Московский Авиационный Институт
(Национальный Исследовательский Университет)
Факультет информационных технологий и прикладной математики
Кафедра вычислительной математики и программирования

Лабораторная работа №8 по курсу
«Операционные системы»

Студент: Кривошапкин Егор Борисович
Группа: М8О-209Б-23
Вариант: 8
Преподаватель: Миронов Евгений Сергеевич
Оценка: _____
Дата: _____
Подпись: _____

Москва, 2024

Содержание

Репозиторий

https://github.com/EgorX2000/os_labs/tree/main/8

(логи Process Monitor находятся там же)

Постановка задачи

Цель работы

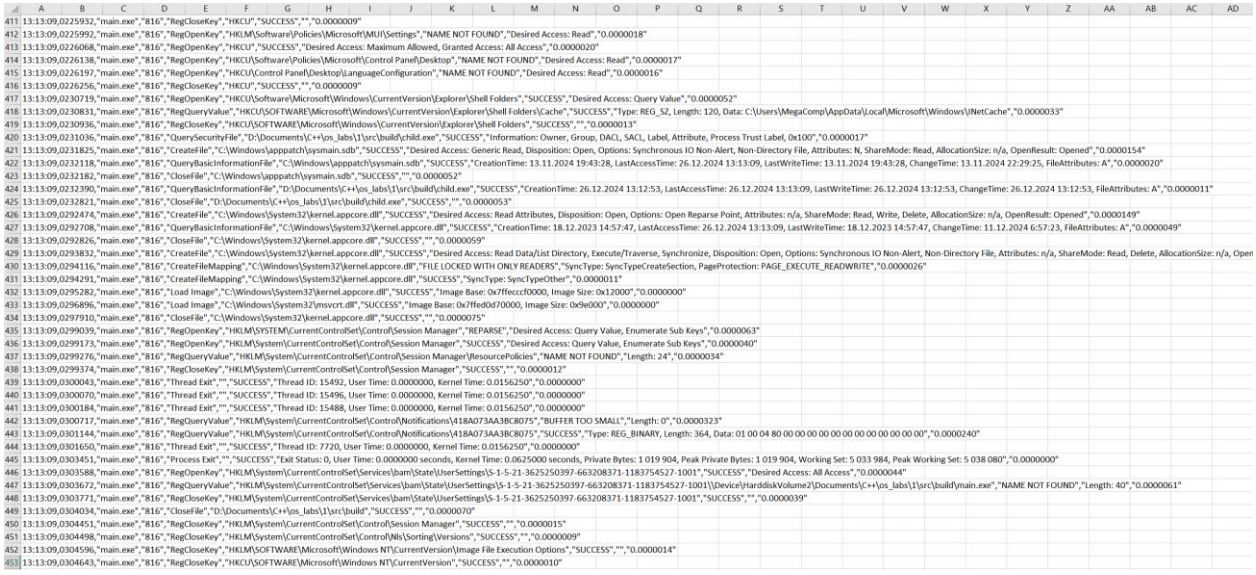
Приобретение практических навыков диагностики работы программного обеспечения.

Задание

При выполнении лабораторных работ по курсу ОС необходимо продемонстрировать ключевые системные вызовы, которые в них используются и то, что их использование соответствует варианту ЛР. По итогам выполнения всех лабораторных работ отчет по данной ЛР должен содержать краткую сводку по исследованию написанных программ.

Выполнение задания

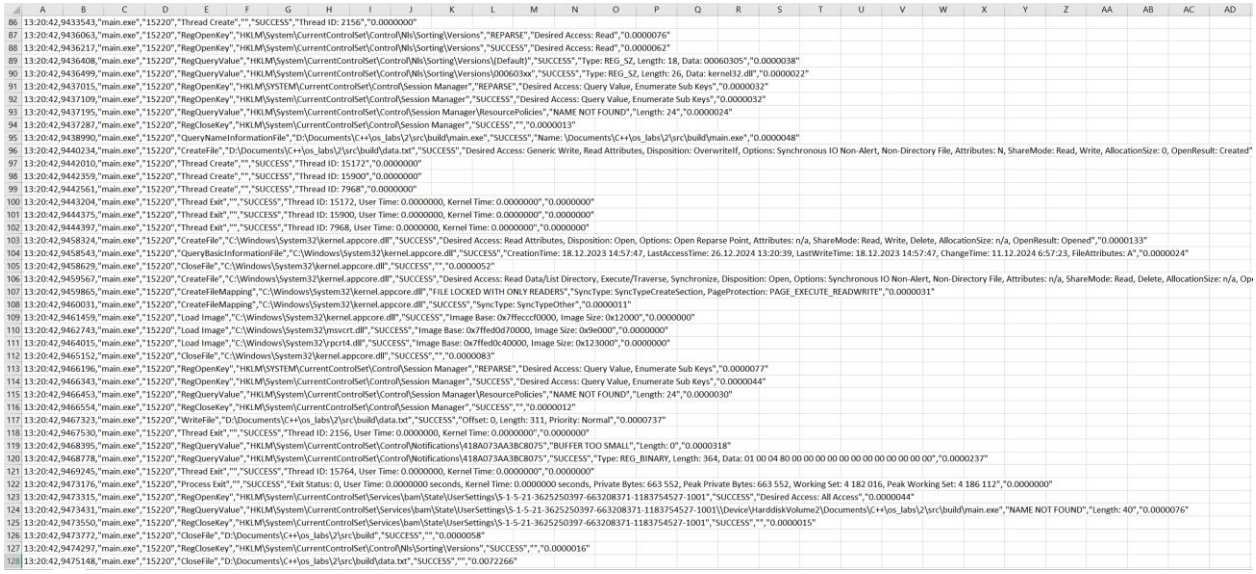
Lab1



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD
411	13:13:09,0225932,"main.exe","816","RegCloseKey","HKCU","SUCCESS","","0.0000009"																													
412	13:13:09,0225992,"main.exe","816","RegOpenKey","HKLM\Software\Policies\Microsoft\MUI\Settings","NAME NOT FOUND","Desired Access: Read","0.0000018"																													
413	13:13:09,0226068,"main.exe","816","RegOpenKey","HKCU","SUCCESS","Desired Access: Maximum Allowed, Granted Access: All Access","0.0000020"																													
414	13:13:09,0226138,"main.exe","816","RegOpenKey","HKCU\Software\Policies\Microsoft\Control Panel\Desktop","NAME NOT FOUND","Desired Access: Read","0.0000017"																													
415	13:13:09,0226197,"main.exe","816","RegOpenKey","HKCU\Control Panel\Desktop\LanguageConfiguration","NAME NOT FOUND","Desired Access: Read","0.0000016"																													
416	13:13:09,0226256,"main.exe","816","RegCloseKey","HKCU","SUCCESS","","0.0000009"																													
417	13:13:09,0230719,"main.exe","816","RegOpenKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","Desired Access: Query Value","0.0000052"																													
418	13:13:09,0230831,"main.exe","816","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ, Length: 120, Data: C:\Users\MegaComp\AppData\Local\Microsoft\Windows\INetCache","0.0000033"																													
419	13:13:09,0230936,"main.exe","816","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","","0.0000013"																													
420	13:13:09,0231036,"main.exe","816","QuerySecurityFile","D:\Documents\C++\os_labs\1\src\build\child.exe","SUCCESS","Information: Owner, Group, DACL, SACL, Label, Attribute, Process Trust Label, 0x100","0.0000017"																													
421	13:13:09,0231825,"main.exe","816","CreateFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, AllocationSize: n/a, OpenResult: Opened","0.0000154"																													
422	13:13:09,0232118,"main.exe","816","QueryBasicInformationFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","CreationTime: 13.11.2024 19:43:28, LastAccessTime: 26.12.2024 13:13:09, LastWriteTime: 13.11.2024 19:43:28, ChangeTime: 13.11.2024 22:29:25, FileAttributes: A","0.0000020"																													
423	13:13:09,0232182,"main.exe","816","CloseFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","","0.0000052"																													
424	13:13:09,0232390,"main.exe","816","QueryBasicInformationFile","D:\Documents\C++\os_labs\1\src\build\child.exe","SUCCESS","CreationTime: 26.12.2024 13:12:53, LastAccessTime: 26.12.2024 13:13:09, LastWriteTime: 26.12.2024 13:12:53, ChangeTime: 26.12.2024 13:12:53, FileAttributes: A","0.0000011"																													
425	13:13:09,0232821,"main.exe","816","CloseFile","D:\Documents\C++\os_labs\1\src\build\child.exe","SUCCESS","","0.0000053"																													
426	13:13:09,0292474,"main.exe","816","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened","0.0000149"																													
427	13:13:09,0292708,"main.exe","816","QueryBasicInformationFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","CreationTime: 18.12.2023 14:57:47, LastAccessTime: 26.12.2024 13:13:09, LastWriteTime: 18.12.2023 14:57:47, ChangeTime: 11.12.2024 6:57:23, FileAttributes: A","0.0000049"																													
428	13:13:09,0292826,"main.exe","816","CloseFile","C:\Windows\system32\kernel.appcore.dll","SUCCESS","","0.0000059"																													
429	13:13:09,0293832,"main.exe","816","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Open																													
430	13:13:09,0294116,"main.exe","816","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","FILE LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE","0.0000026"																													
431	13:13:09,0294291,"main.exe","816","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","SUCCESS","SyncType: SyncTypeOther","0.0000011"																													
432	13:13:09,0295282,"main.exe","816","Load Image","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Image Base: 0x7ffecccf0000, Image Size: 0x12000","0.0000000"																													
433	13:13:09,0296896,"main.exe","816","Load Image","C:\Windows\System32\msvcrt.dll","SUCCESS","Image Base: 0x7ffed0d70000, Image Size: 0x9e000","0.0000000"																													
434	13:13:09,0297910,"main.exe","816","CloseFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","","0.0000075"																													
435	13:13:09,0299039,"main.exe","816","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager","REPARSE","Desired Access: Query Value, Enumerate Sub Keys","0.0000063"																													
436	13:13:09,0299173,"main.exe","816","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","Desired Access: Query Value, Enumerate Sub Keys","0.0000040"																													
437	13:13:09,0299276,"main.exe","816","RegQueryValue","HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies","NAME NOT FOUND","Length: 24","0.0000034"																													
438	13:13:09,0299374,"main.exe","816","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000012"																													
439	13:13:09,0300043,"main.exe","816","Thread Exit","","SUCCESS","Thread ID: 15492, User Time: 0.0000000, Kernel Time: 0.0156250","0.0000000"																													
440	13:13:09,0300070,"main.exe","816","Thread Exit","","SUCCESS","Thread ID: 15496, User Time: 0.0000000, Kernel Time: 0.0156250","0.0000000"																													
441	13:13:09,0300184,"main.exe","816","Thread Exit","","SUCCESS","Thread ID: 15488, User Time: 0.0000000, Kernel Time: 0.0156250","0.0000000"																													
442	13:13:09,0300717,"main.exe","816","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","BUFFER TOO SMALL","Length: 0","0.0000323"																													
443	13:13:09,0301144,"main.exe","816","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","SUCCESS","Type: REG_BINARY, Length: 364, Data: 01 00 04 80 00 00 00 00 00 00 00 00 00 00 00 00","0.0000240"																													
444	13:13:09,0301650,"main.exe","816","Thread Exit","","SUCCESS","Thread ID: 7720, User Time: 0.0000000, Kernel Time: 0.0156250","0.0000000"																													
445	13:13:09,0303451,"main.exe","816","Process Exit","","SUCCESS","Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 1 019 904, Peak Private Bytes: 1 019 904, Working Set: 5 033 984, Peak Working Set: 5 038 080","0.0000000"																													
446	13:13:09,0303588,"main.exe","816","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","Desired Access: All Access","0.0000044"																													
447	13:13:09,0303672,"main.exe","816","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001\\Device\HarddiskVolume2\Documents\C++\os_labs\1\src\build\main.exe","NAME NOT FOUND","Length: 40","0.0000061"																													
448	13:13:09,0303771,"main.exe","816","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","","0.0000039"																													
449	13:13:09,0304034,"main.exe","816","CloseFile","D:\Documents\C++\os_labs\1\src\build","SUCCESS","","0.0000070"																													
450	13:13:09,0304451,"main.exe","816","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000015"																													
451	13:13:09,0304498,"main.exe","816","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS","","0.0000009"																													
452	13:13:09,0304596,"main.exe","816","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options","SUCCESS","","0.0000014"																													
453	13:13:09,0304643,"main.exe","816","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion","SUCCESS","","0.0000010"																													

Системные вызовы:
CreateFile - Создает или открывает файл или устройство ввода-вывода.
CreateProcess - Создает новый процесс и его основной поток.
CreatePipe - Создает анонимный канал и возвращает дескриптор к концам канала чтения и записи.

Lab2

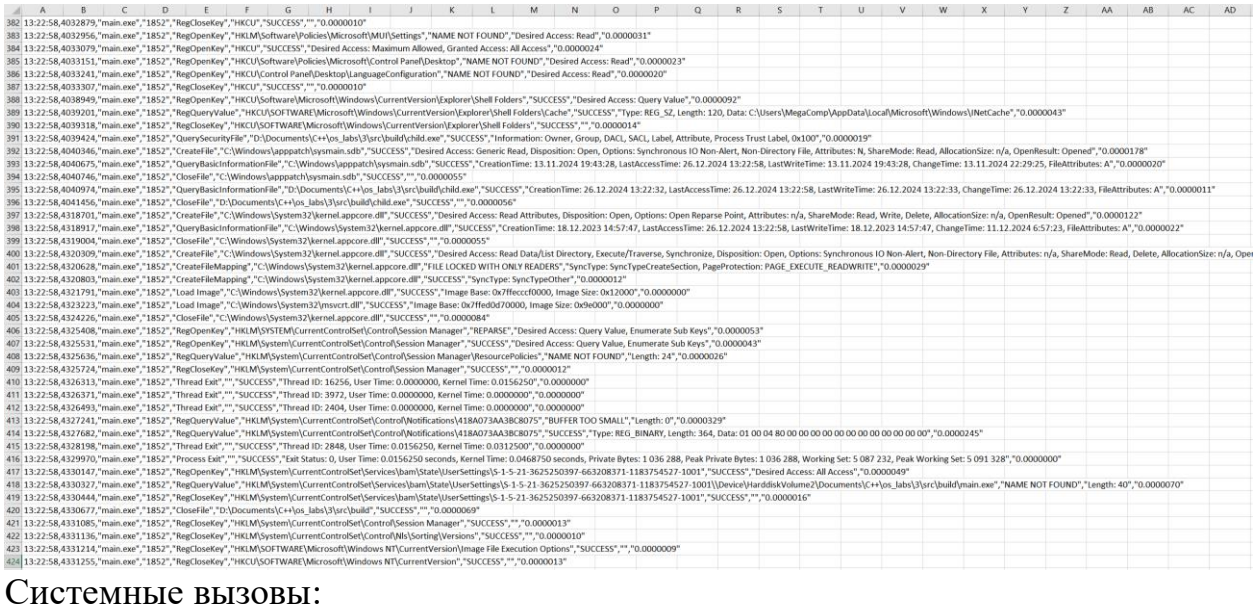


13:20:42,9433543,"main.exe","15220","Thread Create","","SUCCESS","Thread ID: 2156","0.0000000"
13:20:42,9436063,"main.exe","15220","RegOpenKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","REPARSE","Desired Access: Read","0.0000076"
13:20:42,9436217,"main.exe","15220","RegOpenKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS","Desired Access: Read","0.0000062"
13:20:42,9436408,"main.exe","15220","RegQueryValue","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\(Default)","SUCCESS","Type: REG_SZ, Length: 18, Data: 00060305","0.0000038"
13:20:42,9436499,"main.exe","15220","RegQueryValue","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\000603xx","SUCCESS","Type: REG_SZ, Length: 26, Data: kernel32.dll","0.0000022"
13:20:42,9437015,"main.exe","15220","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager","REPARSE","Desired Access: Query Value, Enumerate Sub Keys","0.0000032"
13:20:42,9437109,"main.exe","15220","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","Desired Access: Query Value, Enumerate Sub Keys","0.0000032"
13:20:42,9437195,"main.exe","15220","RegQueryValue","HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies","NAME NOT FOUND","Length: 24","0.0000024"
13:20:42,9437287,"main.exe","15220","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000013"
13:20:42,9438990,"main.exe","15220","QueryNameInformationFile","D:\Documents\C++\os_labs\2\src\build\main.exe","SUCCESS","Name: \Documents\C++\os_labs\2\src\build\main.exe","0.0000048"
13:20:42,9440234,"main.exe","15220","CreateFile","D:\Documents\C++\os_labs\2\src\build\data.txt","SUCCESS","Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Write, AllocationSize: 0, OpenResult: Created"
13:20:42,9442010,"main.exe","15220","Thread Create","","SUCCESS","Thread ID: 15172","0.0000000"
13:20:42,9442359,"main.exe","15220","Thread Create","","SUCCESS","Thread ID: 15900","0.0000000"
13:20:42,9442561,"main.exe","15220","Thread Create","","SUCCESS","Thread ID: 7968","0.0000000"
13:20:42,9443204,"main.exe","15220","Thread Exit","","SUCCESS","Thread ID: 15172, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"
13:20:42,9444375,"main.exe","15220","Thread Exit","","SUCCESS","Thread ID: 15900, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"
13:20:42,9444397,"main.exe","15220","Thread Exit","","SUCCESS","Thread ID: 7968, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"
13:20:42,9458324,"main.exe","15220","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened","0.0000133"
13:20:42,9458543,"main.exe","15220","QueryBasicInformationFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","CreationTime: 18.12.2023 14:57:47, LastAccessTime: 26.12.2024 13:20:39, LastWriteTime: 18.12.2023 14:57:47, ChangeTime: 11.12.2024 6:57:23, FileAttributes: A","0.0000024"
13:20:42,9458629,"main.exe","15220","CloseFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","","0.0000052"
13:20:42,9459567,"main.exe","15220","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Op
13:20:42,9459865,"main.exe","15220","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","FILE LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE","0.0000031"
13:20:42,9460031,"main.exe","15220","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","SUCCESS","SyncType: SyncTypeOther","0.0000011"
13:20:42,9461459,"main.exe","15220","Load Image","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Image Base: 0x7ffeccf0000, Image Size: 0x12000","0.0000000"
13:20:42,9462743,"main.exe","15220","Load Image","C:\Windows\System32\msvcrt.dll","SUCCESS","Image Base: 0x7ffed0d70000, Image Size: 0x9e000","0.0000000"
13:20:42,9464015,"main.exe","15220","Load Image","C:\Windows\System32\rpcrt4.dll","SUCCESS","Image Base: 0x7ffed0c40000, Image Size: 0x123000","0.0000000"
13:20:42,9465152,"main.exe","15220","CloseFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","","0.0000083"
13:20:42,9466196,"main.exe","15220","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager","REPARSE","Desired Access: Query Value, Enumerate Sub Keys","0.0000077"
13:20:42,9466343,"main.exe","15220","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","Desired Access: Query Value, Enumerate Sub Keys","0.0000044"
13:20:42,9466453,"main.exe","15220","RegQueryValue","HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies","NAME NOT FOUND","Length: 24","0.0000030"
13:20:42,9466554,"main.exe","15220","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000012"
13:20:42,9467323,"main.exe","15220","WriteFile","D:\Documents\C++\os_labs\2\src\build\data.txt","SUCCESS","Offset: 0, Length: 311, Priority: Normal","0.0000737"
13:20:42,9467530,"main.exe","15220","Thread Exit","","SUCCESS","Thread ID: 2156, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"
13:20:42,9468395,"main.exe","15220","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","BUFFER TOO SMALL","Length: 0","0.0000318"
13:20:42,9468778,"main.exe","15220","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","SUCCESS","Type: REG_BINARY, Length: 364, Data: 01 00 00 04 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00","0.0000237"
13:20:42,9469245,"main.exe","15220","Thread Exit","","SUCCESS","Thread ID: 15764, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"
13:20:42,9473176,"main.exe","15220","Process Exit","","SUCCESS","Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0000000 seconds, Private Bytes: 663 552, Peak Private Bytes: 663 552, Working Set: 4 182 016, Peak Working Set: 4 186 112","0.0000000"
13:20:42,9473315,"main.exe","15220","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","Desired Access: All Access","0.0000044"
13:20:42,9473431,"main.exe","15220","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001\\Device\HarddiskVolume2\Documents\C++\os_labs\2\src\build\main.exe","NAME NOT FOUND","Length: 40","0.0000076"
13:20:42,9473550,"main.exe","15220","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","","0.0000015"
13:20:42,9473772,"main.exe","15220","CloseFile","D:\Documents\C++\os_labs\2\src\build","SUCCESS","","0.0000058"
13:20:42,9474297,"main.exe","15220","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS","","0.0000016"
13:20:42,9475148,"main.exe","15220","CloseFile","D:\Documents\C++\os_labs\2\src\build\data.txt","SUCCESS","","0.0072266"

Систменые вызовы:

CreateThread - Создает поток для выполнения в виртуальном адресном пространстве вызывающего процесса.

Lab3



13:22:58,4032879,"main.exe","1852","RegCloseKey","HKCU","SUCCESS","","0.0000010"
13:22:58,4032956,"main.exe","1852","RegOpenKey","HKLM\Software\Policies\Microsoft\MUI\Settings","NAME NOT FOUND","Desired Access: Read","0.0000031"
13:22:58,4033079,"main.exe","1852","RegOpenKey","HKCU","SUCCESS","Desired Access: Maximum Allowed, Granted Access: All Access","0.0000024"
13:22:58,4033151,"main.exe","1852","RegOpenKey","HKCU\Software\Policies\Microsoft\Control Panel\Desktop","NAME NOT FOUND","Desired Access: Read","0.0000023"
13:22:58,4033241,"main.exe","1852","RegOpenKey","HKCU\Control Panel\Desktop\LanguageConfiguration","NAME NOT FOUND","Desired Access: Read","0.0000020"
13:22:58,4033307,"main.exe","1852","RegCloseKey","HKCU","SUCCESS","","0.0000010"
13:22:58,4038949,"main.exe","1852","RegOpenKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","Desired Access: Query Value","0.0000092"
13:22:58,4039201,"main.exe","1852","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ, Length: 120, Data: C:\Users\MegaComp\AppData\Local\Microsoft\Windows\INetCache","0.0000043"
13:22:58,4039318,"main.exe","1852","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","","0.0000014"
13:22:58,4039424,"main.exe","1852","QuerySecurityFile","D:\Documents\C++\os_labs\3\src\build\child.exe","SUCCESS","Information: Owner, Group, DACL, SACL, Label, Attribute, Process Trust Label, 0x100","0.0000019"
13:22:58,4040346,"main.exe","1852","CreateFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, AllocationSize: n/a, OpenResult: Opened","0.0000178"
13:22:58,4040675,"main.exe","1852","QueryBasicInformationFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","CreationTime: 13.11.2024 19:43:28, LastAccessTime: 26.12.2024 13:22:58, LastWriteTime: 13.11.2024 19:43:28, ChangeTime: 13.11.2024 22:29:25, FileAttributes: A","0.0000020"
13:22:58,4040746,"main.exe","1852","CloseFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","","0.0000055"
13:22:58,4040974,"main.exe","1852","QueryBasicInformationFile","D:\Documents\C++\os_labs\3\src\build\child.exe","SUCCESS","CreationTime: 26.12.2024 13:22:32, LastAccessTime: 26.12.2024 13:22:58, LastWriteTime: 26.12.2024 13:22:33, ChangeTime: 26.12.2024 13:22:33, FileAttributes: A","0.0000011"
13:22:58,4041456,"main.exe","1852","CloseFile","D:\Documents\C++\os_labs\3\src\build\child.exe","SUCCESS","","0.0000056"
13:22:58,4318701,"main.exe","1852","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened","0.0000122"
13:22:58,4318917,"main.exe","1852","QueryBasicInformationFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","CreationTime: 18.12.2023 14:57:47, LastAccessTime: 26.12.2024 13:22:58, LastWriteTime: 18.12.2023 14:57:47, ChangeTime: 11.12.2024 6:57:23, FileAttributes: A","0.0000022"
13:22:58,4319004,"main.exe","1852","CloseFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","","0.0000055"
13:22:58,4320309,"main.exe","1852","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Oper
13:22:58,4320628,"main.exe","1852","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","FILE LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE","0.0000029"
13:22:58,4320803,"main.exe","1852","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","SUCCESS","SyncType: SyncTypeOther","0.0000012"
13:22:58,4321791,"main.exe","1852","Load Image","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Image Base: 0x7ffeccf0000, Image Size: 0x12000","0.0000000"
13:22:58,4323223,"main.exe","1852","Load Image","C:\Windows\System32\msvcrt.dll","SUCCESS","Image Base: 0x7ffed0d70000, Image Size: 0x9e000","0.0000000"
13:22:58,4324226,"main.exe","1852","CloseFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","","0.0000084"
13:22:58,4325408,"main.exe","1852","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager","REPARSE","Desired Access: Query Value, Enumerate Sub Keys","0.0000053"
13:22:58,4325531,"main.exe","1852","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","Desired Access: Query Value, Enumerate Sub Keys","0.0000043"
13:22:58,4325636,"main.exe","1852","RegQueryValue","HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies","NAME NOT FOUND","Length: 24","0.0000026"
13:22:58,4325724,"main.exe","1852","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000012"
13:22:58,4326313,"main.exe","1852","Thread Exit","","SUCCESS","Thread ID: 16256, User Time: 0.0000000, Kernel Time: 0.0156250","0.0000000"
13:22:58,4326371,"main.exe","1852","Thread Exit","","SUCCESS","Thread ID: 3972, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"
13:22:58,4326493,"main.exe","1852","Thread Exit","","SUCCESS","Thread ID: 2404, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"
13:22:58,4327241,"main.exe","1852","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","BUFFER TOO SMALL","Length: 0","0.0000329"
13:22:58,4327682,"main.exe","1852","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","SUCCESS","Type: REG_BINARY, Length: 364, Data: 01 00 04 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00","0.0000245"
13:22:58,4328198,"main.exe","1852","Thread Exit","","SUCCESS","Thread ID: 2848, User Time: 0.0156250, Kernel Time: 0.0312500","0.0000000"
13:22:58,4329970,"main.exe","1852","Process Exit","","SUCCESS","Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: 1 036 288, Peak Private Bytes: 1 036 288, Working Set: 5 087 232, Peak Working Set: 5 091 328","0.0000000"
13:22:58,4330147,"main.exe","1852","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","Desired Access: All Access","0.0000049"
13:22:58,4330327,"main.exe","1852","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001\\Device\HarddiskVolume2\Documents\C++\os_labs\3\src\build\main.exe","NAME NOT FOUND","Length: 40","0.0000070"
13:22:58,4330444,"main.exe","1852","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","","0.0000016"
13:22:58,4330677,"main.exe","1852","CloseFile","D:\Documents\C++\os_labs\3\src\build","SUCCESS","","0.0000069"
13:22:58,4331085,"main.exe","1852","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000013"
13:22:58,4331136,"main.exe","1852","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS","","0.0000010"
13:22:58,4331214,"main.exe","1852","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options","SUCCESS","","0.0000009"
13:22:58,4331255,"main.exe","1852","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion","SUCCESS","","0.0000013"

Системные вызовы:

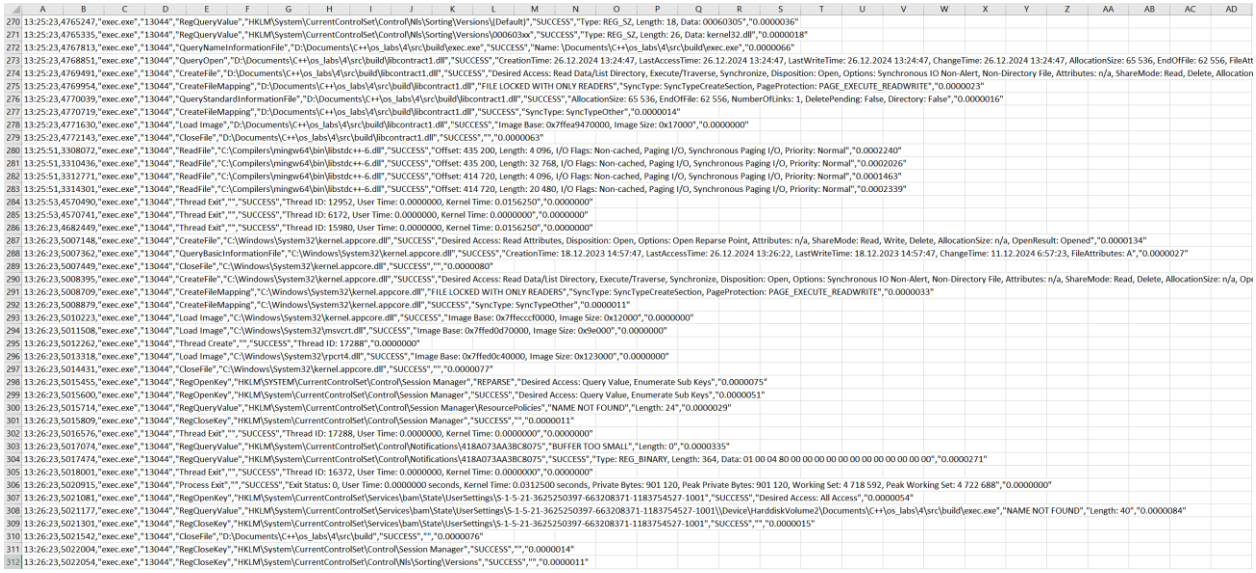
CreateFile - Создает или открывает файл или устройство ввода-вывода.
CreateProcess - Создает новый процесс и его основной поток.
CreateFileMapping - Создает или открывает именованный или неименованный объект сопоставления файлов для указанного файла.

MapViewOfFile - Сопоставляет представление сопоставления файлов в адресное пространство вызывающего процесса.

ReadFile - Считывает данные из указанного файла или устройства ввода-вывода (ввода-вывода).

UnmapViewOfFile - Отменяет сопоставление сопоставленного представления файла из адресного пространства вызывающего процесса.

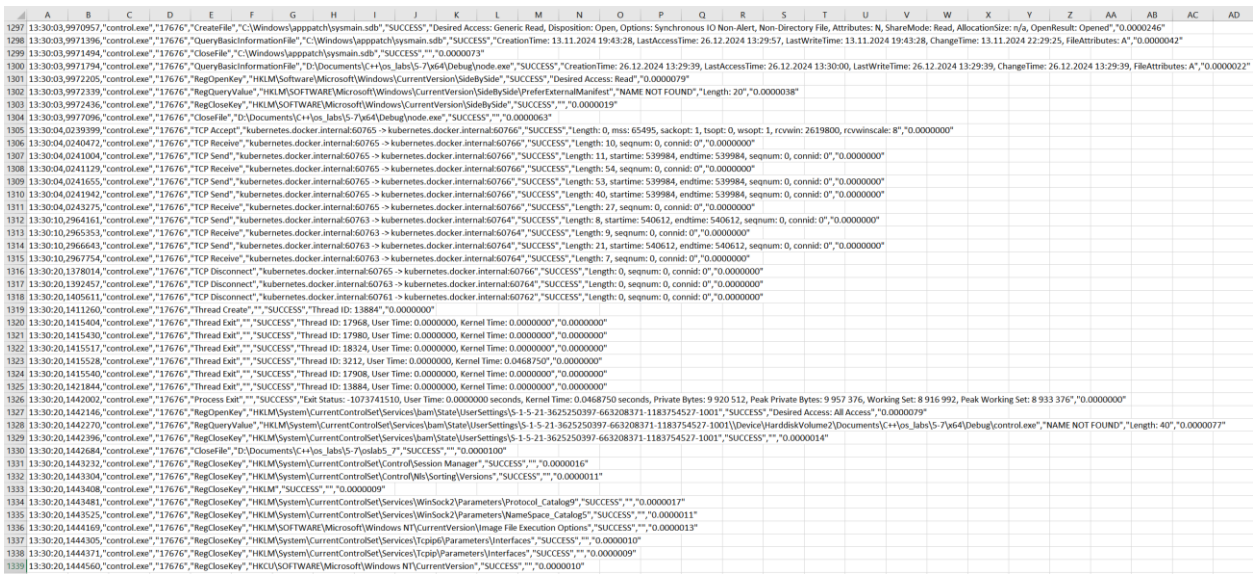
Lab4



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD
270	13:25:23,4765247,"exec.exe","13044","RegQueryValue","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\(Default)","SUCCESS","Type: REG_SZ, Length: 18, Data: 00060305","0.0000036"																												
271	13:25:23,4765335,"exec.exe","13044","RegQueryValue","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\000603xx","SUCCESS","Type: REG_SZ, Length: 26, Data: kernel32.dll","0.0000018"																												
272	13:25:23,4767813,"exec.exe","13044","QueryNameInformationFile","D:\Documents\C++\os_labs\4\src\build\exec.exe","SUCCESS","Name: \Documents\C++\os_labs\4\src\build\exec.exe","0.0000066"																												
273	13:25:23,4768851,"exec.exe","13044","QueryOpen","D:\Documents\C++\os_labs\4\src\build\libcontract1.dll","SUCCESS","CreationTime: 26.12.2024 13:24:47, LastAccessTime: 26.12.2024 13:24:47, LastWriteTime: 26.12.2024 13:24:47, ChangeTime: 26.12.2024 13:24:47, AllocationSize: 65 536, EndOfFile: 62 556, FileAtt																												
274	13:25:23,4769491,"exec.exe","13044","CreateFile","D:\Documents\C++\os_labs\4\src\build\libcontract1.dll","SUCCESS","Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, Allocation																												
275	13:25:23,4769954,"exec.exe","13044","CreateFileMapping","D:\Documents\C++\os_labs\4\src\build\libcontract1.dll","FILE LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE","0.0000023"																												
276	13:25:23,4770039,"exec.exe","13044","QueryStandardInformationFile","D:\Documents\C++\os_labs\4\src\build\libcontract1.dll","SUCCESS","AllocationSize: 65 536, EndOfFile: 62 556, NumberOfLinks: 1, DeletePending: False, Directory: False","0.0000016"																												
277	13:25:23,4770719,"exec.exe","13044","CreateFileMapping","D:\Documents\C++\os_labs\4\src\build\libcontract1.dll","SUCCESS","SyncType: SyncTypeOther","0.0000014"																												
278	13:25:23,4771630,"exec.exe","13044","Load Image","D:\Documents\C++\os_labs\4\src\build\libcontract1.dll","SUCCESS","Image Base: 0x7ffea9470000, Image Size: 0x17000","0.0000000"																												
279	13:25:23,4772143,"exec.exe","13044","CloseFile","D:\Documents\C++\os_labs\4\src\build\libcontract1.dll","SUCCESS","","0.0000063"																												
280	13:25:51,3308072,"exec.exe","13044","ReadFile","C:\Compilers\mingw64\bin\libstdc++-6.dll","SUCCESS","Offset: 435 200, Length: 4 096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal","0.0002240"																												
281	13:25:51,3310436,"exec.exe","13044","ReadFile","C:\Compilers\mingw64\bin\libstdc++-6.dll","SUCCESS","Offset: 435 200, Length: 32 768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal","0.0002026"																												
282	13:25:51,3312771,"exec.exe","13044","ReadFile","C:\Compilers\mingw64\bin\libstdc++-6.dll","SUCCESS","Offset: 414 720, Length: 4 096, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal","0.0001463"																												
283	13:25:51,3314301,"exec.exe","13044","ReadFile","C:\Compilers\mingw64\bin\libstdc++-6.dll","SUCCESS","Offset: 414 720, Length: 20 480, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal","0.0002339"																												
284	13:25:53,4570490,"exec.exe","13044","Thread Exit","","SUCCESS","Thread ID: 12952, User Time: 0.0000000, Kernel Time: 0.0156250","0.0000000"																												
285	13:25:53,4570741,"exec.exe","13044","Thread Exit","","SUCCESS","Thread ID: 6172, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
286	13:26:23,4682449,"exec.exe","13044","Thread Exit","","SUCCESS","Thread ID: 15980, User Time: 0.0000000, Kernel Time: 0.0156250","0.0000000"																												
287	13:26:23,5007148,"exec.exe","13044","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened","0.0000134"																												
288	13:26:23,5007362,"exec.exe","13044","QueryBasicInformationFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","CreationTime: 18.12.2023 14:57:47, LastAccessTime: 26.12.2024 13:26:22, LastWriteTime: 18.12.2023 14:57:47, ChangeTime: 11.12.2024 6:57:23, FileAttributes: A","0.0000027"																												
289	13:26:23,5007449,"exec.exe","13044","CloseFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","","0.0000080"																												
290	13:26:23,5008395,"exec.exe","13044","CreateFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Desired Access: Read Data/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Op																												
291	13:26:23,5008709,"exec.exe","13044","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","FILE LOCKED WITH ONLY READERS","SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_READWRITE","0.0000033"																												
292	13:26:23,5008879,"exec.exe","13044","CreateFileMapping","C:\Windows\System32\kernel.appcore.dll","SUCCESS","SyncType: SyncTypeOther","0.0000011"																												
293	13:26:23,5010223,"exec.exe","13044","Load Image","C:\Windows\System32\kernel.appcore.dll","SUCCESS","Image Base: 0x7ffecccf0000, Image Size: 0x12000","0.0000000"																												
294	13:26:23,5011508,"exec.exe","13044","Load Image","C:\Windows\System32\msvcrt.dll","SUCCESS","Image Base: 0x7ffed0d70000, Image Size: 0x9e000","0.0000000"																												
295	13:26:23,5012262,"exec.exe","13044","Thread Create","","SUCCESS","Thread ID: 17288","0.0000000"																												
296	13:26:23,5013318,"exec.exe","13044","Load Image","C:\Windows\System32\vprt4.dll","SUCCESS","Image Base: 0x7ffed0c40000, Image Size: 0x123000","0.0000000"																												
297	13:26:23,5014431,"exec.exe","13044","CloseFile","C:\Windows\System32\kernel.appcore.dll","SUCCESS","","0.0000077"																												
298	13:26:23,5015455,"exec.exe","13044","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager","REPARSE","Desired Access: Query Value, Enumerate Sub Keys","0.0000075"																												
299	13:26:23,5015600,"exec.exe","13044","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","Desired Access: Query Value, Enumerate Sub Keys","0.0000051"																												
300	13:26:23,5015714,"exec.exe","13044","RegQueryValue","HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies","NAME NOT FOUND","Length: 24","0.0000029"																												
301	13:26:23,5015809,"exec.exe","13044","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000011"																												
302	13:26:23,5016576,"exec.exe","13044","Thread Exit","","SUCCESS","Thread ID: 17288, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
303	13:26:23,5017074,"exec.exe","13044","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","BUFFER TOO SMALL","Length: 0","0.0003335"																												
304	13:26:23,5017474,"exec.exe","13044","RegQueryValue","HKLM\System\CurrentControlSet\Control\Notifications\418A073AA3BC8075","SUCCESS","Type: REG_BINARY, Length: 364, Data: 01 00 04 80 00 00 00 00 00 00 00 00 00 00 00 00 00","0.0000271"																												
305	13:26:23,5018001,"exec.exe","13044","Thread Exit","","SUCCESS","Thread ID: 16372, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
306	13:26:23,5020915,"exec.exe","13044","Process Exit","","SUCCESS","Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0312500 seconds, Private Bytes: 901 120, Peak Private Bytes: 901 120, Working Set: 4 718 592, Peak Working Set: 4 722 688","0.0000000"																												
307	13:26:23,5021081,"exec.exe","13044","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","Desired Access: All Access","0.0000054"																												
308	13:26:23,5021177,"exec.exe","13044","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001\\Device\HarddiskVolume2\Documents\C++\os_labs\4\src\build\exec.exe","NAME NOT FOUND","Length: 40","0.0000084"																												
309	13:26:23,5021301,"exec.exe","13044","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","","0.0000015"																												
310	13:26:23,5021542,"exec.exe","13044","CloseFile","D:\Documents\C++\os_labs\4\src\build","SUCCESS","","0.0000076"																												
311	13:26:23,5022004,"exec.exe","13044","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000014"																												
312	13:26:23,5022054,"exec.exe","13044","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS","","0.0000011"																												

Системные вызовы:
LoadLibrary -Загружает указанный модуль в адресное пространство вызывающего процесса. Указанный модуль может привести к загрузке других модулей.
GetProcAddress - Извлекает адрес экспортируемой функции (также называемой процедурой) или переменной из указанной библиотеки динамической компоновки (DLL).

Lab5-7



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD
1297	13:30:03,9970957,"control.exe","17676","CreateFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, AllocationSize: n/a, OpenResult: Opened","0.0000246"																												
1298	13:30:03,9971396,"control.exe","17676","QueryBasicInformationFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","CreationTime: 13.11.2024 19:43:28, LastAccessTime: 26.12.2024 13:29:57, LastWriteTime: 13.11.2024 19:43:28, ChangeTime: 13.11.2024 22:29:25, FileAttributes: A","0.0000042"																												
1299	13:30:03,9971494,"control.exe","17676","CloseFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","","0.0000073"																												
1300	13:30:03,9971794,"control.exe","17676","QueryBasicInformationFile","D:\Documents\C++\os_labs\5-7\x64\Debug\node.exe","SUCCESS","CreationTime: 26.12.2024 13:29:39, LastAccessTime: 26.12.2024 13:30:00, LastWriteTime: 26.12.2024 13:29:39, ChangeTime: 26.12.2024 13:29:39, FileAttributes: A","0.0000022"																												
1301	13:30:03,9972205,"control.exe","17676","RegOpenKey","HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide","SUCCESS","Desired Access: Read","0.0000079"																												
1302	13:30:03,9972339,"control.exe","17676","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest","NAME NOT FOUND","Length: 20","0.0000038"																												
1303	13:30:03,9972436,"control.exe","17676","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide","SUCCESS","","0.0000019"																												
1304	13:30:03,9977096,"control.exe","17676","CloseFile","D:\Documents\C++\os_labs\5-7\x64\Debug\node.exe","SUCCESS","","0.0000063"																												
1305	13:30:04,0239399,"control.exe","17676","TCP Accept","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 0, mss: 65495, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 2619800, rcvwinscale: 8","0.0000000"																												
1306	13:30:04,0240472,"control.exe","17676","TCP Receive","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 10, seqnum: 0, connid: 0","0.0000000"																												
1307	13:30:04,0241004,"control.exe","17676","TCP Send","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 11, startime: 539984, endtime: 539984, seqnum: 0, connid: 0","0.0000000"																												
1308	13:30:04,0241129,"control.exe","17676","TCP Receive","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 54, seqnum: 0, connid: 0","0.0000000"																												
1309	13:30:04,0241655,"control.exe","17676","TCP Send","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 53, startime: 539984, endtime: 539984, seqnum: 0, connid: 0","0.0000000"																												
1310	13:30:04,0241942,"control.exe","17676","TCP Send","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 40, startime: 539984, endtime: 539984, seqnum: 0, connid: 0","0.0000000"																												
1311	13:30:04,0243275,"control.exe","17676","TCP Receive","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 27, seqnum: 0, connid: 0","0.0000000"																												
1312	13:30:10,2964161,"control.exe","17676","TCP Send","kubernetes.docker.internal:60763 -> kubernetes.docker.internal:60764","SUCCESS","Length: 8, startime: 540612, endtime: 540612, seqnum: 0, connid: 0","0.0000000"																												
1313	13:30:10,2965353,"control.exe","17676","TCP Receive","kubernetes.docker.internal:60763 -> kubernetes.docker.internal:60764","SUCCESS","Length: 9, seqnum: 0, connid: 0","0.0000000"																												
1314	13:30:10,2966643,"control.exe","17676","TCP Send","kubernetes.docker.internal:60763 -> kubernetes.docker.internal:60764","SUCCESS","Length: 21, startime: 540612, endtime: 540612, seqnum: 0, connid: 0","0.0000000"																												
1315	13:30:10,2967754,"control.exe","17676","TCP Receive","kubernetes.docker.internal:60763 -> kubernetes.docker.internal:60764","SUCCESS","Length: 7, seqnum: 0, connid: 0","0.0000000"																												
1316	13:30:20,1378014,"control.exe","17676","TCP Disconnect","kubernetes.docker.internal:60765 -> kubernetes.docker.internal:60766","SUCCESS","Length: 0, seqnum: 0, connid: 0","0.0000000"																												
1317	13:30:20,1392457,"control.exe","17676","TCP Disconnect","kubernetes.docker.internal:60763 -> kubernetes.docker.internal:60764","SUCCESS","Length: 0, seqnum: 0, connid: 0","0.0000000"																												
1318	13:30:20,1405611,"control.exe","17676","TCP Disconnect","kubernetes.docker.internal:60761 -> kubernetes.docker.internal:60762","SUCCESS","Length: 0, seqnum: 0, connid: 0","0.0000000"																												
1319	13:30:20,1411260,"control.exe","17676","Thread Create","","SUCCESS","Thread ID: 13884","0.0000000"																												
1320	13:30:20,1415404,"control.exe","17676","Thread Exit","","SUCCESS","Thread ID: 17968, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
1321	13:30:20,1415430,"control.exe","17676","Thread Exit","","SUCCESS","Thread ID: 17980, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
1322	13:30:20,1415517,"control.exe","17676","Thread Exit","","SUCCESS","Thread ID: 18324, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
1323	13:30:20,1415528,"control.exe","17676","Thread Exit","","SUCCESS","Thread ID: 3212, User Time: 0.0000000, Kernel Time: 0.0468750","0.0000000"																												
1324	13:30:20,1415540,"control.exe","17676","Thread Exit","","SUCCESS","Thread ID: 17908, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
1325	13:30:20,1421844,"control.exe","17676","Thread Exit","","SUCCESS","Thread ID: 13884, User Time: 0.0000000, Kernel Time: 0.0000000","0.0000000"																												
1326	13:30:20,1442002,"control.exe","17676","Process Exit","","SUCCESS","Exit Status: -1073741510, User Time: 0.0000000 seconds, Kernel Time: 0.0468750 seconds, Private Bytes: 9 920 512, Peak Private Bytes: 9 957 376, Working Set: 8 916 992, Peak Working Set: 8 933 376","0.0000000"																												
1327	13:30:20,1442146,"control.exe","17676","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","Desired Access: All Access","0.0000079"																												
1328	13:30:20,1442270,"control.exe","17676","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001\\Device\HarddiskVolume2\Documents\C++\os_labs\5-7\x64\Debug\control.exe","NAME NOT FOUND","Length: 40","0.0000077"																												
1329	13:30:20,1442396,"control.exe","17676","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3625250397-663208371-1183754527-1001","SUCCESS","","0.0000014"																												
1330	13:30:20,1442684,"control.exe","17676","CloseFile","D:\Documents\C++\os_labs\5-7\oslab5_7","SUCCESS","","0.0000100"																												
1331	13:30:20,1443232,"control.exe","17676","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","","0.0000016"																												
1332	13:30:20,1443304,"control.exe","17676","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS","","0.0000011"																												
1333	13:30:20,1443408,"control.exe","17676","RegCloseKey","HKLM","SUCCESS","","0.0000009"																												
1334	13:30:20,1443481,"control.exe","17676","RegCloseKey","HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9","SUCCESS","","0.0000017"																												
1335	13:30:20,1443525,"control.exe","17676","RegCloseKey","HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5","SUCCESS","","0.0000011"																												
1336	13:30:20,1444169,"control.exe","17676","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options","SUCCESS","","0.0000013"																												
1337	13:30:20,1444305,"control.exe","17676","RegCloseKey","HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces","SUCCESS","","0.0000010"																												
1338	13:30:20,1444371,"control.exe","17676","RegCloseKey","HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces","SUCCESS","","0.0000009"																												
1339	13:30:20,1444560,"control.exe","17676","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion","SUCCESS","","0.0000010"																												

Системные вызовы:

connect - Функция connect соединяет сокет с конечной точкой и затем принимает входящие соединения на этой конечной точке.

send - поставит в очередь на сокет часть сообщения, созданную из аргумента buffer.

recv - получает часть сообщения от сокета и сохранить его в аргументе buffer.

Выводы

Проделав работу, я приобрел практические навыки, необходимые для работы с утилитой Proccess Monitor, а также повторил все виды системных вызовов, использованных в лабораторных работах, сделанных в течение курса.