01 - Objectives

• How to **find the root cause if the system runs out of memory** with TaskManager, Windows Performance Recorder, Windows Performance Analyzer, Visual Studio, VMMap.

• **Monitoring the CPU usage** with TaskManager, Windows Performance Recorder, Windows Performance Analyzer.

• Check the amount of network traffic generated by processes with TaskManager, Windows Performance Recorder, Microsoft Network Monitoring, Wireshark.

02 - Memory, CPU and Network Monitoring (Windows)

Introduction

• The Windows operating system comes with plenty of built-in tools to analyze resource usage. The most prominent one is probably the Windows Task Manager, as it highlights resource usage of individual processes, and gives admins and users options to kill any misbehaving ones.

• The Performance Monitor and Resource Monitor are two additional tools that admins and experienced Windows users may use to analyze performance or resources related issues on Windows PCs.

03 - Tutorials/Exercises

The password for log2.zip and build.zip is: parola

Exercise 01. [30p] RAM Monitoring

Chrome.exe chrome.exe chrome.exe chrome.exe chrome.exe chrome.exe	PID 11024 628 12168 13864 16796 13792 1820	Status Running Running Running Running Running	Users Delails Username mmurgan mmurgan mmurgan mmurgan mmurgan		960,000 K 545,772 K 394,952 K 216,520 K 228,168 K	Peak workin 2,421,144 K 874,628 K 1,133,732 K 547,636 K 474,872 K	Memořy (pri 921,940 K 336,720 K 312,424 K 173,640 K 146,952 K	/42 431 614 1,222	Threads Image path name Command 54 CtProgram File "CtProgram 25 CtProgram File"CtProgram 39 CtProgram File 32 CtProgram File "CtProgram
chrome.exe chrome.exe chrome.exe chrome.exe chrome.exe chrome.exe chrome.exe chrome.exe	11024 628 12168 13864 16796 13792 1820	Running Running Running Running Running Running	mmurgan mmurgan mmurgan mmurgan mmurgan	00 00 00 00	960,000 K 545,772 K 394,952 K 216,520 K 228,168 K	2.421,144 K 874,628 K 1,133,732 K 547,636 K	921,940 K 336,720 K 312,424 K 173,640 K	/42 431 614 1,222	54 C\/Program File "C\/Program 25 C\/Program File "C\/Program 39 C\/Program File "C\/Program 32 C\/Program File "C\/Program
chrome.exe chrome.exe chrome.exe chrome.exe chrome.exe wpa.exe chrome.exe	628 12168 13864 16796 13792 1820	Running Running Running Running Running	mmurgan mmurgan mmurgan mmurgan	00 00 00	545,772 K 394,952 K 216,520 K 228,168 K	874,628 K 1,133,732 K 547,636 K	336,720 K 312,424 K 173,640 K	431 614 1,222	25 C\/Program File "C\/Program 39 C\/Program File "C\/Program 32 C\/Program File "C\/Program
Chrome.exe Chrome.exe Chrome.exe Chrome.exe Wypa.exe Chrome.exe	12168 13864 16796 13792 1820	Running Running Running Running	mmurgan mmurgan mmurgan	00 00 00	394,952 K 216,520 K 228,168 K	1,133,732 K 547,636 K	312,424 K 173,640 K	614 1,222	39 C\Program File "C\Program 32 C\Program File "C\Program
chrome.exe chrome.exe chrome.exe wpa.exe chrome.exe	13864 16796 13792 1820	Running Running Running	mmurgan mmurgan	00 00	216,520 K 228,168 K	547,636 K	173,640 K	1,222	32 C\Program File "C\Program
chrome.exe chrome.exe wpa.exe chrome.exe	16796 13792 1820	Running Running	mmurgan	00	228,168 K				
chrome.exe www.exe chrome.exe	13792 1820	Running	9					414	24 C\Program File "C\Program
wpa.exe chrome.exe	1820				262,484 K	671,732 K	144,180 K	370	23 C:\Program File "C:\Program
		Running	mmurgan	00	262,664 K	2,178,876 K	126,912 K	855	24 C:\Program File "C:\Program
Chrame.exe	13952	Running	mmurgan	00	198,604 K	228,068 K	125,544 K	2.444	50 C:\Program File "C:\Program
	14236	Running	mmurgan	00	140.324 K	452,528 K	104,296 K	338	16 C:\Program File "C:\Program
dwm.exe	/024	Running	DWM-6	00	117,844 K	237,700 K	92,028 K	743	12 C:\Windows\Sys "dwm.exe"
	6836	Running	mmurgan	00	200,816 K	305,072 K	90,088 K	2,721	54 C:\Program File "C\Program
	17004	Running	mmurgan	00	129,304 K	370,284 K	73,208 K	341 776	22 C\Program File "C\Program
	12516	Running	mmurgan		165,312 K	1,498,740 K	69,936 K		24 C:\Program File "C:\Program 18 C:\Users\mmur "C:\Users\m
									38 C:\Program File "C:\Program
	13588	Running	mmurgan	00	232.288 K	409.412 K	50.096 K	1.835	42 C:\Program File "C:\Program
slack.exe	16652	Running	mmurgan	00	78,400 K	237,956 K	45,892 K	309	22 C/\Users\mmur "C\Users\m
	9844	Running	mmurgan	00	107,064 K	169,032 K	43,104 K	311	13 C:\Program File "C:\Program
	6912	Running	mmurgan	00	77,672 K	84,240 K	39,408 K	726	19 C:/Program File "C:/Program
		Running	mmurgan					2.811	84 C:\Windows\ex C:\Windows
									2 C\Program Files {D2437B
			-						17 C\Program File "C\Program 28 C\Windows\Sys "C\Window
	dack.exe WINWORD.EXE devenv.exe slack.exe chrome.exe SkypeBrowserHost.exe	Jackewe 828 WINWORDEXE 16788 Overnv.sve 13388 Jackewe 16652 chrome.cxc 9844 Skype3rowsert fost.cxc 6912 explorer.cxc 1312 vcpkgsrv.exe 12824 chrome.rex 12824	Lackew 828 Running WINWORDE.DE: 16788 Running devences 1589 Running Jackewe 16552 Running districtionection.com 9844 Running Skypeiskowseti kol.com 9812 Running wpkorseve 13112 Running Wpkporseve 13242 Running Verphorseve 17028 Running	tackew 828 Running mmrurgan WINWORD 2012 16758 Running mmrurgan Jackewa 1538 Running mmrurgan Jackewa 16552 Running mmrurgan Korone.com 944 Running mmrurgan Skyrekisonecifist.com 812 Running mmrurgan weiphore:eee 17824 Running mmrurgan Verpkorye.we 17824 Running mmrurgan	Incl. eve 828 Running mmurgan 00 MMXXXX6D5.2XE 16788 Running mmurgan 00 devenues 13586 Running mmurgan 00 devenues 16528 Running mmurgan 00 devenues 16652 Running mmurgan 00 Skrytecknown flox.Lee: 984 Running mmurgan 00 Skrytecknown flox.Lee: 9112 Running mmurgan 00 (wylapsyncerse) 13112 Running mmurgan 00 (wylapsyncese) 17028 Running mmurgan 00	Bock-eve 828 Running mmurgan 00 197444 MMXXXX05D2.2XE 16788 Running mmurgan 00 123.25 K Generature 13586 Running mmurgan 00 222.28 K Jack-case 15652 Running mmurgan 00 274.28 K Skloptexistoral tox.tace 9844 Running mmurgan 00 77.64 K Skloptexistoral tox.tace 9112 Running mmurgan 00 77.64 K Skloptexistoral tox.tace 9112 Running mmurgan 00 77.64 K Krophore.cee 1712 Running mmurgan 00 72.65 KK Krophore.tace 1702.4K Running mmurgan 00 42.58 K	Bocknew 828 Running mmurgan 00 197,44/k 978,52/k WMXXXX6D2.22K 16788 Running mmurgan 00 132,52/k Generavae 13586 Running mmurgan 00 212,22/8 K 40,412 K Jackcese 16652 Running mmurgan 00 78,404 K 1650,27 K 164,212 K 164,22 K 164,20 K 165,22 K 164,20 K 165,22 K 164,22 K 164,20 K 1	Back-leve 878 Bunning mmurgan 00 197,441 K 378,542 K 538,752 K WMXXXXD5D282 K 16788 Bunning mmurgan 00 113,354 K 50,716 K Generavae 15388 Bunning mmurgan 00 212,228 K 40,914 Z 50,906 K Jack-leve 16652 Fluming mmurgan 00 78,400 K 237,258 K 45,952 K Jack-leve 3694 Numing mmurgan 00 10,064 K 189,052 K 43,104 K Skiprekhowser/back-leve 9112 Ruming mmurgan 00 17,642 K 94,400 K 39,400 K Skiprekhowser 13112 Ruming mmurgan 00 17,648 K 159,400 K 37,484 K Veryberscere 1202 K Ruming mmurgan 00 12,658 K 159,400 K 37,484 K Veryberscere 1202 K Ruming mmurgan 00 24,554 K 34,792 K 34,792 K 34,792 K 34,792 K 34,792 K 34,792	Back-eve 828 Running mmurgan 00 197.44 k 738,53 k 538,25 k 400 WMWX06D5.24 16788 Running mmurgan 00 123,25 k 130,76 k 53,72 k 400 Gevenvae 1358 Running mmurgan 00 222,28 k 400,41 2 k 50,05 k 48,12 k 50,05 k 48,21 k 45,00 k 45,92 k 45,90 k 45,92 k 45,99 k 43,99 k 26,90 k 13,19 k 2,21 k 43,194 k 2,811 11,18 k 42,19 k 2,41 k 2,42 k 3,494 k 2,811 14,19 k 2,211 k 2,41 k 2,42 k 3,484 k 2,811 14,19 k 2,211 k 2,41 k 2,42 k 2,41 k 2,41 k 2,41 k 2,41 k 2,42 k 2,41 k 2,41 k

Fewer details

[15p] Task A - Identify the problem

than Working Set.

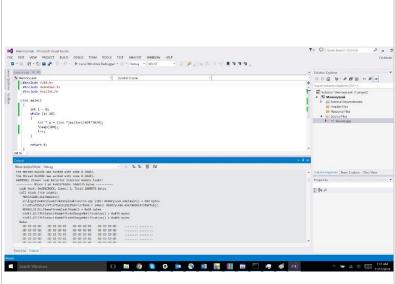
What can you do if the system runs out of memory, but you do not know what causes this?
 Windows Performance Recorder

	windows Performance Recorder	- 🗆 X
	Description information	
	Record system information	•
	This tool will gather information about the interaction of the programs computer for analysis.	and hardware running on this
Imaging a situation when a system	Status: Recording not started	Time:
Imagine a situation when a system encounters issues if some		Buffer: Events dropped:
		Start Cancel
conditions are met, and these		
conditions can be reproduced. To find out the source of this problem	Calast additional profiles for performance speedings	Performance scenario:
start Windows Performance		General ~
Recorder configured as shown	File I/O activity	Detail level:
below.	Networking I/O activity	Logging mode:
	✓ Heap usage ✓ Pool usage	Memory ~
	✓ VirtualAlloc usage □ Power usage	To insert an annotated marker, press CTRL + WIN + x during trace capture.
	GPU activity	trace capture.
	Handle usage	
	Add Profiles	About
Windows Performance Analyze	r	
Run in		
parallel a		
program that		
allocates		
1MB of		
memory		
every 100 MINISCAN LITE-17-201609-38-31 ed Windows Performance Analyzer		
milliseconds	yatr and a second se	
for a while Trace Rundown		
and then Trace Rundown		
stops. After		
the program		
Add all Menory graphs to Analysis View Add all Menory graphs to Analysis View Add all Menory graphs to New Analysis View		
running, save are the capture		
- ingright selector Co		
in Windows		
Performanc		
e Analyzer.		
You should		
get the		
following.		
Click Add all	1	
MAURGAN C11117 2016/26 38 31.4 - Windows Performance Analyzar File: Taxe: Profiles: Window: Help		
graphs to System Activity U Delays By Process, Type 8 + chrome cee (12004)	207 2.335 2023 27 2.739 2276	*
Analysis	 D D D H D D D D D D D D D D D D D D D D D D D	
View and	Trace Rundown	
scroll down	HemanyLevel (18656)	
to Park Outstandin	Working Set 11/26,832 B Working Set 11/26,832 B Zero UNIX non-Skidl 5/26 5/2	
the Virtual	472 500 277 - 4 415 500 000 2 80 596 7 0 -	
Memory	zrisani jayoon zalooni entrone satisete* □ P 0	
Snapshot gra	In France and Index C II P 0 P P C II P C III P C II P C III P C II P C II P C II P C II P C	
ph which		

shows the memory usage for all processes.

Visual Studio

After installing, it requires including the *vld*.*h* file. When writing the code, the following functions need to be overwritten: malloc, free, new, and delete. This allows each memory allocation and deallocation to be tracked. All the detected leakages (having an allocation that is not followed by a deallocation) will be saved in a log file that can be viewed after the program stops running. In the bottom part of the screenshot shown below, it can be noticed where the allocation took place and that it is not followed by a deallocation.



VMMap

• minap		
However, it might be the		
case that this		
is not a		
memory leak,		
and		
somewhere at		
the end of the		
program the		
memory gets	WMAp - byskitternals: www.ayskitternals.com The Edit: View Optione Holp Process: PD: PD:	
unallocated. If	Committeds	· · · · · · · · · · · · · · · · · · ·
this is the	Violating Set:	Select or Launch Process × Waw a running process Launch and theor a new process
	Type Size Committed Private Total., Priva., Bhan., Bhan.,	When you launch an application from Yimmap the application is instrumented to back individual memory allocations (HespAlloc, Virtual/Aloc, Hc) along with the associated mill steply.
case, how can		Application: 01logs2/HemoniteskiDehug/Hemoniteskiese
you determine		Arguments: Start Directary: Dr.Logi2/MomoryLoak/Dobug
which part of		
the program is	Address Type S., C., Pinvelo T., P., S., J., L., S., Rotection Details	1
responsible		
for generating		CK Cencel
the spike?		
This requires		
using another		
tool from		
SysInternals,		
VMMap.		
With this tool		
you can view		
a process's		
-		

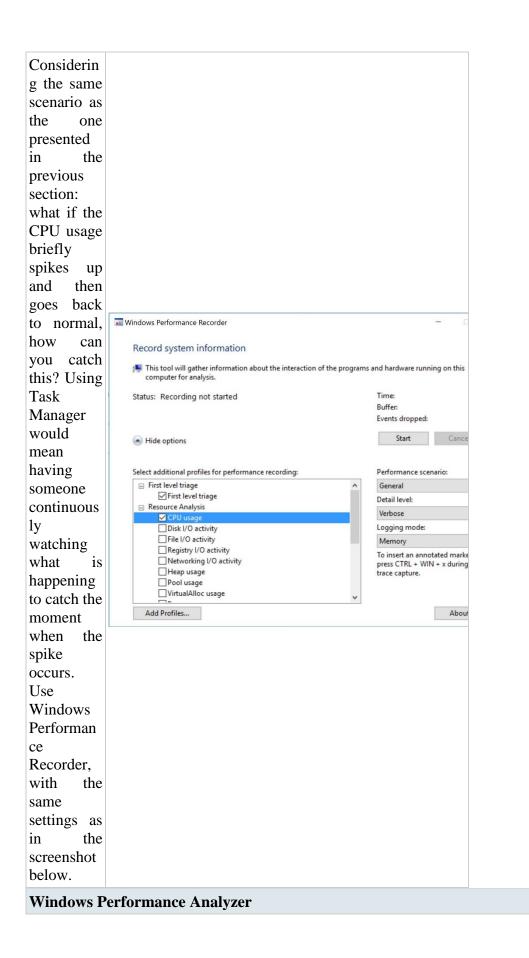
memory allocations and usage. Use it to run the program that allocates 1 MB of memory every 100 milliseconds.	
Prior to starting the tool, go to Options, Configure Symbols and set the paths to the program's, to the Microsoft Symbol Server, and to the program's source files. Start the tool, select Launch and trace a new process, select the	Type Dave Deserved Preven Total. Ford. Ford. 100 100 50 00000 10000 10000 100 100000 100000 100000 100000 100000 100 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 100000 1000000 1000000 1000000<
process, select the directory where it will run, and let it run. You will see something similar to the screenshot below. To view the latest memory allocations, you need to double- click Heap in the upper-part of the screenshot, and hit F5 (refresh) from time to time. In the bottom	Image: Note of the state of the st

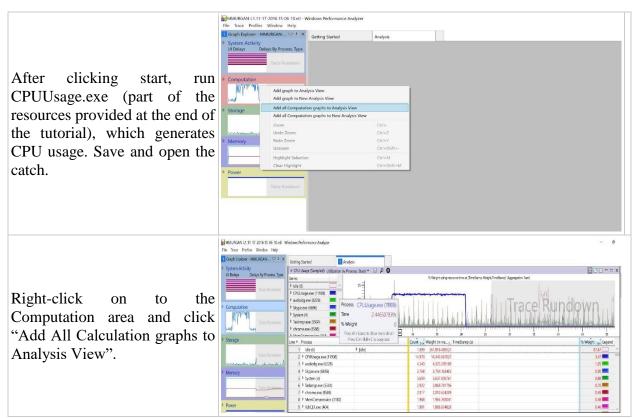
part of the
screenshot,
you can view
the memory
allocations. If
you click one
and
press Heap
Allocations y
•
ou can see the
stack where
the allocation
occurred. By
pressing the
"Source"
button, you
can view the
actual code for
the allocation.
[15-1 Teels D

[15p] Task B - Conclusions

Discuss the output and call the assistant to show him/her your progress.
 Exercise 02. [30p] CPU Monitoring

Task	Mana	ger									
Moni	toring										
the	CPU										
usage											
presei	nts										
simila	ır										
issues	to	i Task Manager File Options View									- • >
		Processes Performance	e Apph	istory Start-up	Users Details S	rvices					
the	ones	Name	PID	Status	Username	CPU	demory (pri	Handles	Threads Image path name Con	mmand line	Description
encou	ntere	System Idle Process audiodg.cxc	0 6220	Running Running	SYSTEM LOCAL SLRV	92 01	4 K 21,432 K	1,390	8 24 C\Windows\Sys C\V	Windows\sys	Percentage of time the processor is idle Windows Audio Device Graph Isolation
cheou	munu	RedrCFE.exe	5504 404	Running Running	mmurgan mmurgan	01	14,152 K 28,856 K	522	24 C:\Windows\Sys "C:\ 11 C:\Program File "C:\		
d	when	Skype.exe	6696	Running	mmurgan	01	71,124 K	1,734	67 C:\Program File "C:\	Program Fil	Skype
		Chrome.exe	2476	Running	mmurgan SYSTEM	01	145,580 K 28 K	386 1,594	23 C:\Program File "C:\ 182 C:\Windows\svs	Program Fil	Google Chrome NT Kernel & System
monit	oring	Chrome.exe	7500	Running	mmurgan	00	110,500 K	394	22 C:\Program File "C:\		Google Chrome
	8	Chrome.exe	8816 3656	Running	mmurgan mmurgan	00	115,788 K 794,232 K	397 508	22 C\Program File *C\ 36 C\Program File *C\		
the		System interrupts	-	Running	SYSTEM	00	ОК	-	-	1000200000000000	Deferred procedure calls and interrupt service rout
		Chrome.exe	8588 9104	Running Running	mmurgan mmurgan	00	145,160 K 117,420 K		45 C\Program File "C\ 22 C\Program File "C\		
memo	ory	Chrome.exe	9548	Running	mmurgan	00	128,608 K		18 C:\Program File "C:\		
	•	dwm.exe explorer.exe	10084 4412	Running	DWM 1	00	180,832 K 39,376 K	677 2.022	11 C:\Windows\Sys "dw		Desktop Window Manager
usage		ELOUTLOOK LXL	4412 8300	Running Running	mmurgan mmurgan	00	39,376 K 127,644 K		79 C:\Windows\ex., C:\V 56 C:\Program Lile., "C:\		
0		Chrome.exe	1236	Running	mmurgan	00	121,116 K	303	17 C\/Program File "C\		
Task		SkypeBrowserHost.exe	7356 10668	Running	mmurgan mmurgan	00	57,332 K 51,272 K	930 819	35 C:\Users\mmur "C:\ 24 C:\Program File "C:\		
۱ <i>۲</i>		Slack.exe	8948	Running	mmurgan	00	119,216 K	425	23 C:\Users\mmur "C:\	Users\mmur	. Slack
Mana	ger	InvSCPAPISvnexe InvSCPAPISvnexe	1524 6772	Running	SYSTEM mmurgan	00	2,348 K 64,956 K	146 2,332	4 C:\Program File "C:\ 66 C:\Program File "C:\		Stereo Vision Control Panel API Server Skype for Business
can	help	~		1.000 m	1999		and showing the	10000			· · · · · · · · · · · · · · · · · · ·
	-	Fewer details									End task
find o	ut the										
curren	nt										
CPU	usage										
for	a										
proce	55.										
Wind	lows P	erforma	ano	e Re	ecorde	r					
						-					





The graph shows the impact of CPUUsage.exe, which inflicts a 12% CPU usage. Part of the problem is solved, it was determined who is generating the CPU usage. Now, to further debug the situation, as in the previous case of the memory, if this process was not written by you, check if it is useful, and if not, make sure to stop it. If it is useful, but it's not yours, you can try to find an update to fix the problem, or report the problem to the producer. If the program is written by you (this course - Performance Evaluation - targets the processes written by us), then it is important to determine what causes this problem. Unfortunately, unlike in the case of monitoring the memory usage, there is no tool that shows the stack with the problem, so you need to create one. Open EvenimenteProcMon, which has the purpose of integrating your messages with ProcessMonitor so they can be viewed as the process unfolds. It is necessary to understand any code, not perfectly, but at least to get the big picture of what is going on.

A ProcessMonitor class with 5 functions was created:

- **OpenProcMon** opens up a handle for the ProcessMonitor's message interface.
- **CloseProcMon** closes this handle.
- **ProcMonLog** writes the message that is passed as a parameter to the ProcessMonitor interface.
- **MyProcMon** is the class constructor. It is called when a MyProcMon object is declared.

• ~ **MyProcMon** is the class destructor. It is called to destroy the MyProcMon object.

The code below highlights that it was declared globally:

MyProcMon __procMon;

This means that at the start of the process, before executing the main function, when the global variables are initialized, our class instance will be constructed along with the implicit handle for the ProcessMonitor message interface. The handle is closed when the object is destroyed, after the program's execution ends.

Another class was declared, ProcMonLogFunc, with the purpose of highlighting when entering and leaving a function. This led to defining the following macro, which declares a ProcMonLogFunc object and passes it the name of the current function as a parameter.

#define DBGTRACE_FN_ () ProcMonLogFunc __my_log __ (__ FUNCTIONW__)

Start	
ProcessMonitor	
and change the	
filter to	
ProcessName	Process Monitor - Sysinternals: www.sysinternals.com File Edit Event Filter Tools Options Help
contains	😂 🖬 💸 📴 🖾 🗢 🖉 🖻 🛤 🦻 🎎 🗟 🎎 🕸 📶
EvenimenteProc	
Mon. Select the	
profiling button	
as shown below.	
Running the	Process Monitor - Spinternaks.com File Edit Event Filter Tools Options Help
program,	Image: Control (Control (Contro (Control (Control (Control (Control (Contro) (Control (Control (
generates a	4-4264 885155494 T Greenmetchen, 6152 Lithersen Freding SUCCESS User Time 0.0000000 seconds, Rende 1 Time 0.0000000 seconds, Rende 1 4-426 8852107 PM T Exementative, 052 Lithersen Tending SUCCESS User Time 0.0000000 seconds, Rende 1 0019255 seconds, Printel 4-426 8852101 PM T Exementative, 052 Lithersen Tending SUCCESS User Time 0.000000 seconds, Rende 1 Feb 2019255 seconds, Printel 4-426 8852101 PM T Exementative, 052 Lithersen Tending SUCCESS User Time 0.000000 seconds, Rende 1 Feb 2019255 seconds, Printel 4-426 8852101 PM T Exementative, 052 Lithersen Tending SUCCESS User Time 0.000000 seconds, Rende 1 Feb 2019255 seconds, Printel 4-426 8852101 PM E Exementative, SUCCESS SUCCESS User Time 0.000000 seconds, Rende 1 Feb 2019255 seconds, Printel 4-426 8852101 PM E Exementative, SUCCESS S
Process Monitor	4.427 134555 PM # Ememethine. 552 _Lbbiq.0dp.d. 04.4 0447 - 0467
capture like this	4-Q271144920 PM ■ Comment/hm . GS2 _L Debag Odgat. Odgat - Odgat - offend2 4-Q27114020 PM ■ Comment/hm . GS2 _L Debag Odgat. Odgat - Odgat - offend2 4-Q27114005 PM ■ Comment/hm . GS2 _L Debag Odgat. Odgat - Odgat - offend3 4-Q27114005 PM ■ Comment/hm . GS2 _L Debag Odgat. Odgat - Odgat - offend3
one.	4 42 37 183148 MR ■ Exeministrative. ISS2 _Li Deling Odput . Odput . Odput contain 4 42 37 183148 MR ■ Exeministrative. ISS2 _Li Deling OdputOdput contain

Notice messages such as Output: \Rightarrow Func1 and Output: \Leftarrow = Func1, with the associated times for these events in the left-hand side of the screenshot, in the Time of Day column. The difference between the times (4:42:07.1848883 and 4:42:07.1848955) is 72, and since the times after the comma are expressed in hundreds of nanoseconds, this means that func1 took 7.2 microseconds.

As it is inefficient to calculate by hand the times for each function, save the output in csv format (File \rightarrow Save and choose the "Comma-Separated Values" option). The generated file will look like this:

"4:42:07.1846936 Profiling","","","Output: ===	PM","EvenimenteProcMon.exe","6352","Debug >main"	Output
"4:42:07.1848812 Profiling","","","Output: Ac	PM", "EvenimenteProcMon.exe", "6352", "Debug esta e logul meu 1"	Output
"4:42:07.1848883 Profiling","","","Output: ===	PM","EvenimenteProcMon.exe","6352","Debug >Func1"	Output
"4:42:07.1848955 Profiling","","","Output: <=	PM","EvenimenteProcMon.exe","6352","Debug =Func1"	Output
"4:42:07.1848990 Profiling","","","Output: ===	PM","EvenimenteProcMon.exe","6352","Debug >Func2"	Output
"4:42:07.1849038 Profiling","","","Output: <=	PM","EvenimenteProcMon.exe","6352","Debug =Func2"	Output
"4:42:07.1849069 Profiling","","","Output: ===	PM","EvenimenteProcMon.exe","6352","Debug >Func3"	Output

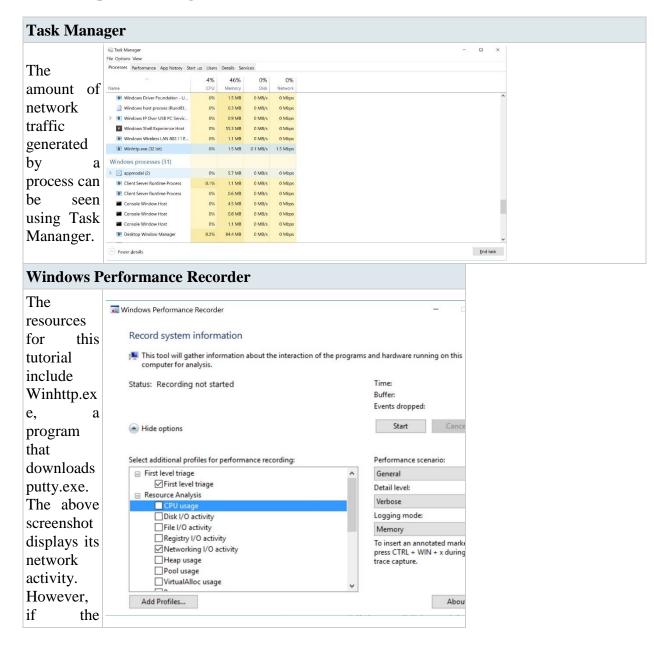
"4:42:07.1849105 Profiling","","","Output: <==	PM","EvenimenteProcMon.exe","6352","Debug =Func3"	Output
"4:42:07.1849148 Profiling","","","Output: Acc	PM", "EvenimenteProcMon.exe", "6352", "Debug esta e logul meu 2"	Output
"4:42:07.1849184 Profiling","","","Output: <==	PM","EvenimenteProcMon.exe","6352","Debug =main"	Output

Making a parser in Python would make it easy to notice in which of the functions was spent the most time. If you only want to take into account the CPU usage, you need to have logging messages before and after every I/O operation, in order to not count in their time.

Integrate CPUUsage with ProcessMonitor and find out the total time spent in every function.

Exercise 03. [40p] Network Monitoring

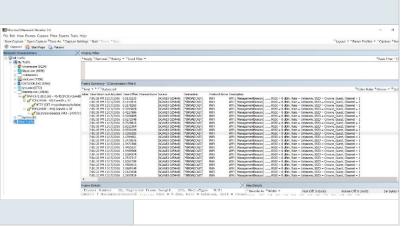
Task A [20p] - Go through tutorial



process	
generatin	ıg
the	
network	
activity	
unknown	
you can u	
Windows	
Performa	ın
ce	
Recorder	
with t	
following	g
settings.	
	nd
open t	
capture	
	it.
The	
statistics	
offered l	•
Windows	
Performa	ın
ce	
Analyzer	
are for the	
total use	of
the	
network,	
rather the	
per proce	
statistics.	•

Microsoft Network Monitoring

For this reason, we are calling upon another tool developed by Microsoft. Install it, start it using "Run as administrator", and select the network interface through which the traffic is expected to pass (cable, wifi, ...). You should get a capture such as this one:



Wireshark

As in the case of the CPU, inspecting the events taking place on the network involves some amount of work for the analyst. However, this being a simple case, you can just expand the view on the raffic generated by Winhttp.exe, and notice the request for <i>putty.exe</i> . If it is noticelar why some requests are there or why leads book on the raffic generated by winht you can integrate the application that you vish to to tr. This way you can insert logging elements to find out what request are made and how long they take. The part with timing	As in the			
for putty.exe. If it is not clear why some requests are there or why they last so long, you can integrate the application that you with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	CPU, inspecting the events taking place on the network involves some amount of work for the analyst. However, this being a simple case, you can just expand the view on the traffic generated by Winhttp.exe, and notice	The Wineback Rescond Andreer (Wineback 222) (522) (4-975600) The field you go (paters Andree Status) Telephony Josh Josenna Halp The field you go (paters Andree Status) Telephony Josh Josenna Halp The field you of the field of the the telephone field of telephone fiel	ar Apply Save	
traffic generated by Winhttp.exe, and notice the request for <i>putty.exe</i> . If it is not clear why some requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	expand the			
<pre>generated by Winhttp:exe, and notic the request for putty.exe. If it is not clear why some requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part</pre>				
Winhttp.exc, and notice the request for putty.exc. If it is not clear why some requests are there or why they last so long, you can integrate the the that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part				
and notice the request for <i>putty.exe</i> . If it is not clear why some requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part		The Wreshark Network Analyzer (Wreshark 222 (v222-0-g775/008))		
the request for putty.exe. If it is not clear why some requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	-	SONNE DEAD (FFFFEE BG 44		
for <i>putty</i> .exe. If it is not clear why some requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part		The World's Most Deputer Network Prote		
If it is not clear why some requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	-	Capture		
clear why some self-and and and requests are self-and and there or why self-and and they last so self-and and long, you can integrate the application that you with ProcessMoni self-and and tor. This way you can insert logging elements to find out what request are made and how long they they take. The part		A	Open a previously captured file	
some requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part		Choose one or more interfaces to capture from then Start	Sample Captures	
requests are there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	-	Bluttooth Network Connection		
there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	requests are	Start a capture with detailed options		
they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part				
can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	-			
the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why	Capture Help		
application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you	Capture Help		
that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate	Capture Help		
wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the	Capture Help		
investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application	Capture Help		
with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application that you	Capture Help How to Capture		
ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to	Capture Help How to Capture		
tor. This way you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate	Capture Help How to Capture		
you can insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with	Capture Help How to Capture		
insert logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni	Capture Help		
logging elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way	Capture Help How to Capture		
elements to find out what request are made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can	Capture Help How to Capture		
request are made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert	Capture Help How to Capture		
made and how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging	Capture Help How to Capture		
how long they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to	Capture Help How to Capture		
they take. The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what	Capture Help		
The part	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and	Capture Help How to Capture How to Capture		
	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long	Capture Help		
with timing	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take.	Cepture Help How to Cepture		
	there or why they last so long, you can integrate the application that you wish to investigate with ProcessMoni tor. This way you can insert logging elements to find out what request are made and how long they take. The part	Capture Help		

the requests and traffic can be determined straight from Network Monitor by considering the times of the packets. For displaying all traffic on a http connection (it can also be https as long as you control the server, but this in not in the scope of this tutorial), you can use another tool, Wiresh ark. Install Wireshark (64bit!!!) accepting the default settings. Start it and select the	
this in not in	
this tutorial),	
Wireshark	
accepting the default	
Start it and select the	
interface that you want to listen to.	
Click	Interruption with (percepts) ac22/02/2010/0000000000000000000000000000
the Start butt	International Description Description <thdescription< th=""> <thdescription< th=""></thdescription<></thdescription<>
on and run Winhttp.exe.	1112 22:05504 127:05.7.14 004;193.5.19 tra 51 24884-417 [Col] appl. doi:10.1001 [Col] appl. doi:10.100
After Winhttp.exe	146 72,202,21 74,202
stops, click the Stop	1476 23, 446966 172, 202, 141 266, 1499, 152 9 FCF 31 2468-451 [ACC] append Acc-2013 wine-251 wine-0 1427 21, 4471 21, 4511 21, 4511, 4511, 21 Appletic modular 1427 24, 4571 20, 4511, 4511, 4511, 4511, 4511, 4511, 4514, 4514, 4511, 4514,
button in	
Wireshark.	00000 000000 000000 00000 00000

This way	
you have obtained a traffic capture while winhttp.exe was running. Viewing the code for winhttp.exe, it can be	Reply from 86.106.30.115: bytes=32 time=143ms TTL=48 Reply from 86.106.30.115: bytes=32 time=143ms TTL=48
	13. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 14. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 15. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 16. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 17. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 18. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 19. m. 80%-172.0% 1. m. 10%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 19. m. 80%-172.0% 1. m. 10%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 19. m. 80%-172.0% 1. m. 10%-172.0% 1. m. 80%-172.0% 1. m. 80%-172.0% 19. m. 80%-172.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 19. m. 80%-173.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 19. m. 80%-174.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 19. m. 80%-174.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 1. m. 10%-172.0% 10. m. 10%-174.0% 1. m. 10%-174.0% 1. m. 10%-174.0% 1. m. 10%-174.0% 10. m. 10%-174.0% 1. m. 10%-174.0% 1. m. 10%-174.0% 1. m. 10%-174.0% <t< td=""></t<>
In the bottom part of the Wireshark window, at the "Show and save data as" option choose	No. 1 Control Control <th< td=""></th<>

"Raw". Save the capture (using the "Save as" button) as " <i>my.pdf</i> ".	
Use Notepad++ to open the my.pdf file and remove the headers as shown in the screenshot below.	Conservation • <t< th=""></t<>
Save it, close Notepad++ and double- click on the newly saved file (my.pdf).	Typed Addee Ander Valuater French Attende Ferr Editar Violater French Attende Tegrina principali Instrumenta Tegrina principali Instrumenta

Task B [20p] - Conclusions

• Discuss the output and call the assistant to show him/her your progress.