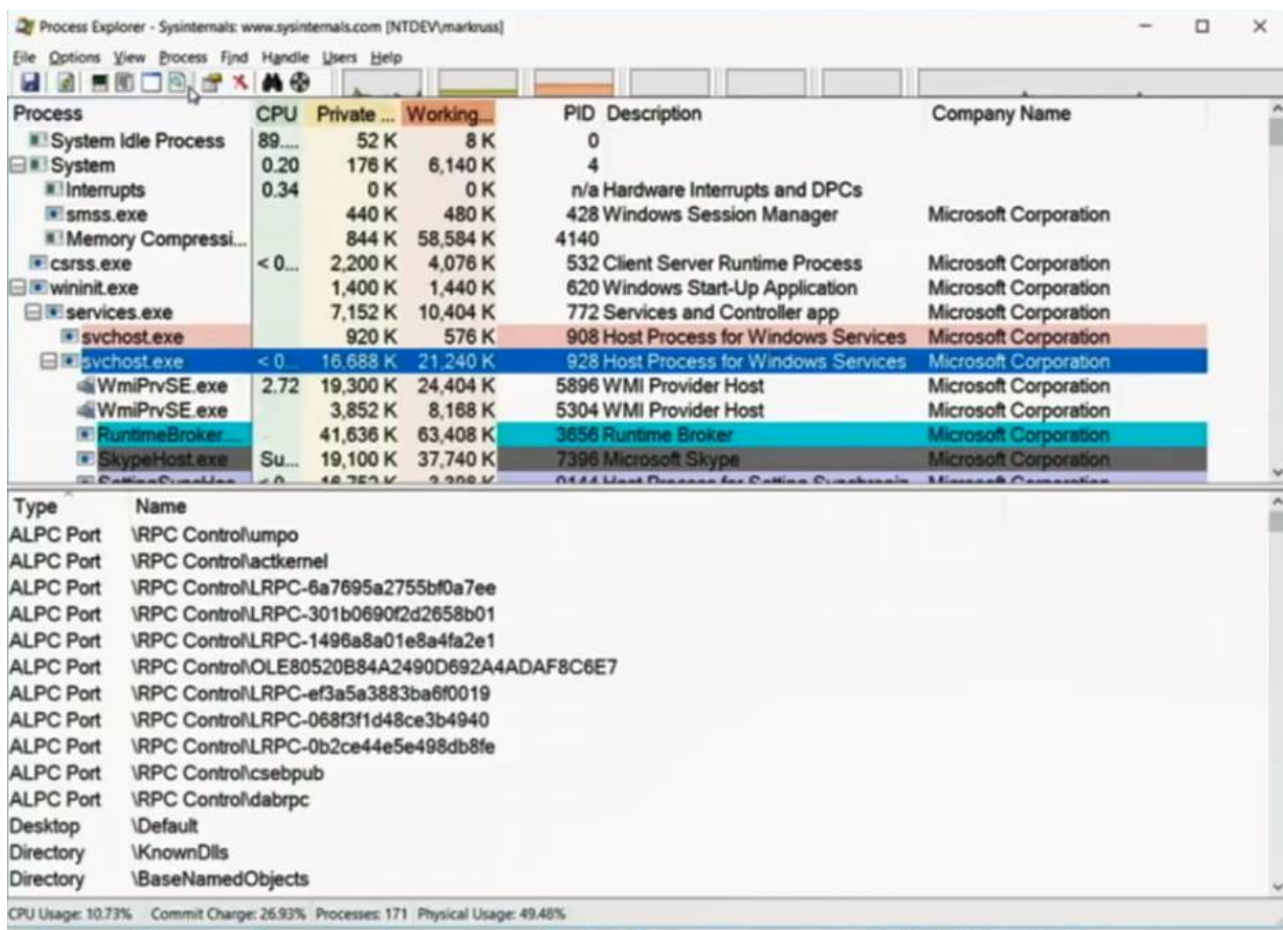
By double click to one of the graphical monitoring blocks on the top of the process explorer it open a window which shows the different processes with the name and marked in different colors



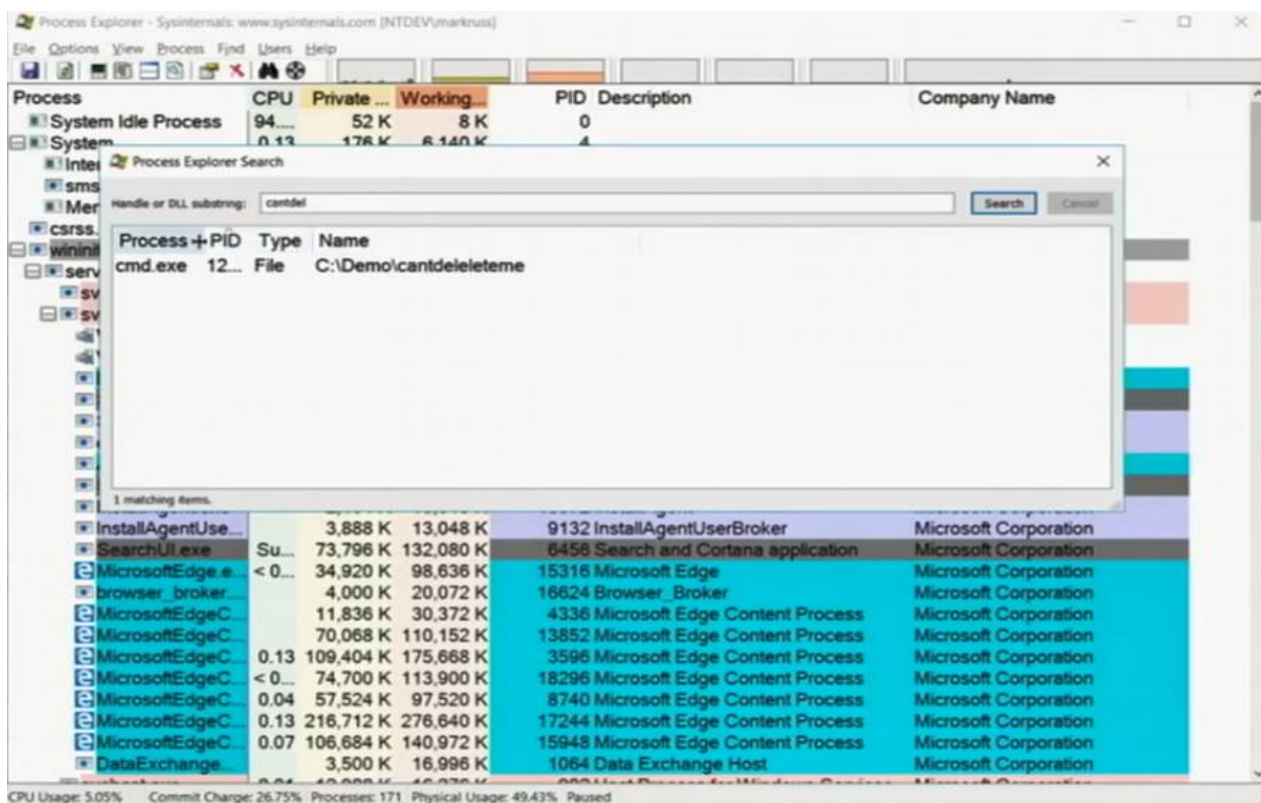
Process	CPU	Private	CPU	Description	Company Name
System Idle Process	95...	52 K	4.75%		
System	0.14	176 K	1.40% PROCXPM6.exe:18692		
Interrupts	0.29	0 K	0 K	n/a Hardware Interrupts and DPCs	
smss.exe		440 K	480 K	428 Windows Session Manager	Microsoft Corporation
Memory Compressi...		844 K	59,492 K	4140	

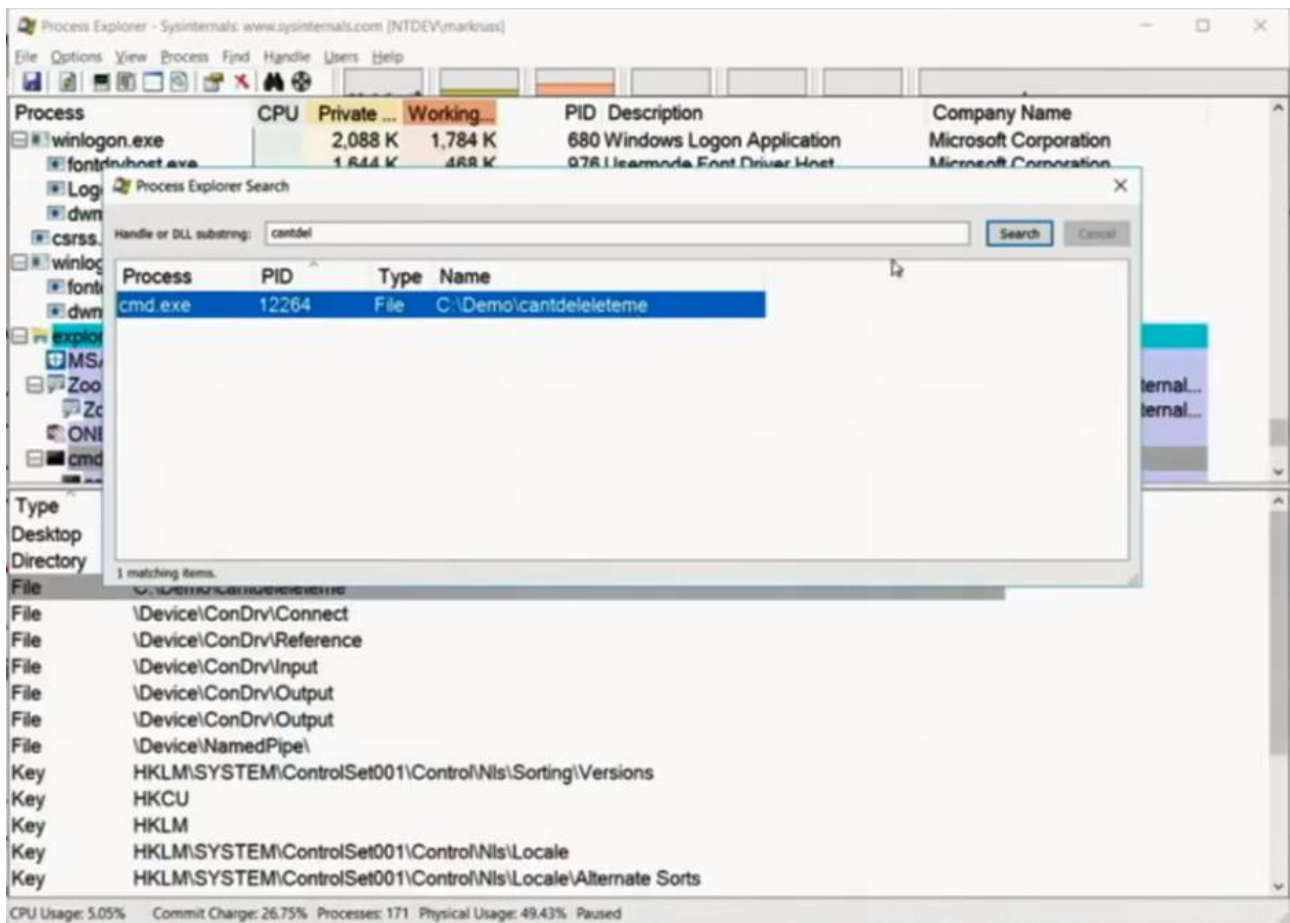


By clicking in the process explorer of one of the symbols of the middle right top you can switch between the active kernel resources and the dll file resources view.



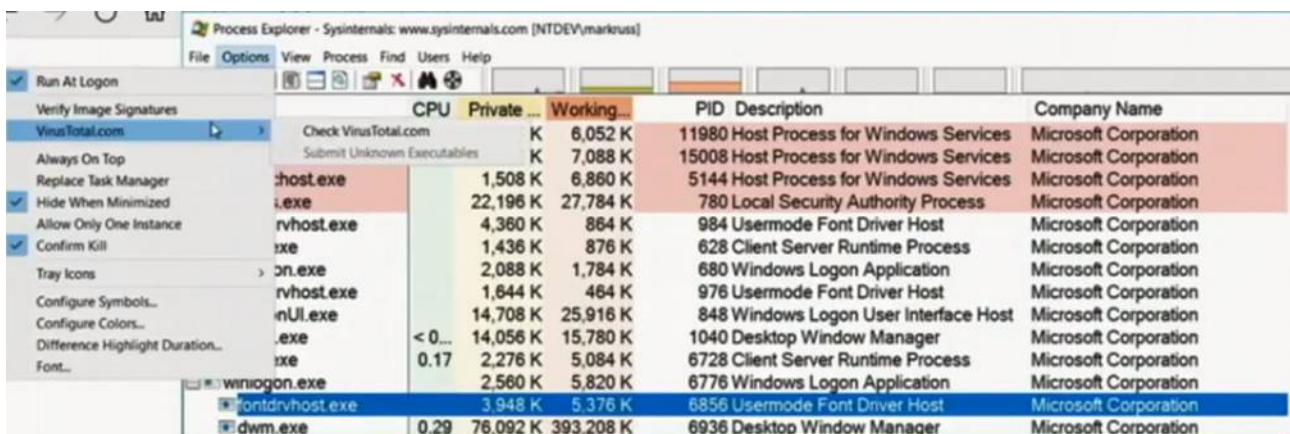
Clicking on the telescope button it opens a search bar which you can search for different matches for the current problem. So it scan the complete bunch in process explorer for that and shows the matched results. By double clicking the result it jumps into details.





Use Process Explorer to find Malware

You can also search for malware use the integrated virus total check (internet connection required). Therefore use the Options register.



After that hashes of the process files will be uploaded to virus total and checked. So the results will be displayed in process explorer as a new field. A match which is up to 10 or more virus engines are highly sure malware.

Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markruss]

File Options View Process Find Users Help

Run At Logon

Verify Image Signatures

VirusTotal.com

Always On Top

Replace Task Manager

Hide When Minimized

Allow Only One Instance

Confirm Kill

Tray Icons

Configure Symbols...

Configure Colors...

Difference Highlight Duration...

Font...

CPU Private ... Working...

Check VirusTotal.com

Submit Unknown Executables

host.exe

svchost.exe

svchost.exe

csrss.exe

winlogon.exe

fontdrvhost.exe

fontdrvhost.exe

dmv.exe

6,052 K

7,088 K

6,880 K

22,196 K

4,360 K

1,436 K

2,088 K

1,644 K

14,708 K

< 0...

2,276 K

2,560 K

3,948 K

76,092 K

8,052 K

7,088 K

6,880 K

27,784 K

864 K

876 K

1,784 K

464 K

25,916 K

15,780 K

5,084 K

5,820 K

5,376 K

393,208 K

11980

15008

5144

780

984

628

680

976

848

1040

6728

6776

6856

6936

Host Process for Windows Services

Host Process for Windows Services

Host Process for Windows Services

Local Security Authority Process

Usermode Font Driver Host

Client Server Runtime Process

Windows Logon Application

Usermode Font Driver Host

Windows Logon User Interface Host

Desktop Window Manager

Client Server Runtime Process

Windows Logon Application

Usermode Font Driver Host

Desktop Window Manager

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

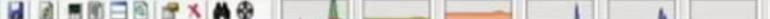
Microsoft Corporation

Microsoft Corporation

Microsoft Corporation

Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markus]

File Options View Process Find Users Help



Process	CPU	Private ...	Working...	PID	Description	Company Name	VirusTotal
svchost.exe		1,424 K	6,052 K	11980	Host Process for Windows Services	Microsoft Corporation	0/64
svchost.exe		2,256 K	7,088 K	15008	Host Process for Windows Services	Microsoft Corporation	0/64
svchost.exe		1,508 K	6,860 K	5144	Host Process for Windows Services	Microsoft Corporation	0/64
lsass.exe	< 0...	22,196 K	27,800 K	780	Local Security Authority Process	Microsoft Corporation	0/65
fontdrvhost.exe		4,360 K	864 K	984	Usermode Font Driver Host	Microsoft Corporation	0/65
csrss.exe		1,436 K	876 K	628	Client Server Runtime Process	Microsoft Corporation	0/63
winlogon.exe		2,088 K	1,784 K	680	Windows Logon Application	Microsoft Corporation	0/65
fontdrvhost.exe		1,644 K	464 K	976	Usermode Font Driver Host	Microsoft Corporation	0/65
LogonUI.exe		14,708 K	25,916 K	848	Windows Logon User Interface Host	Microsoft Corporation	0/65

A second option is added in the Option register for virus total called Verify Image Signatures which verify all signatures on the system showing in process explorer

Process Explorer - Sysinternals: www.sysinternals.com [NTDEV\markrus]

File Options View Process Find Users Help

Run At Logon

Verify Image Signatures

VirusTotal.com

Always On Top

Replace Task Manager

Hide When Minimized

Allow Only One Instance

Confirm Kill

Tray Icons

Configure Symbols...

Configure Colors...

Difference Highlight Duration...

Font...

	CPU	Private ...	Working...	PID	Description	Company Name	VirusTotal
svchost.exe	0.19	2,292 K	5,024 K	6728	Client Server Runtime Process	Microsoft Corporation	0/63
svchost.exe	0.12	2,560 K	5,820 K	6776	Windows Logon Application	Microsoft Corporation	0/65
svchost.exe	0.53	77,856 K	404,532 K	6856	Usermode Font Driver Host	Microsoft Corporation	0/65
svchost.exe	0.12	88,760 K	161,988 K	6936	Desktop Window Manager	Microsoft Corporation	0/65
explorer.exe	0.12	88,760 K	161,988 K	7184	Windows Explorer	Microsoft Corporation	0/64
smss.exe	1,980 K	5,364 K	11332	Windows Defender notification icon	Microsoft Corporation	0/65	
notepad.exe	1,424 K	4,736 K	11696	Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.com	0/65	
cmd.exe	3,392 K	21,240 K	11736	Sysinternals Screen Magnifier	Sysinternals - www.sysinternals.com	Unknown	
notepad.exe	2,300 K	5,504 K	11764	Send to OneNote Tool	Microsoft Corporation	0/64	
notepad.exe	2,368 K	16,596 K	12264	Windows Command Processor	Microsoft Corporation	0/65	
notepad.exe	6,992 K	19,408 K	3040	Console Window Host	Microsoft Corporation	0/64	
notepad.exe	224,100 K	263,936 K	8284	Microsoft PowerPoint	Microsoft Corporation	0/65	
notepad.exe	2,484 K	3,868 K	13300	Windows Command Processor	Microsoft Corporation	0/65	
notepad.exe	7,332 K	25,952 K	4216	Console Window Host	Microsoft Corporation	0/64	

Option	Status
Run At Logon	Checked
Verify Image Signatures	Checked
VirusTotal.com	Checked
Always On Top	Not Checked
Replace Task Manager	Not Checked
Hide When Minimized	Checked
Allow Only One Instance	Not Checked
Confirm Kill	Checked
Tray Icons	Not Checked
Configure Symbols...	Not Checked
Configure Colors...	Not Checked
Difference Highlight Duration...	Not Checked
Font...	Not Checked

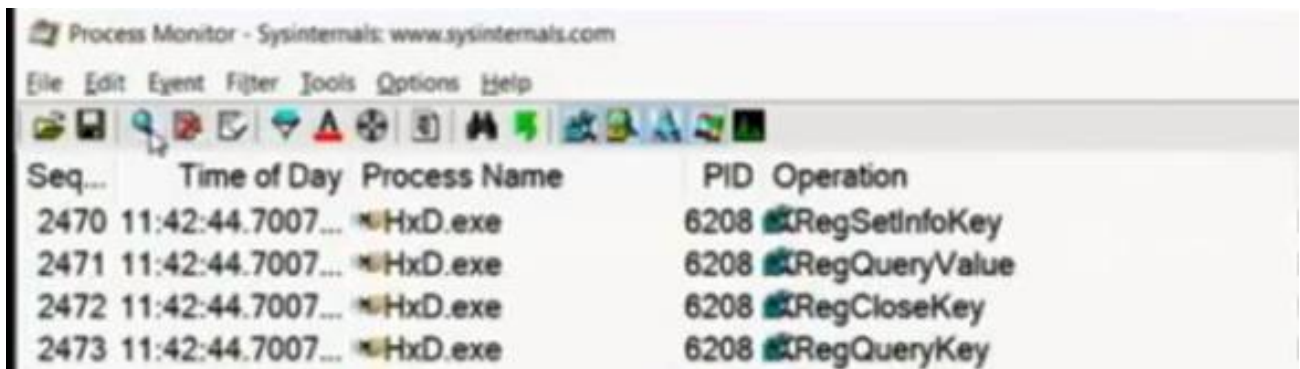
Company Name	VirusTotal	Verified Signer
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/64	(Verified) Microsoft Corporation
Microsoft Corp.	0/64	(Verified) Microsoft Corporation
Microsoft Corp.	0/64	(Verified) Microsoft Corporation
Microsoft Corporation	0/63	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/65	(Verified) Microsoft Corporation
Microsoft Corporation	0/63	(Verified) Microsoft Corporation

Troubelshooting with Process Monitor (Procmon)

By starting process monitor it starts capturing every traffic on the system immediatly.

Seq...	Time of Day	Process Name	PID	Operation	Path	Result	Detail
0	11:36:09.8016...	svchost.exe	3320	TCP Send	mi-saw.ntdev.corp.microsoft.com:21721 -> red1.ras...	SUCCESS	Length: 229, starttime: 47212722, endtim...
1	11:36:09.8016...	svchost.exe	3320	TCP Receive	mi-saw.ntdev.corp.microsoft.com:21721 -> red1.ras...	SUCCESS	Length: 261, seqnum: 0, connid: 0
2	11:36:09.8027...	SearchIndexer.exe	18...	FileSystemControl	C:	SUCCESS	Length: 229, starttime: 47212722, endtim...
3	11:36:09.8027...	SearchIndexer.exe	18...	FileSystemControl	C:	SUCCESS	Control: FSCTL_READ_USN_JOURNAL
4	11:36:09.8053...	taskhostw.exe	7296	RegOpenKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
5	11:36:09.8053...	taskhostw.exe	7296	RegOpenKey	HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
6	11:36:09.8054...	taskhostw.exe	7296	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\EnableTest...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
7	11:36:09.8054...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
8	11:36:09.8056...	taskhostw.exe	7296	RegOpenKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
9	11:36:09.8056...	taskhostw.exe	7296	RegOpenKey	HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
10	11:36:09.8057...	taskhostw.exe	7296	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11	11:36:09.8057...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
12	11:36:09.8058...	taskhostw.exe	7296	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
13	11:36:09.8059...	taskhostw.exe	7296	RegOpenKey	HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
14	11:36:09.8060...	taskhostw.exe	7296	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
15	11:36:09.8060...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
16	11:36:09.8265...	svchost.exe	1572	WriteFile	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,166,144, Length: 65,536
17	11:36:09.8291...	svchost.exe	1572	WriteFile	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,231,680, Length: 65,536
18	11:36:09.8294...	MicrosoftEdgeCP.exe	8740	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
19	11:36:09.8295...	MicrosoftEdgeCP.exe	8740	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersi...	SUCCESS	Desired Access: Read
20	11:36:09.8295...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	Type: REG_SZ, Length: 108, Data: "C:\...
21	11:36:09.8296...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
22	11:36:09.8296...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
23	11:36:09.8296...	MicrosoftEdgeCP.exe	8740	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	
24	11:36:09.8297...	MicrosoftEdgeCP.exe	8740	RegOpenKey	HKU	SUCCESS	Query: HandleTags, HandleTags: 0x0
25	11:36:09.8297...	MicrosoftEdgeCP.exe	8740	RegOpenKey	HKCU\Software\Classes\Local Settings\Software\IML...	REPARSE	Desired Access: Query Value
26	11:36:09.8297...	MicrosoftEdgeCP.exe	8740	RegOpenKey	HKCU\Software\Classes\Local Settings\Software\IML...	SUCCESS	Desired Access: Query Value
27	11:36:09.8298...	MicrosoftEdgeCP.exe	8740	RegQueryValue	HKCU\Software\Classes\Local Settings\Software\IML...	SUCCESS	Type: REG_SZ, Length: 8, Data: 001
28	11:36:09.8298...	MicrosoftEdgeCP.exe	8740	RegCloseKey	HKCU\Software\Classes\Local Settings\Software\IML...	SUCCESS	

To stop process monitor to capture the traffic clicking on the search button on the top. It will stop and display a searchbutton with a black string. You can continue capturing by cklicking the search button again.

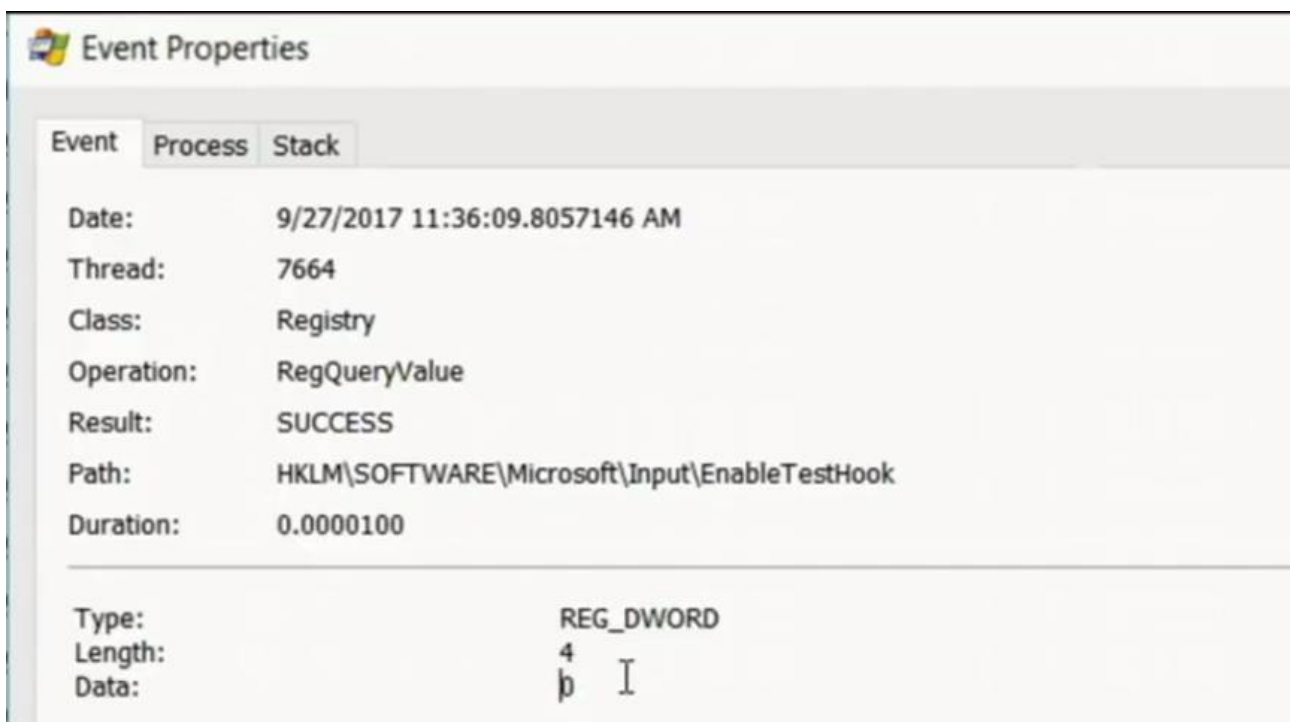


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Seq...	Time of Day	Process Name	PID	Operation
2470	11:42:44.7007...	HxD.exe	6208	RegSetInfoKey
2471	11:42:44.7007...	HxD.exe	6208	RegQueryValue
2472	11:42:44.7007...	HxD.exe	6208	RegCloseKey
2473	11:42:44.7007...	HxD.exe	6208	RegQueryKey

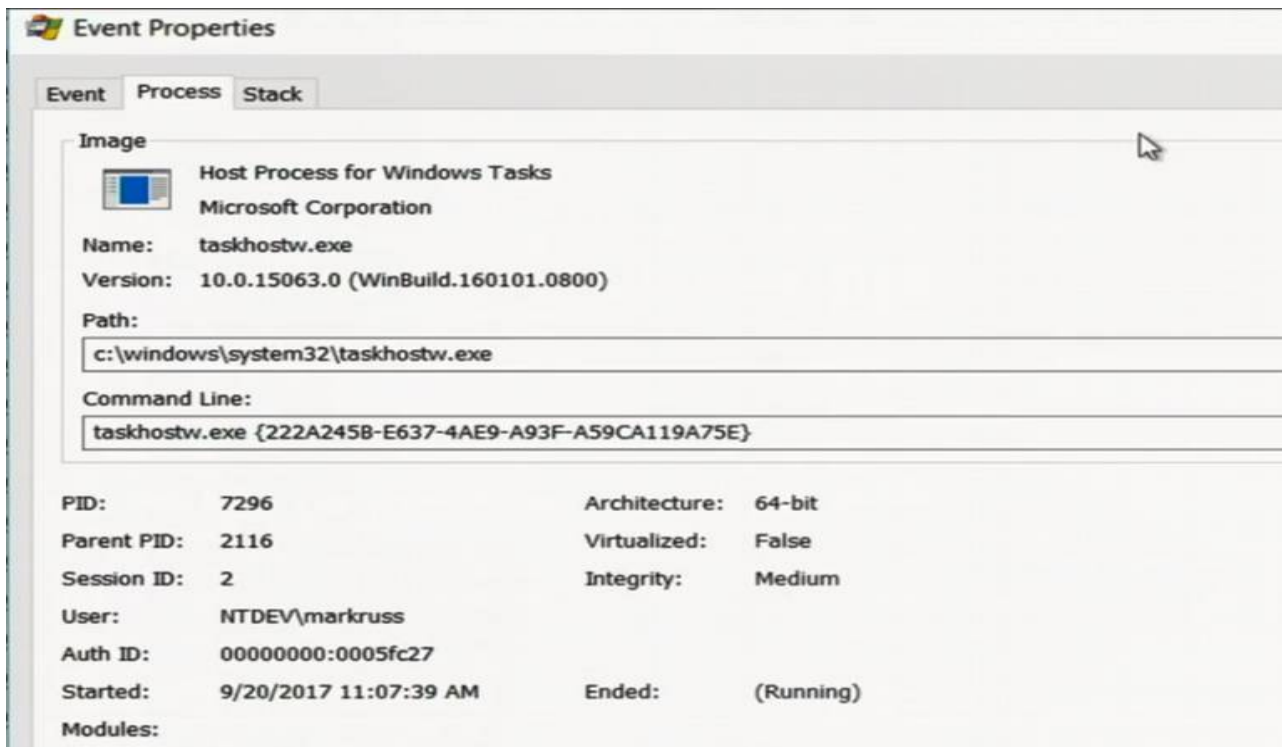
By double clicking of one of the running processes it opens a window which shows detailed information about the current process.



Event Properties

Event	Process	Stack
Date:	9/27/2017 11:36:09.8057146 AM	
Thread:	7664	
Class:	Registry	
Operation:	RegQueryValue	
Result:	SUCCESS	
Path:	HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	
Duration:	0.0000100	
Type:	REG_DWORD	
Length:	4	
Data:	p I	

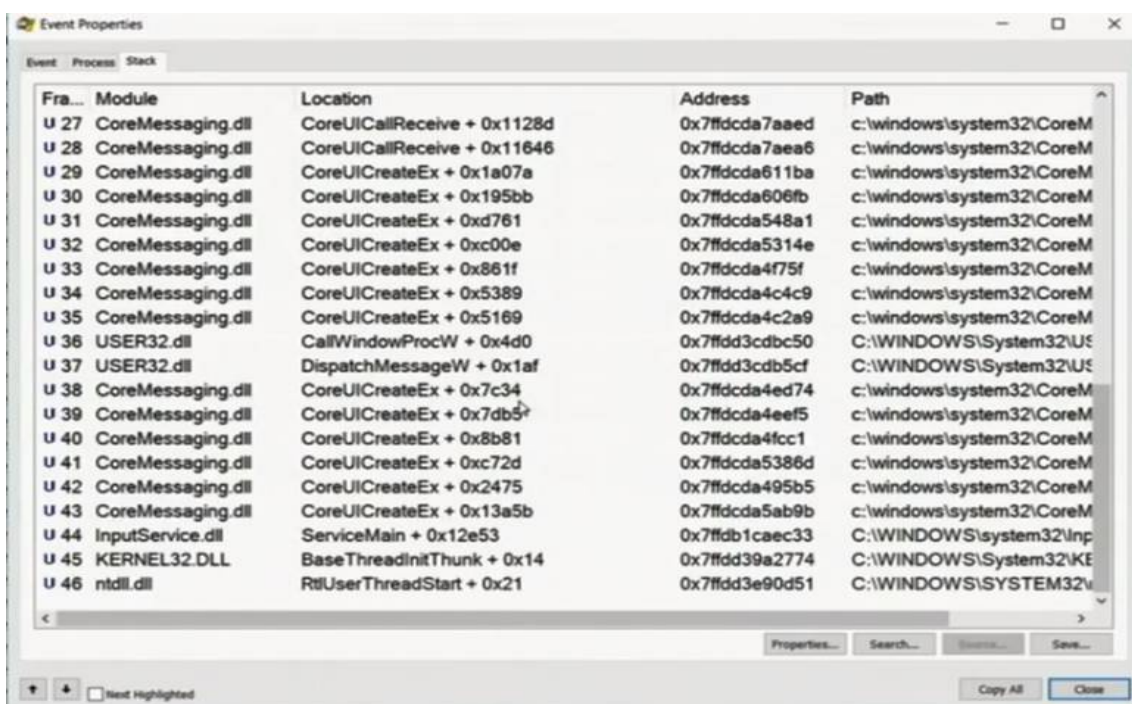
The Process register contains the same information as process explorer including dll Moduls.



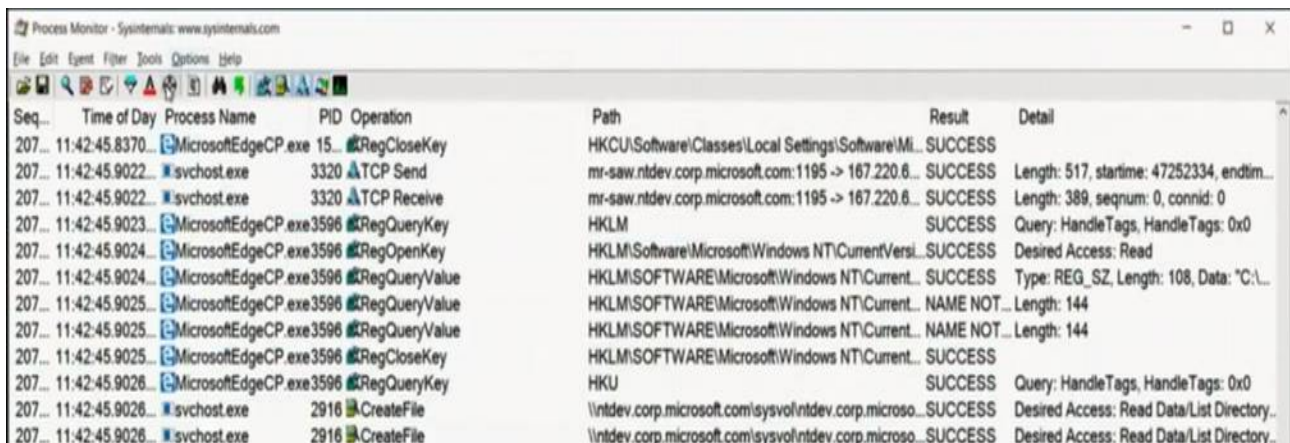
Modules:

Module	Address	Size	Path	Company	Version
taskhostw.exe	0x7ff786ed0000	0x18000	c:\windows\system32\taskhostw.exe	Microsoft Corpor...	10.0.1506
tiptsf.dll	0x7ffdb0cf0000	0xa1000	C:\Program Files\Common Files\microso...	Microsoft Corpor...	10.0.1506
EditBufferTestHoo...	0x7ffdb1c70000	0x18000	c:\windows\system32>EditBufferTestHo...	Microsoft Corpor...	10.0.1506
InputService.dll	0x7ffdb1c90000	0x2d7000	C:\WINDOWS\system32\InputService.dll	Microsoft Corpor...	10.0.1506
PlaySndSrv.dll	0x7ffdb2010000	0x1a000	C:\WINDOWS\System32\PlaySndSrv.dll	Microsoft Corpor...	10.0.1506
MSUTB.dll	0x7ffdb2030000	0x77000	C:\WINDOWS\system32\MSUTB.dll	Microsoft Corpor...	10.0.1506
MsCtfMonitor.dll	0x7ffdb2360000	0x16000	C:\WINDOWS\system32\MsCtfMonitor.dll	Microsoft Corpor...	10.0.1506
innuthost.dll	0x7ffdb3a20000	0x24000	C:\WINDOWS\SYSTEM32\innuthost.dll		

The **Stack register** shows the **functions in the dll modules which was executed by the program**

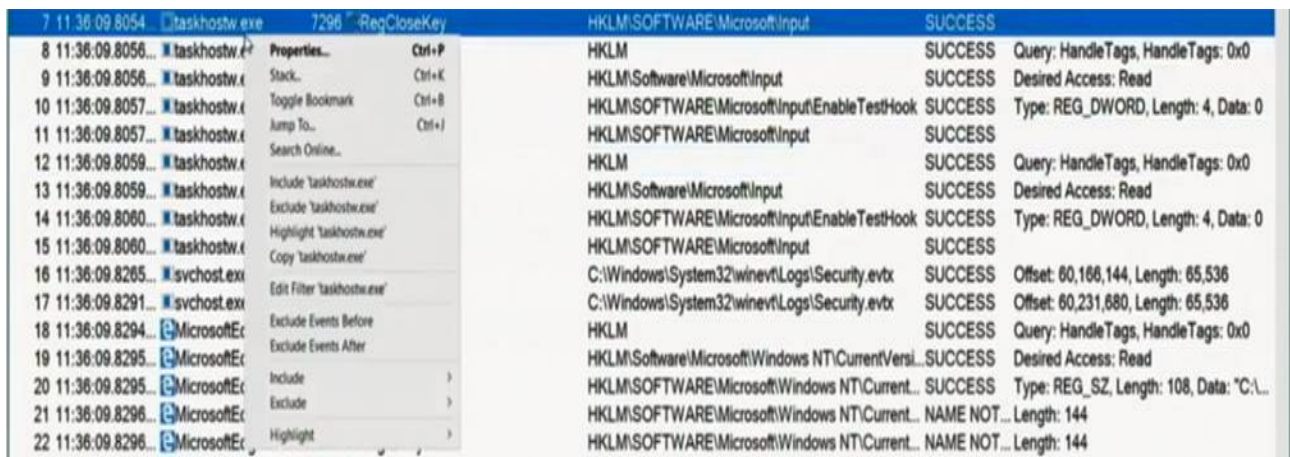


For filtering for a specific process the easiest way if the program is running in foreground is to use the capture button and capture this process by sliding with the mouse to the program window.

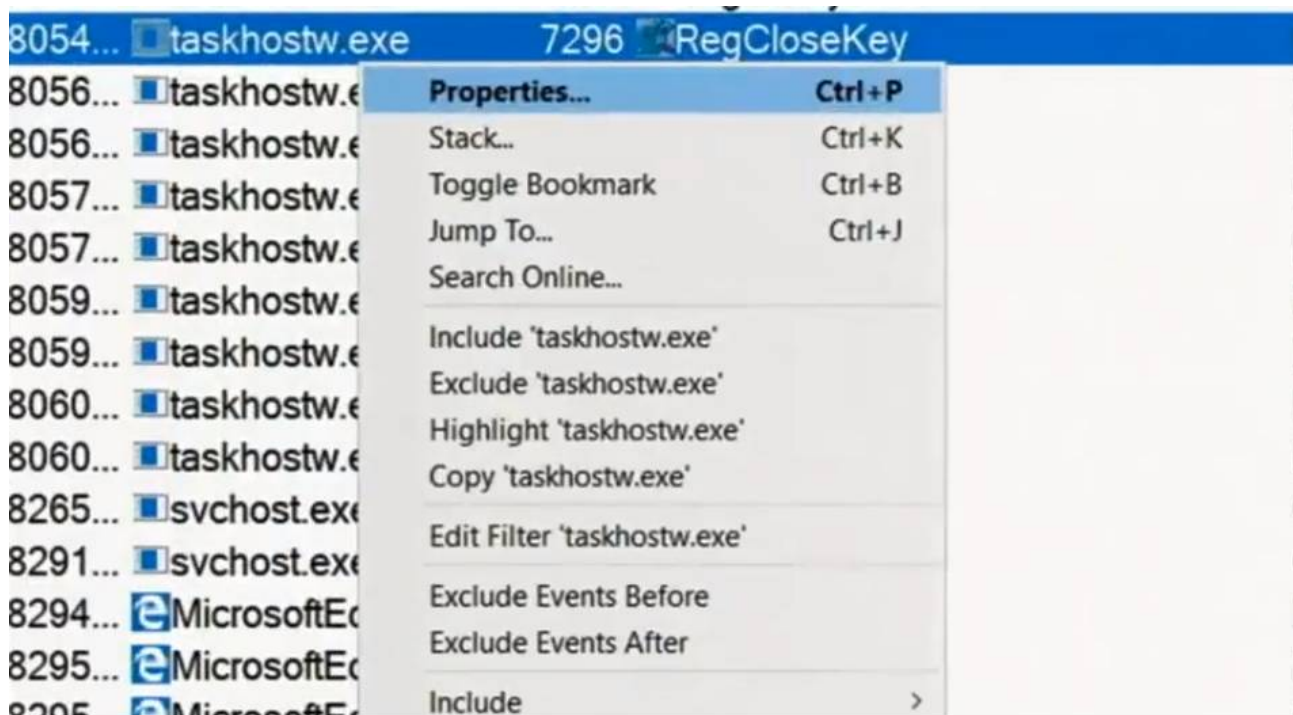


Seq...	Time of Day	Process Name	PID	Operation	Path	Result	Detail
207...	11:42:45.8370...	MicrosoftEdgeCP.exe	15...	RegCloseKey	HKCU\Software\Classes\Local Settings\Software\MI...	SUCCESS	
207...	11:42:45.9022...	svchost.exe	3320	TCP Send	mr-saw.ntdev.corp.microsoft.com:1195 -> 167.220.6...	SUCCESS	Length: 517, starttime: 47252334, endtim...
207...	11:42:45.9022...	svchost.exe	3320	TCP Receive	mr-saw.ntdev.corp.microsoft.com:1195 -> 167.220.6...	SUCCESS	Length: 389, seqnum: 0, connid: 0
207...	11:42:45.9023...	MicrosoftEdgeCP.exe	3596	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
207...	11:42:45.9024...	MicrosoftEdgeCP.exe	3596	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersi...	SUCCESS	Desired Access: Read
207...	11:42:45.9024...	MicrosoftEdgeCP.exe	3596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	Type: REG_SZ, Length: 108, Data: "C:\...
207...	11:42:45.9025...	MicrosoftEdgeCP.exe	3596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
207...	11:42:45.9025...	MicrosoftEdgeCP.exe	3596	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
207...	11:42:45.9025...	MicrosoftEdgeCP.exe	3596	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	
207...	11:42:45.9026...	MicrosoftEdgeCP.exe	3596	RegQueryKey	HKU	SUCCESS	Query: HandleTags, HandleTags: 0x0
207...	11:42:45.9026...	svchost.exe	2916	CreateFile	\\ntdev.corp.microsoft.com\sysvol\ntdev.corp.microso...	SUCCESS	Desired Access: Read Data/List Directory...
207...	11:42:45.9026...	svchost.exe	2916	CreateFile	\\ntdev.corp.microsoft.com\sysvol\ntdev.corp.microso...	SUCCESS	Desired Access: Read Data/List Directory...

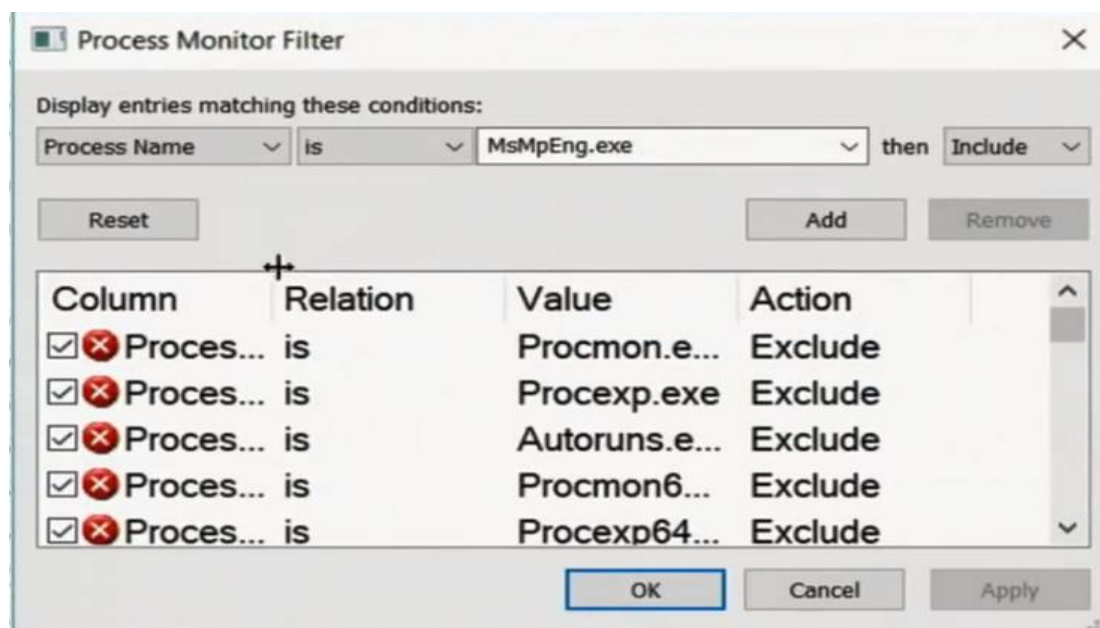
It is also possible to filter for relevant information by right clicking and selecting the options you need.



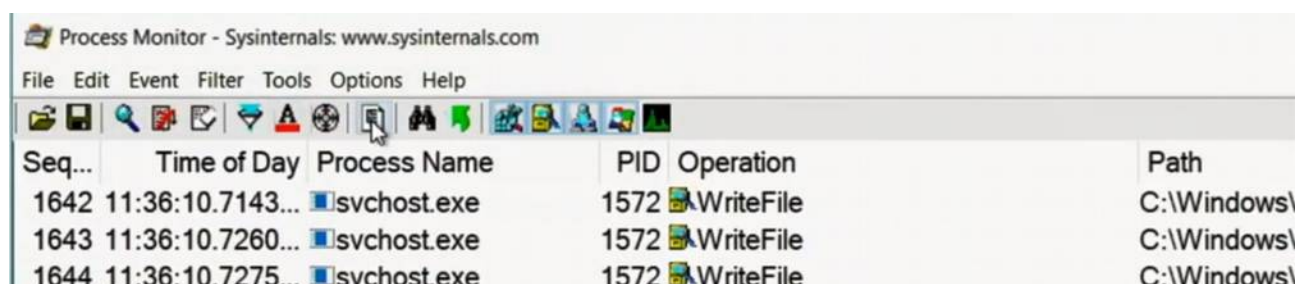
Seq...	Time of Day	Process Name	PID	Operation	Path	Result	Detail
7	11:36:09.8054...	taskhostw.exe	7296	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
8	11:36:09.8056...	taskhostw.exe		Properties...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
9	11:36:09.8056...	taskhostw.exe		Stack...	HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
10	11:36:09.8057...	taskhostw.exe		Toggle Bookmark	HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11	11:36:09.8057...	taskhostw.exe		Jump To...	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
12	11:36:09.8059...	taskhostw.exe		Search Online...	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
13	11:36:09.8059...	taskhostw.exe		Include 'taskhostw.exe'	HKLM\Software\Microsoft\Input	SUCCESS	Desired Access: Read
14	11:36:09.8060...	taskhostw.exe		Exclude 'taskhostw.exe'	HKLM\SOFTWARE\Microsoft\Input\EnableTestHook	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
15	11:36:09.8060...	taskhostw.exe		Highlight 'taskhostw.exe'	HKLM\SOFTWARE\Microsoft\Input	SUCCESS	
16	11:36:09.8265...	svchost.exe		Copy 'taskhostw.exe'	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,166,144, Length: 65,536
17	11:36:09.8291...	svchost.exe		Edit Filter 'taskhostw.exe'	C:\Windows\System32\winevt\Logs\Security.evtx	SUCCESS	Offset: 60,231,680, Length: 65,536
18	11:36:09.8294...	MicrosoftEc...		Exclude Events Before	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
19	11:36:09.8295...	MicrosoftEc...		Exclude Events After	HKLM\Software\Microsoft\Windows NT\CurrentVersi...	SUCCESS	Desired Access: Read
20	11:36:09.8295...	MicrosoftEc...		Include	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	SUCCESS	Type: REG_SZ, Length: 108, Data: "C:\...
21	11:36:09.8296...	MicrosoftEc...		Exclude	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144
22	11:36:09.8296...	MicrosoftEc...		Highlight	HKLM\SOFTWARE\Microsoft\Windows NT\Current...	NAME NOT...	Length: 144



You can also use a **own filter** to use the **Edit Filter** option.



If you searching for a **specific process** it is also possible to search it on the **process tree** and select them. To open the process tree click on the **note symbol** in the middle of the process monitor.

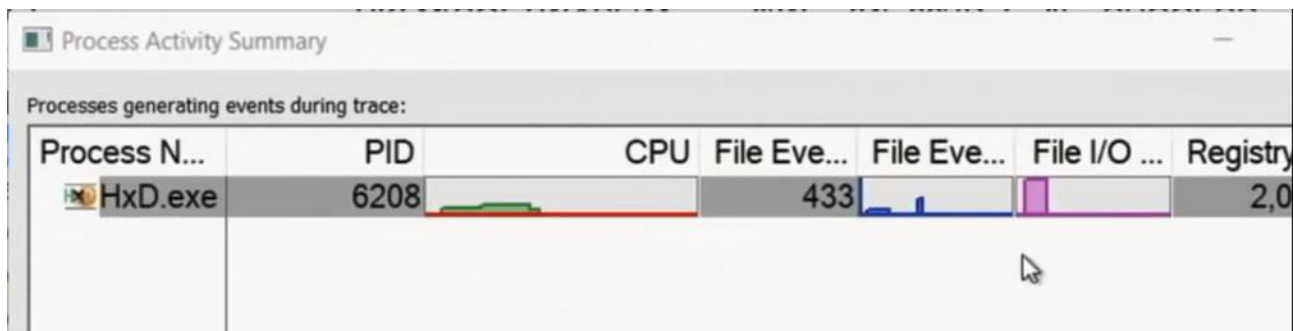


Process Tree		
<input type="checkbox"/> Only show processes still running at end of current trace <input checked="" type="checkbox"/> Timelines cover displayed events only		
Process	Descript...	Image Path
svchost.exe (1376)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (1384)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (1400)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (1408)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (1416)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (1424)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (1572)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (1708)	Host Pro...	c:\windows\system32\svchost.exe

MSOIDSVC.EXE (3292)	Microsoft...	C:\Program Files\Common Files\Microsoft S...
MSOIDSvc.exe (4000)	Microsoft...	C:\Program Files\Common Files\Microsoft S...
IpOverUsbSvc.exe (3308)	Windows...	C:\Program Files (x86)\Common Files\Micro...
svchost.exe (3320)	Host Pro...	c:\windows\system32\svchost.exe
svchost.exe (3348)	Host Pro...	c:\windows\system32\svchost.exe
OfficeClickToRun.exe (3380)	Microsoft...	C:\Program Files\Common Files\Microsoft S...
AppVShNotify.exe (17196)	AppVSh...	C:\Program Files\Common Files\Microsoft S...
sqlwriter.exe (3392)	SQL Ser...	C:\Program Files\Microsoft SQL Server\90\...
svchost.exe (3408)	Host Pro...	c:\windows\system32\svchost.exe
SecurityHealthService.exe (3428)	Windows...	C:\WINDOWS\system32\SecurityHealthSe...
TelemetryHost.exe (3428)	Telemetr...	C:\Program Files (x86)\Microsoft\Telemetry...

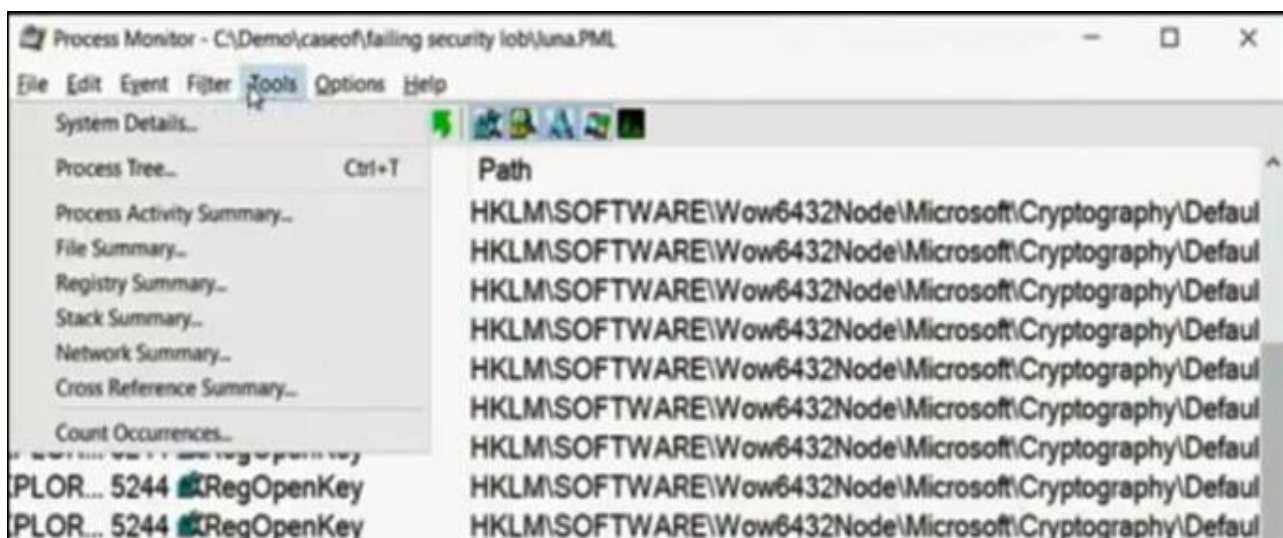
By filtering a specific process a advanced option of process monitor is also useful. So by clicking on the Tool register on the top you can use the different summary graphs of hardware and software activities e.g Process Activity Summary (CPU, File I/O etc) and after selecting you can jump to the specific line in the capturing trace.

Process Monitor - Sysinternals: www.sysinternals.com				
File Edit Event Filter Tools Options Help				
System Details...				
Process Tree... Ctrl+T				
Process Activity Summary...				
File Summary...				
Registry Summary...				
Stack Summary...				
Network Summary...				
Cross Reference Summary...				
Count Occurrences...				
Process Name	PID	Operation	Path	
svchost.exe	6208	QueryNameInformationFile	C:\Window	
svchost.exe	6208	CloseFile	C:\Window	
svchost.exe	6208	RegOpenKey	HKLM\Soft	
svchost.exe	6208	RegQueryValue	HKLM\SOI	
svchost.exe	6208	RegQueryValue	HKLM\SOI	
svchost.exe	6208	RegCloseKey	HKLM\SOI	
svchost.exe	6208	QueryEaFile	C:\Window	
45 11:42:30.4729... HxD.exe	6208	QueryStreamInformationFile	C:\Window	



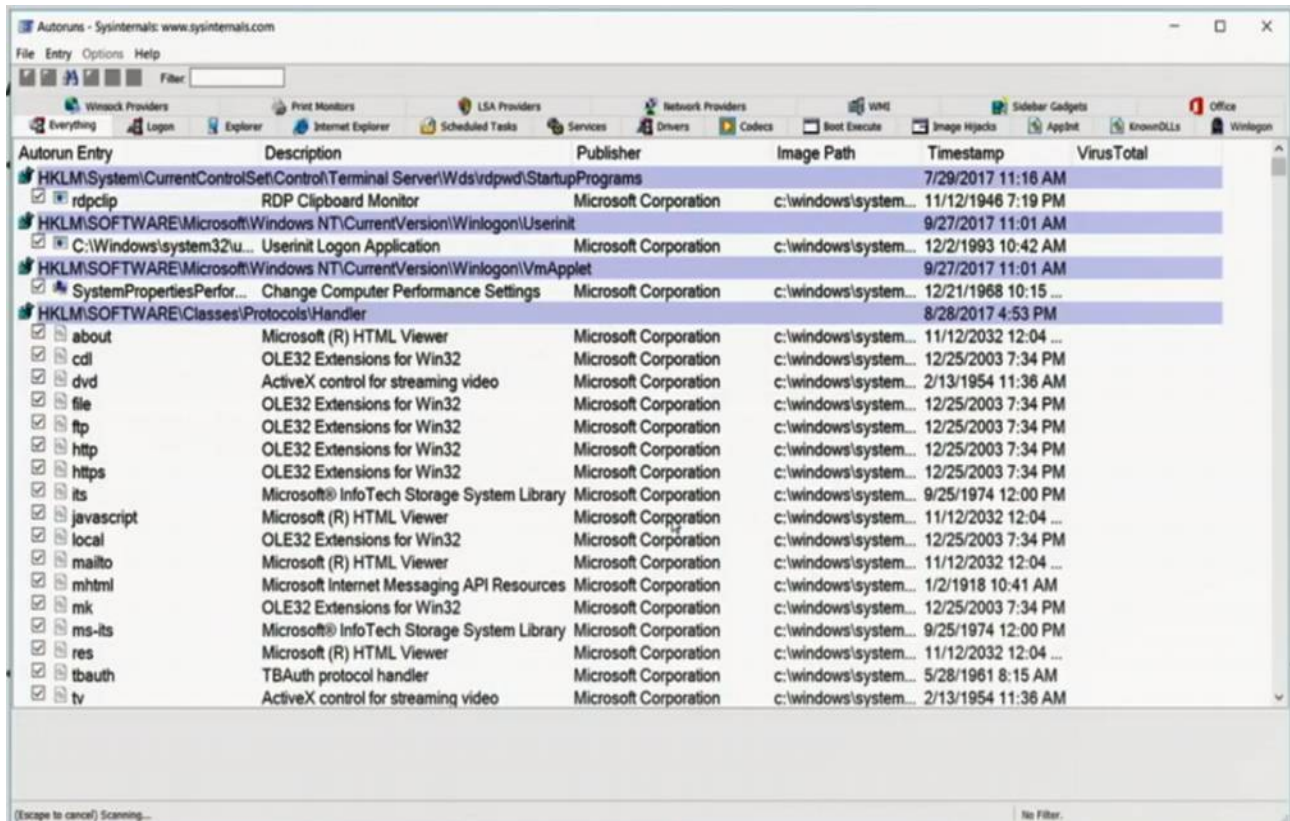
890	11:42:35.5455...	HxD.exe	6208	ReadFile	C:\Bin\HxD.ini	SUCCESS	Offset: 0, Length: 77,555, Priority: Normal
891	11:42:35.5460...	HxD.exe	6208	CloseFile	C:\Bin\HxD.ini	SUCCESS	
892	11:42:41.5737...	HxD.exe	6208	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
893	11:42:41.5737...	HxD.exe	6208	RegQueryKey	HKLM	SUCCESS	Query: Name

Another helpful option by filtering issues is to use the Count Occurrences in the Tool register. You can more specifically the Occurrences by selecting the drop-down-menu.



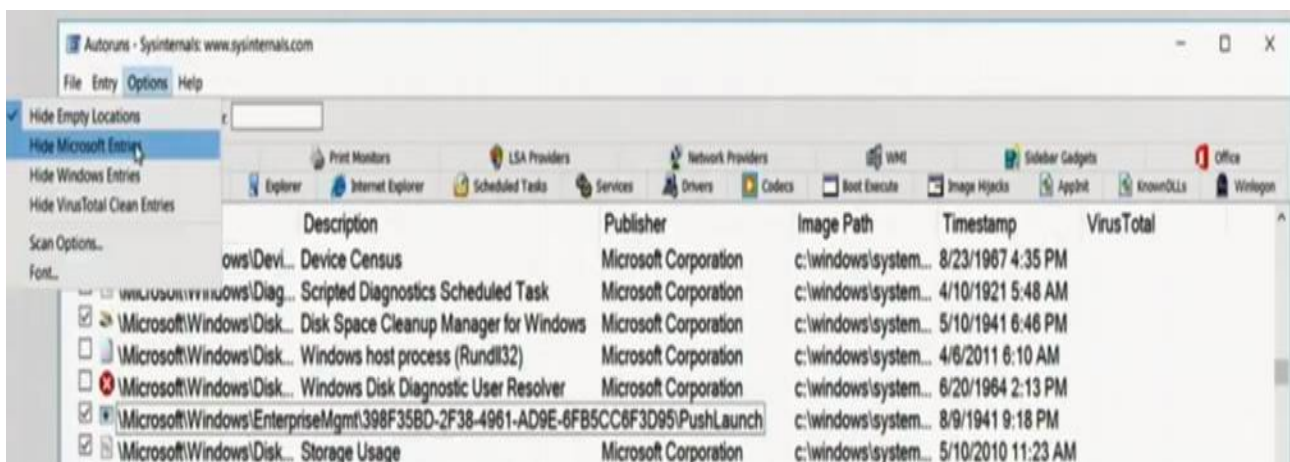
Using Autoruns for Troubleshooting

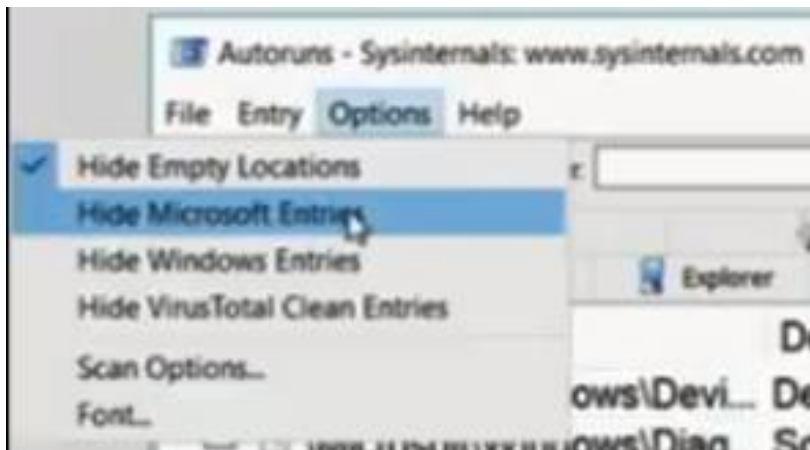
Autoruns also shows you detailed information about different system components e.g dll files, drivers, services, scheduled tasks, codecs, office plugins etc.



You can also use Autoruns to filter information or for malware scanning

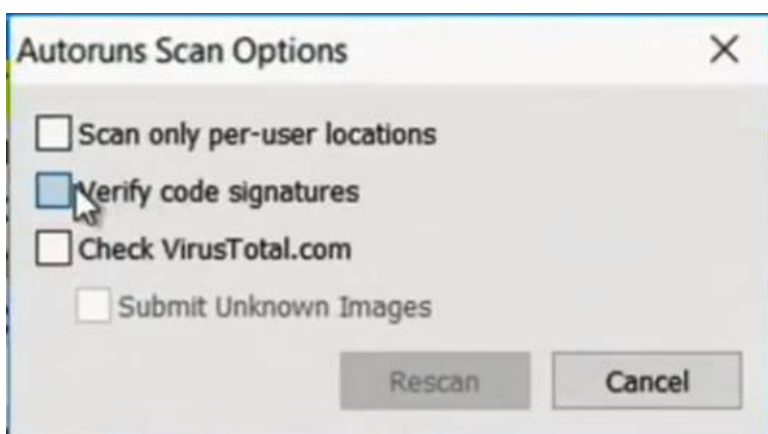
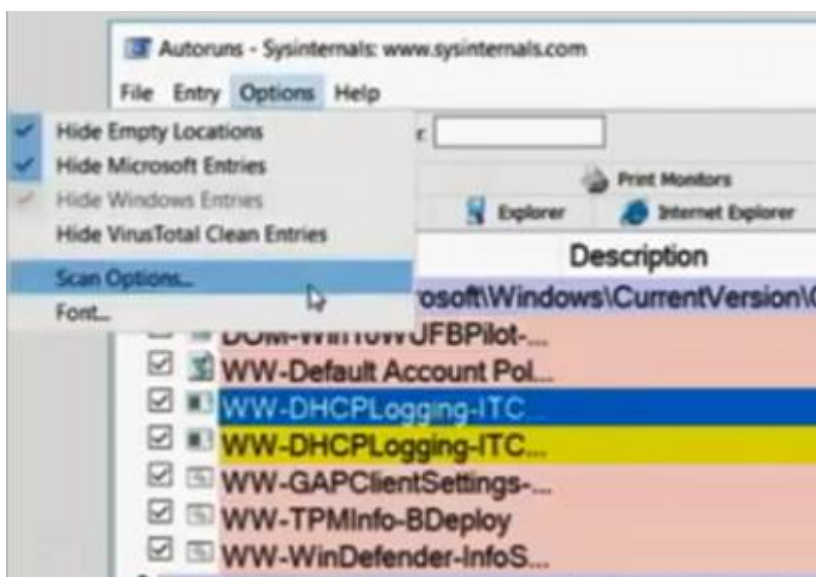
To filter information use the Options register at the top and turn on and off default filters or use a own filter option





To use the Autoruns for scanning malware use the Entry register at the top and use the Scan Options. Select the options you want.

Be careful with the Submit Unknown Images Option because this file information we be published in public and are not possible to delete so it could be a privacy incident !



Signatures can also be checked with the tool sigcheck

Quellen:

[Steve Whiting - Case of the Unexplained](#)

Tech-Days 2012 – Windows Debugging and Troubelshooting

[Windows Debugging and Troubleshooting - Invidious \(kavin.rocks\)](#)

[Case of the Unexplained Windows Troubleshooting with Mark Russinovich - 2017 - Invidious \(kavin.rocks\)](#)

<https://dumpanalysis.org>

<https://blogs.msdn.com/ntdebugging>