#### 01 - Objectives

• How to determine the root sources of having intensive disk usage/RAM/CPU and intensive networking using **Task Manager** (Processes, Performance, App history, Start-up, Users, Details, Services).

• Analyzing performance issues due to intensive disk use using **Windows Performance Recorder, Process Monitor** and **Process Explorer**.

• Monitor the disk activity, identify who is generating it and how to figure out the issue by looking at the pdbs and the code.

02 - I/O Monitoring – Windows

#### Introduction

• Since computers started to surface, for many people it was a mystery what was happening behind the screen and it seemed magical when it wasn't working and even more magical when it was working. Since Linux is open-source, all sorts of tools appeared over time to analyse problems when they came up. On Windows on the other hand, the system being closed made it harder for tools to appear.

• The first tools were provided by Sysinternals. These were written by Mike Rusinovich, who chose to make public tools such as "File monitor" and "Registry monitor", which were later combined into "Process monitor". The tools were so good that even Microsoft's support teams were using them. Seeing their usefulness and appreciating the know-how of their operating system, Microsoft decided to buy Sysinternals, so now the original website redirects to https://technet.microsoft.com/en-us/sysinternals (outside Romania it probably redirects to a different link due to localization reasons that consider the language of the country where redirection is made).

• On this website can be found some of the tools that will be used in this tutorial - Process Monitor, Process Explorer, VMMap, Autoruns. Starting with Windows 7, Microsoft has begun to invest more and more in the performance of the system and in ways to monitor the system's performance. Some tools already existed since Windows 2000, but they were only used internally.

## Task Manager

			А. Т	ask	Mai	nager - Processes tab
Processes						
tab shows	sig Task Manager File Options View					- • ×
all the	Processes Performance App history Sta	rt up Users	Details Ser	vices		
running	Name	4% CPU	46% Memory	0% Disk	0% Network	
running	Windows Driver Foundation - U	0%	1.5 MB	0 MB/s	0 Mbps	
processes	Windows host process (Rundll3	0%	0.3 MB	0 MB/s	0 Mbps	
and thair	Windows IP Over USB PC Servic	0%	0.9 MB	0 MB/s	0 Mbps	
	<ul> <li>Windows Shell Experience Host</li> </ul>	0%	55.3 MB	0 MB/s	0 Mbps	
current	Windows Wireless LAN 802.11 E	0%	1.1 MB	0 MB/s	0 Mbps	
• • • • • • • • • • • • • • • • • • • •	winnttp.exe (32 bit)	025	1.5 MB	U.T Mb/s	1.5 Mops	
resource	Windows processes (31)					
usaga in	> 💽 appmodel (2)	0%	5.7 MB	0 MB/s	0 Mbps	
usage m	Client Server Runtime Process	0.1%	1.1 MB	0 MB/s	0 Mbps	
terms of	Client Server Runtime Process	0%	0.6 MB	0 MB/s	0 Mbps	
CDLL	Console Window Host	0%	4.5 MB	0 MB/s	0 Mops	
CPU,	Console Window Host	0%	1.1 MB	0 MB/s	0 Mbps	
Memory.	Desktop Window Manager	0.2%	84.4 MB	0 MB/s	0 Mbps	
Disk and	Fewer details					End task
Network.						

# Shows the process name responsible for constant disk thrashing either by reads or writes. To start Task manager use the shortcut: Ctrl + Shift + Esc.

**B.** Task Manager - Performance tab



## C. Task Manager - App history tab

at start-up,

(or at least

Microsoft's vision - this will be

further

in

🚳 NVIDIA Update Backend

Waves MaxAudio Service A...

🔈 Realtek HD Audio Manager

Skype (2)

• Fewer details

Update.exe (9)

The <b>App</b>					
history					
ah was first					
idded to					
Windows 8,					
and it shows					
the resource	ile Options View				
consumption	Processes Performance App hist	PTY Start up Users Det	ails Services		
consumption	Resource usage since 10/27/2016 fo Delete usage history	or current user account.			
of metro	Name	CPU time	Network	Metered network	Tile updates
applications.	3D Builder	0:00:00	0 MB	0 MB	0 MB
Motro	Alarms & Clock	0:00:02	0 MB	0 MB	0 MB
vietro	Calculator	0:00:43	0 MB	0 MB	0 MB
applications	Camera	0:00:00	0 MB	0 MB	0 MB
are touch-	Connect	0:00:00	0 MB	0 MB	0 MB
	Cortana	0:03:28	3.4 MB	0 MB	0 MB
screen-	Duolingo	0:00:00	0 MB	0 MB	о мв
friendly	Eclipse Manager	0:00:00	0 MB	0 MB	0 MB
	Feedback Hub	0:00:00	0 MB	0 MB	0 MB
applications	Fresh Paint	0:00:00	0 MB	0 MB	0 MB
vritten	Fewer details			0.1.0	
especially	and the second state of th				
for					
IOL					
Microsoft's					
WinRT					
·· · · · · · · · · · · · · · · · · · ·					
programmin					
g interfaces.					
	~				
D. Task Mana	ager - Star	t-up tal	)		
The <b>Start</b> -					
	Task Manager				
	cesses Performance App history	Start-up Users Details	Services		
tab shows					
all the		Dublicher	Clabar	Chart up in-	
	8 Bluetooth Tray Application (2)	Broadcom Corporation.	Enabled	Low	
application	Sisco AnyConnect User Inte	Cisco Systems, Inc.	Enabled	High	
s that start	N Dell System Detect	Dell	Enabled	Not measured	
A start	DPM Client (2)     HD Audio Background Proc	Microsoft Corporation	Enabled	Medium	

Enabled

Enabled

Enabled

Enabled

Enabled

NVIDIA Corporation

Realtek Semiconductor

Skype Technologies S.A.

s Audio Ltd

w

Low Low High High Low

detailed in	
the	
Autoruns	
section),	
and their	
impact on	
the boot	
time. It is	
helpful to	
check this	
tab in case	
your	
computer	
takes a long	
to to start	
up.	

# E. Task Manager - Users tab



to add or
remove
columns
In the
screenshot
presented
below the
following
columns
were
added
Handles
Threads
Image Dath
Name and
Command
Line
These now
a alumna
are very
userul: the
III'st one
(Handles)
when
investigati
ng a
handle
leak, the
second one
(Threads)
in the case
of
investigati
ng
processes
that create
too many
threads,
the third
one (Image
Path
Name) to
find out
the path
from
where the
process
was
started,
and the last
one
(Commond

Line) to	
find out	
the	
parameters	
with which	
it was	
started.	

#### G. Task Manager - Services tab

	Real Task Manager File Options View				-	×
	Processes Performance	App history Start up Users Details Services				
	Name PID	Description	Status	Group		^
	Service	Te.Service	Stopped			
Services tab shows the service	SStandardC	Visual Studio Standard Collector Service	Stopped			
	SipOverUsbSvc 4496	Windows Phone IP over USB Transport (IpOverUsbSvc)	Running			
status A Windows comises con	WSearch 9424	Windows Search	Running			
status. A windows service can	WMPNetwor	Windows Media Player Network Sharing Service WMI Reformance Adaptor	Stopped			
	WinDefend	Windows Defender Senice	Stopped			
be considered similar to a Linux	WdNisSvc	Windows Defender Network Inspection Service	Stopped			
oe considered similar to a Emax	wbengine	Block Level Backup Engine Service	Stopped			
1	WavesSysSvc 3148	Waves Audio Services	Running			
daemon: a process without a	Szvss	Volume Shadow Copy	Stopped			
I I I I I I I I I I I I I I I I I I I	SVsEtwService	Visual Studio ETW Event Collection Service	Stopped			
visual interface offering	Sypnagent 2124	Cisco AnyConnect Secure Mobility Agent	Running			
visual interface, offering	Syds	Virtual Disk	Stopped			
· · · · · · · · · · · · · · · · · · ·	VaultSvc 716	Credential Manager	Running			
services to user-created	UlloDetect	Interactive Services Detection	Stopped			
services to user created	CevAgentSer	User Experience Virtualization Service	Stopped			
processo	TieringEngin	Storane Tiers Management	Stopped			
processes.	S. Thunderbolt	Thunderbolt(TM) Service	Stopped			
L	Stereo Service 1528	NVIDIA Stereoscopic 3D Driver Service	Running			
	SQLWriter 7620	SQL Server VSS Writer	Running			
	SQLBrowser	SQL Server Browser	Stopped			
	Sppsvc	Software Protection	Stopped			

#### **Conclusion:**

Task Manager can be used to identify which process uses a lot of RAM, CPU, accesses the disk many times or generates a lot of traffic on the network at a certain moment (Services tab). However, it does not offer information if in the long run, that same process is the one that generated the slowdown of the system. It does offer some information for longer periods of time, in the Startup tab, which shows what process had higher impact at start-up, but does not specify the area that was impacted (disk space, RAM, CPU).

You can sort by I/O read or I/O Writes, but no option to sort the results by Total I/O (combined Read & Write).

To overcome Task manager's limitation, and to perform a thorough analysis, use the excellent Resource Monitor (Resmon) utility, which is built-in to Windows.

#### Windows Performance Recorder

Installing Windows ADK will install Windows Performance Recorder. Check by clicking the windows button and typing "windows performance recorder".

Wi	indows Performance Recorder				
	windows Performance Recorder		-		×
Start Windows Performance	Record system information This tool will gather information about the interaction of the program computer for analysis.	ns and hardware runr	ning on	🕜	
You will see the following:	Status: Recording not started	Time: Buffer: Events dropped:			
	✓ More options	Start	C	ancel	[

	1	
	Windows Performance Recorder	
	Record system information	0
	This tool will gather information about the interaction of the progr computer for analysis.	ams and hardware running on this
	Status: Recording not started	Time: Buffer: Events dropped:
Click the More options button	Hide options	Start Cancel
b get the list shown in the	Select additional profiles for performance recording:	Performance scenario:
creenshot right below.	Resource Analysis	General ~
	CPU usage	Detail level:
	File I/O activity	Verbose $\checkmark$
	Registry I/O activity	Logging mode:
	Networking I/O activity	Memory ~
	<ul> <li>✓ Heap usage</li> <li>✓ Pool usage</li> <li>✓ VirtualAlloc usage</li> <li>☐ Power usage</li> <li>☐ GPU activity</li> </ul>	To insert an annotated marker, press CTRL + WIN + x during trace capture.
	Add Profiles	About

# Datafile: Logs.exe and GoodLog.exe

Make sure that you select the same check boxes as in the screenshot, but do not click start just yet. Create a new directory and copy

the **Logs.exe** and **GoodLo g.exe** files into this directory. The behaviour of these two executables is similar to logging applications that write logs to the disk. Open a terminal and change the path to the directory where you copied the files.



## Windows Performance Recorder

Start Windows Performance Recorder and right after run GoodLog.exe and then Logs.exe. Once the two applications finish running, click the Save button in Windows Performance Recorder.

Command Prompt	Windows Performance Recorder	
Microsoft Windows [Version 10.0.143 (c) 2016 Microsoft Corporation. All	Gathering system information for General Trace	
C:\Users\mmurgan>d:		
D:\>cd Logs	File Name: C:\Users\mmurgan\Documents\WPR Files\MMURGa	AN-L1
D:\Logs>Logs.exe	mylogs	
D:\Logs>GoodLog.exe		
D:\Logs>		
	This recording may contain personally identifiable or security necessarily limited to paths to files accessed, paths to registry depends on the events that were logged. Please be aware of th people.	relate acces: is wh
	This recording may contain personally identifiable or security necessarily limited to paths to files accessed, paths to registry depends on the events that were logged. Please be aware of th people.	relate acces is wh

Windows Performance Analyzer



The graph looks interesting.						
Processes						
can be						
selected for						
observing	Ng Task Manager			di Mari		- C × BbCcDe AaBbCc
	File Options View					Command Prompt Logs are
their	Processes Performance App history Sta	rt up Users 37%	Details Ser	akes 3%	0%	Microsoft Windows (Version 18.0.14393) (c) 2016 Microsoft Corporation. All rights reserved.
activity on	Name HD Audio Background Process	0%	0.4 MB	0 MB/s	0 Mbps	C:\USers\mmungerod: D:\>cd Logs
the distribute	HD Audio Background Process	0%	0.6 MB	0 MB/s	0 Mbps	D:\Logs>Logs.exe
the disk. It	Flost Process for Windows Tasks	0%	2.6 MB	0 MB/s	0 Mbps	D:\Logs>GoodLog.exe
1	📕 Host Process for Windows Tasks	0%	D.5 MB	0 MB/s	0 Mbps	D:\Logs>Logs.exe
can be	🗧 🇵 ightCU/Service Madule	07Xa	0.3 MB	0 MB/s	0 Mbps	D:\Logs>Logs.exe
mational that	🔳 InstallAgent	0%	0.2 MB	O MB/s	0 Mbps	D:\Logs>Logs.exe
noticed that	InstallAgentUserBroker	0%	0.2 MB	0 MB/s	0 Mbps	
	<ul> <li>Intel(R) Dynamic Application Lo.</li> <li>Total 20 Dynamic Stations and Total</li> </ul>	0%	0.4 MB	0 MB/s	0 Mbps	
our	<ul> <li>Intel(i) Oynamic Platform and L.</li> <li>Intel(i) Oynamic Platform and I.</li> </ul>	0%	0.2 MB	0 MB/s	D Mbrs	
	Intel(R) Local Management Serv	0%	2.6 MB	O MR/s	0 Mbps	
processes	> 🔝 Intel(R) Security Assist (32 bit)	0%	2.0 MB	0 MB/s	0 Mbps	
- 	IntelCpHeciSvc Executable (32 b	0%	0.4 MB	0 MB/s	0 Mbps	
are not	🐨 Logs.exe (32 bit)	15.2%	0.5 MB	0.5 MB/s	0 Mbps	
shown. Run	· Fewer getails					End task
Logs.exe						
again while						
uguin white						
keeping						
Task						
M						
Manager						
on.						
~						

## **Conclusions:**

• This shows that there is activity on the disk. The question is why doesn't Windows Performance Analyzer show it. The way Windows Performance Recorder records activity is based on events generated by the Windows kernel. It registers to track the events, listens to them, and during the recording period it constantly samples which process uses which resource at the time of sampling.

• It sums up the number of time that a process was caught doing something. In our case, the two processes want to write to the disk, but they are not the ones that get to do the actual writing. They tell the system that they want to write, and the System process schedules the writing. The reason for this is targeting a more efficient disk writing, as the System process is trying to minimise the impact to the disk. This is why our process's writing is passed over to the System process.

## **Process Monitor**

Process Monitor is an excellent troubleshooting tool from Windows Sysinternals that displays the files and registry keys that applications access in real-time. The results can be saved to a log file, which you can send it to an expert for analyzing a problem and troubleshooting it.

How to Use Process Monitor to Track Registry and File System Changes?

#### Step 1: Running Process Monitor & Configuring Filters

1. Download Process Monitor from Windows Sysinternals site.

**2.** Extract the zip file contents to a folder of your choice.

**3.** Run the Process Monitor application.

**4.** Include the processes that you want to track the activity on. For this example, you want to include Notepad.exe in the (Include) Filters.

**5.** Click Add, and click OK.

6. From the Options menu, click Select Columns.

7. Under "Event Details", enable Sequence Number, and click OK.

You can add multiple entries as well, in case if you want to track few more processes along with Notepad.exe. To keep this example simpler, let's only track Notepad.exe. (You'll now see the Process Monitor main window tracking the list of registry and file accesses by processes real-time, as and whey they occur.)

# **Step 2: Capturing Events**

**8.** Open Notepad.

**9.** Switch to Process Monitor window.

**10.** Enable the "Capture" mode (if it's not already ON). You can see the status of the "Capture" mode via the Process Monitor toolbar.

**11.** The highlighted button above is the "Capture" button, which is current disabled. You need to click that button (or use Ctrl + E key sequence) to enable capturing of events.

12. Cleanup the existing events list using Ctrl + X key sequence (Important) and start afresh.

**13.** Now switch to Notepad and try to reproduce the problem.

**14.** To reproduce the problem (for this example), try writing to HOSTS file

(C:\Windows\System32\Drivers\Etc\HOSTS) and saving it. Windows offers to save the file (by showing the Save As dialog) with a different name, or in a different location. So, what happens under the hood when you save to HOSTS file? Process Monitor shows that exactly.

**15.** Switch to Process Monitor window, and turn off Capturing (Ctrl + E) as soon as you reproduce the problem. Important Note: Don't take much time to reproduce the problem after enabling capturing. Similarly turn off capturing as soon as you finish reproducing the problem. This is to prevent Process Monitor from recording other unneeded data (which makes analysis part more difficult). You need to do all that as quickly as you can.

The log file above tells us that Notepad encountered an ACCESS DENIED error when writing to the HOSTS file. The solution would be to simply run Notepad elevated (right-click and choose "Run as Administrator") to be able to write to HOSTS file successfully.

## **Step 3: Saving the Output**

16. In the Process Monitor window, select the File menu and click Save.

**17.** Select Native Process Monitor Format (PML), mention the output file name and Path, save the file.

**18.** Right-click on the Logfile.PML file, click Send To, and choose Compressed (zipped) folder. This compresses the file by ~90%. Look at the graphic below. You certainly want to zip the log file before sending it to someone.

04 - Exercises

## Exercise 01. [30p] Task Manager, Windows Performance Recorder and Process Monitor

• Go through the tutorials: Task Manager, Windows Performance Recorder and Process Monitor. Discuss the output and call the assistant to show him/her your progress.

# Exercise 02. [10p] Task Manager

• Which program is constantly reading or writing to your hard disk?

# How to:

- Open Task Manager, and select the Details tab.
- Right-click on the column header (Name, PID, Status etc) and click Select Columns.
- Enable the following checkboxes and click OK.

I/O read bytes is the number of bytes read in input/output operations generated by a process, including file, network, and device I/Os. Whereas I/O write bytes is the number of bytes written in input/output operations by a process, including file, network, and device I/Os. I/O Read Bytes & I/O Write Bytes directed to CONSOLE (console input object) handles are not counted.

• Next, sort the listings by I/O Read bytes and see which application is generating the maximum I/O (in bytes/sec). Similarly, sort by I/O Write bytes to see which program is writing to the hard disk continuously.

• Once you identify the program, decide if you need the program or not. Leave it as it is if the I/O operations are justified. Else, remove the program or consult its documentation to tweak the settings if any. For instance, one of your browser extensions may cause high disk or CPU usage. You need to isolate the extension, add-on or the browser's feature causing the trouble.

Exercise 03. [30p] Process Monitor

Download the archive logs-final.7z and check if you have "Process Monitor" installed (Windows 10).

logs-final.7z: parola HandleLeak.7z: parola7 Task.7z: parola17 [10p] Task A - Checking logging file

	File Edit Event Filter	Tools Options Help			
	🗃 🖬 🕴 🔍 🎯 🖾	🗢 🔺 😨   🗉	🔺 📕 📓 🖓 🖓 🖊		
	Time Process Name	PID Operation	Path	Result Detail	
by	3:23:0 I dvm.exe 3:23:0 I dvm.exe 3:23:0 I dvm.exe 3:23:0 I dvm.exe 3:23:0 Gvm.exe 3:23:0 Searchindexer 3:23:0 Searchindexer 3:23:0 Searchindexer 3:23:0 Explorer EXE 3:23:0 Explorer EXE	5680 ReadFile 5680 RegQueryValu 5680 RegQueryValu 5680 RegQueryValu 5680 RegQueryValu 5680 RegQueryValu 9424 FileSystemCont 9424 RegQueryValu 9556 ReadFile 9556 ReadFile	C:\Windows'System32'dwm.exe HKCU\SOFTWARE\Microsoft\Window. HKCU\SOFTWARE\Microsoft\Window. HKCU\SOFTWARE\Microsoft\Window. IKCU\SOFTWARE\Microsoft\Window. IKCI\SOFTWARE\Microsoft\Window. C:\Windows'sxplorer.exe C:\Windows'sxplorer.exe C:\Windows'sxplorer.exe	SUCCESS Offee: 35.328. Len., SUCCESS Type: REG_DWO., SUCCESS Type: REG_DWO., SUCCESS Type: REG_DWO., SUCCESS Type: REG_DWO., SUCCESS Corticl: FSCT., R., SUCCESS Corticl: FSCT., R., SUCCESS Offee: 2089.84, SUCCESS Offee: 2089.84, SUCCESS Offee: 2089.84,	
	3:23:0 Explorer EXE	9656 KRegQueryKey	HKCU\Software\Classes	SUCCESS Query: Name	
	3:23:0 Replorer EXE	9656 RegQueryKey	HKCU/Software/Classes	SUCCESS Query: Handle Tag	
•	3:23:0 Explorer EXE	9656 RegQueryKey	HKCU/Software/Classes HKCU/Software/Classes/Applications/	NAME NOT FOUND Desired Access: B	
ntlv	3:23:0 Explorer.EXE	9656 RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND Desired Access: R	
nuy	3:23:0 Fxplorer.EXE	9656 KRegQueryKey	HKCU\Software\Classes	SUCCESS Query: Name	
bod	3:23:0 Explorer.EXE	9656 RegQueryKey	HKCU/Software/Classes	SUCCESS Query: Handle Tag SUCCESS Query: Name	
eu	3:23:0 Explorer.EXE	9656 RegOpenKey	HKCU/Software/Classes/Applications/.	NAME NOT FOUND Desired Access: R	
	3.23.0 Explorer.EXE	9656 RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND Desired Access: R	
288	2230.         ••• Explorer EXE           2231.         ••• Explorer EXE           2232.         ••• Explorer EXE           224.         ••• Explorer EXE           224.         ••• Explorer EXE	9656 A.CreateFile 9556 A.CoseFile 9556 A.CoseFile 9556 RegOpenKey 9556 RegOpen	C:\Leen'rmurgan\kep1bat.\Leen'Te. C:\Leen'rmurgan\kep1bat.\Leen'Te. C:\Leen'rmurgan\kep1bat.\Leen'Te. HKIM MSOFTWARE\Mcroseft'Window: HKUN SOFTWARE\Mcroseft'Window: HKCU SOFTWARE\Mcroseft'Window:	SUCCESS Desired Access R. SUCCESS Creation Time: 11/1. SUCCESS Oury: Honde Tig. SUCCESS Description of the Success O. SUCCESS Type: REG_DWO SUCCESS Deserved Access O. SUCCESS Ouery: Hande Tig. SUCCESS Deserved Access O. SUCCESS Ouery: Hande Tig. SUCCESS Ouery: Hande Tig. SUCCESS Deserved Access O. NAME NOT FOUND Desired Access O. NAME NOT FOUND Desired Access O. SUCCESS Type: REG_DWO. SUCCESS Type: REG_DWO.	
; 55	Artesis Venter Systematicular several      Ale last faint fa	1973 J. 60 S Filip D A S S S S S S S S S S S S S S S S S S	Tex.k         Deal           50:0221         Offer X33 (an.           60:0221         Offer X33 (an.           0:0000         Offer X33 (an.		- <i>e</i> ×

Looking at the logs created by the two apps - bad.log, good.log - they are identical, but Logs.exe has a significantly longer running time compared to GoodLog.exe. Start Process Monitor.

If the 4 buttons in the black area on the upper part of the window are selected, Proces Monitor will display the activity (in this order) for: registry, files, networking, process and thread activity. By unchecking them, the corresponding events will be no longer displayed. In the menu bar there is the Filter field. If selected, it will trigger a dropdown menu that contains another Filterfield. If this second Filter field is selected, it will open the window shown below. Replicate this on your computer.



From the two dropdown menus in the upper part of the context window, select "Process Name" instead of "Architecture" and "is" instead of "contains". In the text filed add Logs.exe, click the Add button and then the OKbutton. Open the terminal and run Logs.exe. After the program is done running, save the Process Monitor capture. Use Ctrl + Xto reset all the events captured in Process Monitor. Go to Filter  $\rightarrow$  Filter area, doubleclick on the filter that was just added and change Logs.exe with GoodLog.exe, then click Add and Ok. Start GoodLog.exe and save the capture once the program finishes running. Scroll down in the two capture-logs until you notice the activity for bad.log respectively good.log.

Edit Event Filter Tools Options Help				File Edit Event Filter Tools Options Help						
N 10 LY		-2 m				10 A A A				
Good on eve	12732 Queryliametria. D \Loos\GoodLog eve	SUCCESS	Neme: V.ocs.V	3383 Eloners	8428 A Dem Name Info	SUCCESS	Name: Vices/Loos			
GoodLog see	12732 CreateRe D\Loos\cood.log	SUCCESS	Desired Acces	3-38-3. 1 Loos eue	8428 CreateFile D'Llogs had log	SUCCESS	Desired Access G			
GoodLog.exe	12732 QueryStandardl D. Logs good log	SUCCESS	AllocationSize:	3.38.3 Logs.exe	8428 QueryStandardl D \Logs\badlog	SUCCESS	Allocation Size: 0. E			
GoodLog exe	12732 QueryStandardI. D.\Logs\good log	SUCCESS	AllocationSize:	3.38.3 TLogs.exe	8428 Query Standardl D. \Logs\bad log	SUCCESS	Allocation Size: 0, E			
GoodLog.exe	12732 AQueryStandardID.\Logs\good.log	SUCCESS	Allocation Size :	3.38.3. TLogs.ess	8428 AueryStandardl. D \Loge\bad log	SUCCESS	AllocationSize: 0, E			
GoodLog exe	12/32 www.ene U/Logs/good.log	SUCCESS	Cmaet: 0, Long	3.38:3. Logs.exe	8428 WiteFie D'Logs'badlog	SUCCESS	Offset: 0, Length; 2			
GoodLog.exe	12732 Adder File Dill and and for	SUCCESS	Mucation Size:	3.38.3. Logs.exe	sezs shubsere D'Logs'badlog	SUCCESS	0			
GoodLog exe	12732 QueryStandardl., D.\Logs\dood.log	SUCCESS	AllocationSine	3.383 Elaca ere	8428 Query Standardi, D \  con\/hod ton	SUCCESS	MonationSize: 24			
GoodLog.exe	12732 WitteRie D\Loge\good.log	SUCCESS	Offset: 8.552.1	3.38.3 E Loos eve	8428 ReadFile D\Logs\badlog	SUCCESS	Offset: 20 Length:			
GoodLog.exe	12732 AQueryStandardl D \Logs\good log	SUCCESS	AllocationSize:	3383 ELogs ese	8428 QueryStandardlD. \Logs\badlog	SUCCESS	AllocationSize: 24,			
GoodLog.exe	12732 WitteRie D.\Logs\good.log	SUCCESS	Offset: 12,827.	3:38:3 🛎 Logs.exe	8428 QueryStandardl D. \Logs'bad log	SUCCESS	AllocationSize: 24,			
GoodLog.exe	12732 AQueryStandardlD \Logs\good.log	SUCCESS	AllocationSize:	3.38.3. TLogs.ese	8428 WiteFie D \Logs'badlog	SUCCESS	Offset: 21, Length			
soodlog eee	12732 www.energie.co.u.v.logs/good.log	SUCCESS	Umaer: 17,101.	2.30.3. • Logs.exe	8428 ACloseFile D:\Logs\badlog	SUCCESS	D			
Good on me	12232 WiteFie D\logs\andler	SUCCESS	Offset: 21.325	1383 Logs ese	8428 A Dian Standard D Logs badlog	SUCCESS	Allocation Size 48			
GoodLog.exe	12732 QueryStandardI., D.\Logs\good.log	SUCCESS	AlocationSize	3383 Floorer	8428 ReadFite D \Loop/hadley	SUCCESS	Offset 41 Length			
GoodLog exe	12732 WitteRie D.\Logs\good.log	SUCCESS	Offset: 25,646	3.38-3 Logs eve	8428 QueryStandardl., D.\Logs\bad.log	SUCCESS	Allocation Size: 48.			
GoodLog.exe	12732 AueryStandardlD.\Logs\good log	SUCCESS	AllocationSize:	3.38.3. TLogs.ese	8428 QueryStandardl D \Logs\bad log	SUCCESS	Allocation Size: 43,			
GoodLog.exe	12732 WitteRie D.\Logs\good.log	SUCCESS	Offset: 29,912	3.38.3 Logs.exe	8428 WiteFie D:\Logs\badlog	SUCCESS	Offset: 42. Length:			
GoodLog.exe	12732 KGueyStandardI. D \Logs\good log	SUCCESS	AllocationSize:	3.38.3 Logs.exe	8428 ACloseFile D \Logs\badlog	SUCCESS	-			
Good on me	12712 A unit Renderfl D'Unaniacodian	SUCCESS	Offset: 34,179	3.38.3 Logs.exe	0420 CreateFile D'Logs/badlog	SUCCESS	Liesired Access: G.			
Good on eve	12222 With File D Lloss acord loss	SUCCESS	Offent: 38.445	3.36.3. Logs.ete	0/20 Device Diversion	SULLESS	relocation size: 64, Offerst: 62, Length:			
GoodLog exe	12732 QueryStandardl. D \Loos \pood log	SUCCESS	AllocationSize:	3.38.3 T Loon con	8428 A Duere Standardi D \Loop bad loo	SUCCESS	Allocation Szer 64			
GoodLog mes	12732 WitteRie D \Logs\good log	SUCCESS	Offset: 42,712	3.38.3. Logs.exe	8428 QueryStandardl D \Logs\bad log	SUCCESS	AllocationSize: 64			
GoodLog.exe	12732 KGueryStandardID.\Logs\good.log	SUCCESS	AllocationSize:	3.38.3 TLogs.ese	8428 WiteFie D.\Logs'badlog	SUCCESS	Offset: 63, Length:			
GoodLog.exe	12732 WitteRie D.\Logs\good.log	SUCCESS	Offset: 46,979.	3.38.3. E Logs.exe	8428 CloseFile D.\Logs\badlog	SUCCESS				
GoodLog.exe	12732 AQueryStandardlD \Logs\good.log	SUCCESS	AllocationSize:	3.38.3. TLogs.ese	8428 CreateRie D.\Logs\badlog	SUCCESS	Desired Access: G.			
Good og exe	12732 Numerice U. Loga good log	SUCCESS	Umser: 51,245.	3.30.3. Logs.exe	8428 Thursdard D \Logs bad log	SUCCESS	AllocationSize: 88,			
Good on me	12712 Wite Ele Di Jost Jood los	SUCCESS	Peocetion addit	3.3e.3. Logs ele	exce preserves UnLogs/badleg	SUCCESS	unset: 53, Length:			
GoodLog eve	12732 QueryStendardi, D.\Logs\stood log	SUCCESS	AlocationSize	3.38.3 Logs.exe	8228 A Cover Standard D \Log8 843.00	SUCCESS	Monation Sar 10			
GoodLog exe	12732 WiteRie D \Logs\good log	SUCCESS	Offset: 59.779	1383 Loos ere	8428 WiteFie D'Loss'badlog	SUCCESS	Offset: 84 Length:			
GoodLog.exe	12732 QueryStandardl D \Logs\good log	SUCCESS	AllocationSize:	3.38.3. Logs ese	8428 CloseFile D \Logs\badlog	SUCCESS	and the second second			
GoodLog min	12732 WitteFile D.\Logs\good.log	SUCCESS	Offset: 64,046.	3.38.3 TLogs.exe	8428 CreateFie D.\Logs\badlog	SUCCESS	Desired Access: G.			
googrog wee	127.32 Tk witterie D. Loga goodlog	5000255	U198: 54,045.	3.36.3 Logi eve	S428 Chesterie D. Logs bestog	SUCCESS	Desired Access. G			

Notice the difference. On the left-hand side it is shown the faster logging process, and on the righthand side the slower one. Look in the red highlighted area to see the difference. On the left-hand side the logging file is opened, followed by continuous writing, while on the right-hand side the file is opened and closed for every writing operation which explains the significant slowdown.

To recap, Task Manager shows what processes use the disk intensively at the current time, Windows Performance Recorder / Windows Performance Analyzer show who used the disc during a longer time period, although they were showing the activity as belonging to the System process instead of our process. Using Process Monitor we could identify our processes' entire activity and we could determine why one is slower than the other. But what if we could find out which line in the code causes the problem? Go back to Process Monitor. Use the window of the badly written logging program (Logs.exe). Go to Options  $\rightarrow$  Configure

Configure Symbols ×
Process Monitor uses symbols to resolve function names when displaying thread stack locations on the Stack page of an event's properties dialog.
If you do not require that information you do not need to configure symbols.
DbgHelp.dll path (version 6.0 or later):
C:\Windows\SYSTEM32\dbghelp.dll
Symbol paths:
srv*https://msdl.microsoft.com/download/symbols
When displaying stack traces for modules for which you have both symbols and source code available Process Monitor can let you view the source associated with a stack frame.
Source code paths:
OK Cancel

Symbols, which will open the window shown below.

In the log (D:\Logs\bad.log) go to CreateFile. Double-click to open the Event Properties window. Choose the Stacktab, scroll down and you can notice that in the main function of main\_bad\_log.cpp, at line 12 the opening takes place. Click the "Source" button to view the source code containing the issue.



# [20p] Task B - Investigating a handle leak

In logs-final.7z you have another example of two executables: **good.exe** and **bad.exe**. Both have the same outcome, the only difference being their running time (one of them is significantly slower). **Identify the problem**.

## How to:

• A handle leak consists of a process that opens files and does not close them. On modern computers if this action is performed millions of times, the system may become unresponsive and will either experience an overall slowdown or the application that causes this will eventually crash. You may think that millions of handles are impossible to reach, so it is not worth paying attention to this problem. However, imagine that there are services running on servers for years. As an example, having a handle leak every 2 seconds amounts for over 10 million handle leaks in a year. How should such problems be investigated?

• **Hint:** Open up a terminal and run HandleLeak.exe. Check out the "Details" tab in Task Manager after adding the "Handles" column.

## Exercise 04. [30p] Process Explorer

• It can be noticed that the number of handles keeps growing. This is clearly a problem, but how do we investigate it?

## How to:

• Run it as administrator. It is similar to Task Manager. Select the process that you are interested in, namely HandleLeak, and press "Ctrl + H".

• "Ctrl + H" opens a window under the "Process" section that displays all open handles along with information about them. Thus it will display file handles, registry handles, threads handles, and so on. There is another view (Ctrl + D) that displays all the loaded dlls.

• So it can be noticed that the leaks are on the following file: D:\Logs\HandleLeak\leak.txt. This is very useful information, but it would be better to find out who is responsible for the leak in code. Run Process Monitor with a filter on HandleLeak.exe and to notice the stack where the leakage is happens.