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: Тарасов Егор Дмитриевич
Группа: М8О-209Б-23
Вариант: 19
Преподаватель: Миронов Евгений Сергеевич
Оценка: _____
Дата: _____
Подпись: _____

Москва, 2024

Содержание

- Репозиторий
- Постановка задачи
- Демонстрация работы программы
- Выводы

Репозиторий

https://github.com/EgorTarasov1/mai-os-labs

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.

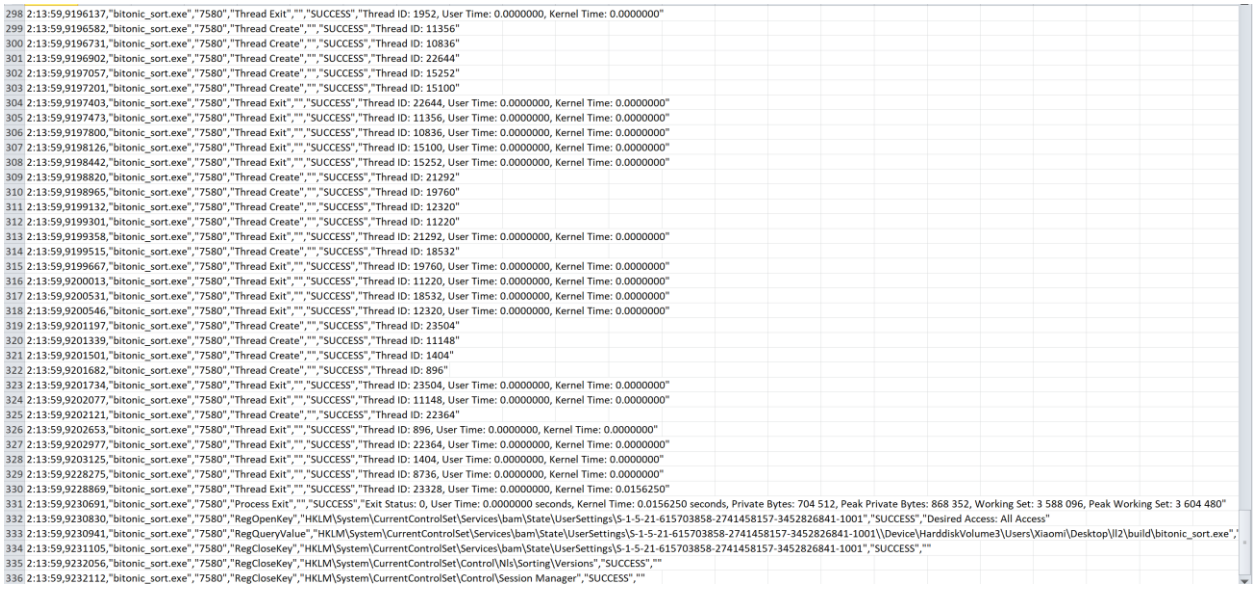
Выполнение задания

Lab1

```
1:56:38,0884634,"parent.exe","8608","CreateFileMapping","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","SyncType: SyncTypeOther"
1:56:38,0885365,"parent.exe","8608","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\child2.exe","NAME NOT FOUND","Desired Access: Query Value, Enumerate Sub Keys"
1:56:38,0885654,"parent.exe","8608","QuerySecurityFile","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","Information: Label"
1:56:38,0886272,"parent.exe","8608","QueryNameInformationFile","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","Name: \Users\Xiaomi\Desktop\ll1\build\child2.exe"
1:56:38,0910537,"parent.exe","8608","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS","Desired Access: All Access"
1:56:38,0910683,"parent.exe","8608","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001\\Device\HarddiskVolume3\Users\Xiaomi\Desktop\ll1\build\child2.exe","NAME NOT FOUND","Length: 40"
1:56:38,0910886,"parent.exe","8608","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS",""
1:56:38,0910981,"parent.exe","8608","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM","REPARSE","Desired Access: Query Value"
1:56:38,0911083,"parent.exe","8608","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager\BAM","NAME NOT FOUND","Desired Access: Query Value"
1:56:38,0911396,"parent.exe","8608","Process Create","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","PID: 12272, Command line: child2.exe ""C:\Users\Xiaomi\Desktop\ll1\second.txt"""
1:56:38,0911807,"parent.exe","8608","RegOpenKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","Desired Access: Query Value"
1:56:38,0911946,"parent.exe","8608","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ, Length: 116, Data: C:\Users\Xiaomi\AppData\Local\Microsoft\Windows\INetCache"
1:56:38,0912057,"parent.exe","8608","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS",""
1:56:38,0912130,"parent.exe","8608","RegOpenKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Query Value"
1:56:38,0912233,"parent.exe","8608","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","NAME NOT FOUND","Length: 16"
1:56:38,0912318,"parent.exe","8608","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
1:56:38,0912452,"parent.exe","8608","QuerySecurityFile","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","Information: Owner, Group, DACL, SACL, Label, Attribute, Process Trust Label, 0x100"
1:56:38,0913302,"parent.exe","8608","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"
1:56:38,0913671,"parent.exe","8608","QueryBasicInformationFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","CreationTime: 12.11.2024 22:20:25, LastAccessTime: 28.12.2024 1:56:00, LastWriteTime: 12.11.2024 22:20:25, ChangeTime: 13.11.2024 0:30:43, FileAttributes: A"
1:56:38,0913731,"parent.exe","8608","CloseFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS",""
1:56:38,0913943,"parent.exe","8608","QueryBasicInformationFile","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","CreationTime: 04.10.2024 10:55:39, LastAccessTime: 28.12.2024 1:53:36, LastWriteTime: 04.10.2024 11:05:10, ChangeTime: 04.10.2024 11:05:10, FileAttributes: A"
1:56:38,0914357,"parent.exe","8608","RegOpenKey","HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide","SUCCESS","Desired Access: Read"
1:56:38,0914475,"parent.exe","8608","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest","NAME NOT FOUND","Length: 20"
1:56:38,0914560,"parent.exe","8608","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide","SUCCESS",""
1:56:38,0918259,"parent.exe","8608","RegOpenKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","Desired Access: Query Value"
1:56:38,0918406,"parent.exe","8608","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ, Length: 116, Data: C:\Users\Xiaomi\AppData\Local\Microsoft\Windows\INetCache"
1:56:38,0918606,"parent.exe","8608","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS",""
1:56:38,0918745,"parent.exe","8608","QuerySecurityFile","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","Information: Owner, Group, DACL, SACL, Label, Attribute, Process Trust Label, 0x100"
1:56:38,0919641,"parent.exe","8608","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"
1:56:38,0920022,"parent.exe","8608","QueryBasicInformationFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS","CreationTime: 12.11.2024 22:20:25, LastAccessTime: 28.12.2024 1:56:00, LastWriteTime: 12.11.2024 22:20:25, ChangeTime: 13.11.2024 0:30:43, FileAttributes: A"
1:56:38,0920091,"parent.exe","8608","CloseFile","C:\Windows\apppatch\sysmain.sdb","SUCCESS",""
1:56:38,0920602,"parent.exe","8608","QueryBasicInformationFile","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS","CreationTime: 04.10.2024 10:55:39, LastAccessTime: 28.12.2024 1:53:36, LastWriteTime: 04.10.2024 11:05:10, ChangeTime: 04.10.2024 11:05:10, FileAttributes: A"
1:56:38,0921092,"parent.exe","8608","CloseFile","C:\Users\Xiaomi\Desktop\ll1\build\child2.exe","SUCCESS",""
1:56:51,9123914,"parent.exe","8608","Thread Create","","SUCCESS","Thread ID: 13560"
1:56:51,9125845,"parent.exe","8608","Thread Exit","","SUCCESS","Thread ID: 940, User Time: 0.0000000, Kernel Time: 0.0000000"
1:56:51,9125987,"parent.exe","8608","Thread Exit","","SUCCESS","Thread ID: 12580, User Time: 0.0000000, Kernel Time: 0.0000000"
1:56:51,9126000,"parent.exe","8608","Thread Exit","","SUCCESS","Thread ID: 2764, User Time: 0.0000000, Kernel Time: 0.0000000"
1:56:51,9127001,"parent.exe","8608","Thread Exit","","SUCCESS","Thread ID: 13560, User Time: 0.0000000, Kernel Time: 0.0000000"
1:56:51,9131279,"parent.exe","8608","Process Exit","","SUCCESS","Exit Status: -1073741510, User Time: 0.0000000 seconds, Kernel Time: 0.0000000 seconds, Private Bytes: 860 160, Peak Private Bytes: 868 352, Working Set: 3 899 392, Peak Working Set: 3 903 488"
1:56:51,9131436,"parent.exe","8608","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS","Desired Access: All Access"
1:56:51,9131531,"parent.exe","8608","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001\\Device\HarddiskVolume3\Users\Xiaomi\Desktop\ll1\build\parent.exe","NAME NOT FOUND","Length: 40"
1:56:51,9131635,"parent.exe","8608","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS",""
1:56:51,9131933,"parent.exe","8608","CloseFile","C:\Users\Xiaomi\Desktop\ll1\build","SUCCESS",""
1:56:51,9132511,"parent.exe","8608","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS",""
1:56:51,9132682,"parent.exe","8608","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options","SUCCESS",""
1:56:51,9132786,"parent.exe","8608","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion","SUCCESS",""
```

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



```
2:13:59,9196137,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 1952, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9196582,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 11356"
2:13:59,9196731,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 10836"
2:13:59,9196902,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 22644"
2:13:59,9197057,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 15252"
2:13:59,9197201,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 15100"
2:13:59,9197403,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 22644, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9197473,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 11356, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9197800,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 10836, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9198126,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 15100, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9198442,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 15252, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9198820,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 21292"
2:13:59,9198965,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 19760"
2:13:59,9199132,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 12320"
2:13:59,9199301,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 11220"
2:13:59,9199358,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 21292, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9199515,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 18532"
2:13:59,9199667,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 19760, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9200013,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 11220, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9200531,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 18532, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9200546,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 12320, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9201197,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 23504"
2:13:59,9201339,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 11148"
2:13:59,9201501,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 1404"
2:13:59,9201682,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 896"
2:13:59,9201734,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 23504, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9202077,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 11148, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9202121,"bitonic_sort.exe","7580","Thread Create","","SUCCESS","Thread ID: 22364"
2:13:59,9202653,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 896, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9202977,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 22364, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9203125,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 1404, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9228275,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 8736, User Time: 0.0000000, Kernel Time: 0.0000000"
2:13:59,9228869,"bitonic_sort.exe","7580","Thread Exit","","SUCCESS","Thread ID: 23328, User Time: 0.0000000, Kernel Time: 0.0156250"
2:13:59,9230691,"bitonic_sort.exe","7580","Process Exit","","SUCCESS","Exit Status: 0, User Time: 0.0000000 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 704 512, Peak Private Bytes: 868 352, Working Set: 3 588 096, Peak Working Set: 3 604 480"
2:13:59,9230830,"bitonic_sort.exe","7580","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS","Desired Access: All Access"
2:13:59,9230941,"bitonic_sort.exe","7580","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001\\Device\HarddiskVolume3\Users\Xiaomi\Desktop\lI2\build\bitonic_sort.exe","
2:13:59,9231105,"bitonic_sort.exe","7580","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS",""
2:13:59,9232056,"bitonic_sort.exe","7580","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS",""
2:13:59,9232112,"bitonic_sort.exe","7580","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS",""
```

Систменые вызовы:

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

Lab3

```
2:04:41,7306517,"parent.exe","11648","RegCloseKey","HKCU","SUCCESS",""
2:04:41,7306568,"parent.exe","11648","RegOpenKey","HKLM\Software\Policies\Microsoft\MUI\Settings","NAME NOT FOUND","Desired Access: Read"
2:04:41,7306631,"parent.exe","11648","RegOpenKey","HKCU","SUCCESS","Desired Access: Maximum Allowed, Granted Access: All Access"
2:04:41,7306691,"parent.exe","11648","RegOpenKey","HKCU\Control Panel\Desktop\MuiCached","SUCCESS","Desired Access: Read"
2:04:41,7306751,"parent.exe","11648","RegQueryValue","HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages","BUFFER OVERFLOW","Length: 12"
2:04:41,7306832,"parent.exe","11648","RegQueryValue","HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages","SUCCESS","Type: REG_MULTI_SZ, Length: 12, Data: ru-RU"
2:04:41,7306899,"parent.exe","11648","RegCloseKey","HKCU\Control Panel\Desktop\MuiCached","SUCCESS",""
2:04:41,7306947,"parent.exe","11648","RegCloseKey","HKCU","SUCCESS",""
2:04:41,7309611,"parent.exe","11648","RegOpenKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","Desired Access: Query Value"
2:04:41,7309715,"parent.exe","11648","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ, Length: 116, Data: C:\Users\Xiaomi\AppData\Local\Microsoft\Windows\INetCache"
2:04:41,7309808,"parent.exe","11648","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS",""
2:04:41,7316961,"parent.exe","11648","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\child2.exe","NAME NOT FOUND","Desired Access: Query Value, Enumerate Sub Keys"
2:04:41,7317073,"parent.exe","11648","RegOpenKey","HKLM\Software\Microsoft\Wow64\x86\xtajit","NAME NOT FOUND","Desired Access: Query Value"
2:04:41,7650827,"parent.exe","11648","RegOpenKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\child2.exe","NAME NOT FOUND","Desired Access: Query Value, Enumerate Sub Keys"
2:04:41,7677495,"parent.exe","11648","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS","Desired Access: All Access"
2:04:41,7677713,"parent.exe","11648","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001\\Device\HarddiskVolume3\Users\Xiaomi\Desktop\lI3\build\child2.exe","NAME NOT FOUND","Length: 40"
2:04:41,7677918,"parent.exe","11648","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS",""
2:04:41,7678028,"parent.exe","11648","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM","REPARSE","Desired Access: Query Value"
2:04:41,7678137,"parent.exe","11648","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager\BAM","NAME NOT FOUND","Desired Access: Query Value"
2:04:41,7678533,"parent.exe","11648","Process Create","C:\Users\Xiaomi\Desktop\lI3\build\child2.exe","SUCCESS","PID: 3888, Command line: child2.exe ""C:\Users\Xiaomi\Desktop\lI3\second.txt"""
2:04:41,7679084,"parent.exe","11648","RegOpenKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","Desired Access: Query Value"
2:04:41,7679257,"parent.exe","11648","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ, Length: 116, Data: C:\Users\Xiaomi\AppData\Local\Microsoft\Windows\INetCache"
2:04:41,7679368,"parent.exe","11648","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS",""
2:04:41,7679440,"parent.exe","11648","RegOpenKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS","Desired Access: Query Value"
2:04:41,7679530,"parent.exe","11648","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\Xiaomi\Desktop\lI3\build\child2.exe","NAME NOT FOUND","Length: 16"
2:04:41,7679596,"parent.exe","11648","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers","SUCCESS",""
2:04:41,7682600,"parent.exe","11648","RegOpenKey","HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide","SUCCESS","Desired Access: Read"
2:04:41,7682726,"parent.exe","11648","RegQueryValue","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest","NAME NOT FOUND","Length: 20"
2:04:41,7682812,"parent.exe","11648","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide","SUCCESS",""
2:04:41,7685112,"parent.exe","11648","RegOpenKey","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS","Desired Access: Query Value"
2:04:41,7685223,"parent.exe","11648","RegQueryValue","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache","SUCCESS","Type: REG_SZ, Length: 116, Data: C:\Users\Xiaomi\AppData\Local\Microsoft\Windows\INetCache"
2:04:41,7685322,"parent.exe","11648","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders","SUCCESS",""
2:04:55,8032787,"parent.exe","11648","Thread Create","","SUCCESS","Thread ID: 17288"
2:04:55,8035700,"parent.exe","11648","Thread Exit","","SUCCESS","Thread ID: 2888, User Time: 0.0000000, Kernel Time: 0.0000000"
2:04:55,8035737,"parent.exe","11648","Thread Exit","","SUCCESS","Thread ID: 9032, User Time: 0.0000000, Kernel Time: 0.0000000"
2:04:55,8035823,"parent.exe","11648","Thread Exit","","SUCCESS","Thread ID: 17364, User Time: 0.0000000, Kernel Time: 0.0156250"
2:04:55,8037795,"parent.exe","11648","Thread Exit","","SUCCESS","Thread ID: 17288, User Time: 0.0000000, Kernel Time: 0.0000000"
2:04:55,8042124,"parent.exe","11648","Process Exit","","SUCCESS","Exit Status: -1073741510, User Time: 0.0000000 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 847 872, Peak Private Bytes: 856 064, Working Set: 4 042 752, Peak Working Set: 4 046 848"
2:04:55,8042755,"parent.exe","11648","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS","Desired Access: All Access"
2:04:55,8043088,"parent.exe","11648","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001\\Device\HarddiskVolume3\Users\Xiaomi\Desktop\lI3\build\parent.exe","NAME NOT FOUND","Length: 40"
2:04:55,8043522,"parent.exe","11648","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS",""
2:04:55,8046111,"parent.exe","11648","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS",""
2:04:55,8046360,"parent.exe","11648","RegCloseKey","HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options","SUCCESS",""
2:04:55,8047617,"parent.exe","11648","RegCloseKey","HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion","SUCCESS",""
```

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

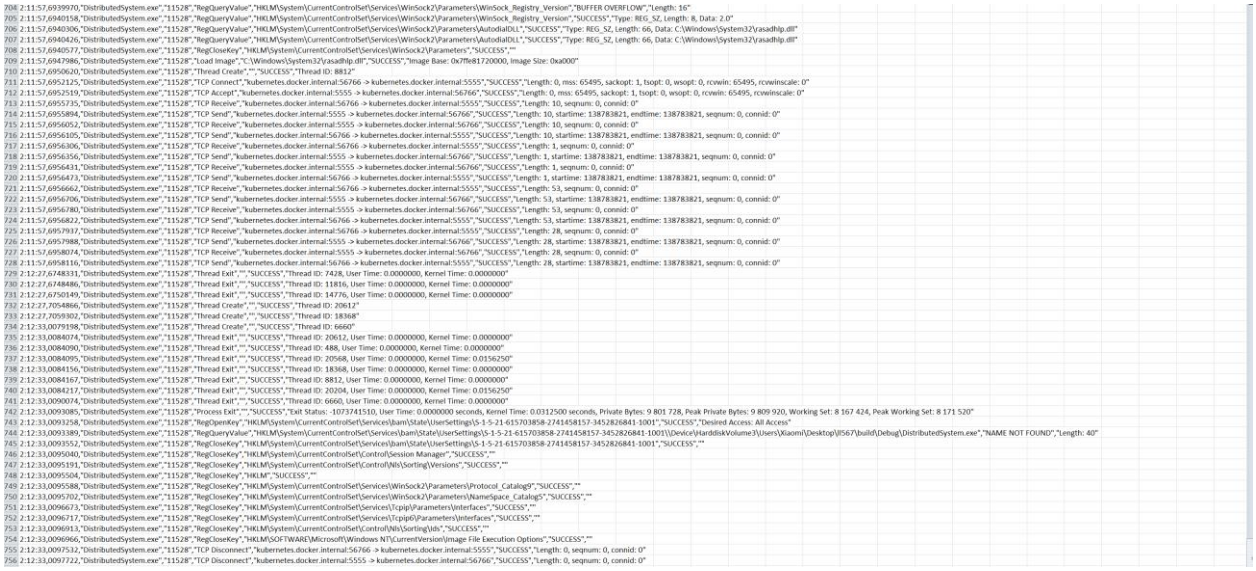
```
2:09:56,5235035,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys","REPARSE","Desired Access: Read"
2:09:56,5235202,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys","NAME NOT FOUND","Desired Access: Read"
2:09:56,5235646,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\WMI\Security\05f95efe-7f75-49c7-a994-60a55cc09571","NAME NOT FOUND","Length: 528"
2:09:56,5236359,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Terminal Server","REPARSE","Desired Access: Read"
2:09:56,5236445,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Terminal Server","SUCCESS","Desired Access: Read"
2:09:56,5236543,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat","NAME NOT FOUND","Length: 548"
2:09:56,5236604,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled","SUCCESS","Type: REG_DWORD, Length: 4, Data: 0"
2:09:56,5236683,"program2.exe","21104","RegCloseKey","HKLM\System\CurrentControlSet\Control\Terminal Server","SUCCESS",""
2:09:56,5236880,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\WMI\Security\e36c4458-ed80-4ad7-a8be-52dda1eb5f1c","NAME NOT FOUND","Length: 528"
2:09:56,5238122,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\SafeBoot\Option","REPARSE","Desired Access: Query Value, Set Value"
2:09:56,5238187,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\SafeBoot\Option","NAME NOT FOUND","Desired Access: Query Value, Set Value"
2:09:56,5238269,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Srp\GP\DLL","REPARSE","Desired Access: Read"
2:09:56,5238331,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Srp\GP\DLL","NAME NOT FOUND","Desired Access: Read"
2:09:56,5238412,"program2.exe","21104","RegOpenKey","HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers","SUCCESS","Desired Access: Query Value"
2:09:56,5238528,"program2.exe","21104","RegQueryValue","HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled","NAME NOT FOUND","Length: 80"
2:09:56,5238603,"program2.exe","21104","RegCloseKey","HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers","SUCCESS",""
2:09:56,5238693,"program2.exe","21104","RegOpenKey","HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers","NAME NOT FOUND","Desired Access: Query Value"
2:09:56,5238853,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\FileSystem\","REPARSE","Desired Access: Read"
2:09:56,5238943,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\FileSystem","SUCCESS","Desired Access: Read"
2:09:56,5239009,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\FileSystem\LongPathsEnabled","SUCCESS","Type: REG_DWORD, Length: 4, Data: 0"
2:09:56,5239089,"program2.exe","21104","RegCloseKey","HKLM\System\CurrentControlSet\Control\FileSystem","SUCCESS",""
2:09:56,5241479,"program2.exe","21104","Load Image","C:\Windows\System32\msvcrt.dll","SUCCESS","Image Base: 0x7ffe8d490000, Image Size: 0x9e000"
2:09:56,5242740,"program2.exe","21104","Thread Create","","SUCCESS","Thread ID: 22580"
2:09:56,5245313,"program2.exe","21104","RegOpenKey","HKLM\SYSTEM\CurrentControlSet\Control\Session Manager","REPARSE","Desired Access: Query Value, Enumerate Sub Keys"
2:09:56,5245441,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","Desired Access: Query Value, Enumerate Sub Keys"
2:09:56,5245566,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies","NAME NOT FOUND","Length: 24"
2:09:56,5245722,"program2.exe","21104","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS",""
2:09:56,5246453,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","REPARSE","Desired Access: Read"
2:09:56,5246557,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS","Desired Access: Read"
2:09:56,5246738,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\(Default)","SUCCESS","Type: REG_SZ, Length: 18, Data: 00060305"
2:09:56,5246842,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\000603xx","SUCCESS","Type: REG_SZ, Length: 26, Data: kernel32.dll"
2:09:56,5249266,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","REPARSE","Desired Access: Query Value"
2:09:56,5249379,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS","Desired Access: Query Value"
2:09:56,5249491,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode","SUCCESS","Type: REG_DWORD, Length: 4, Data: 1"
2:09:56,5255958,"program2.exe","21104","Load Image","C:\Users\Xiaomi\Desktop\ll4\build\bin\liblibrary1.dll","SUCCESS","Image Base: 0x7ffe86170000, Image Size: 0x15000"
2:09:58,1514593,"program2.exe","21104","Load Image","C:\Users\Xiaomi\Desktop\ll4\build\bin\liblibrary2.dll","SUCCESS","Image Base: 0x7ffe11dc0000, Image Size: 0x2ab000"
2:10:06,5630029,"program2.exe","21104","Thread Create","","SUCCESS","Thread ID: 11696"
2:10:06,5633161,"program2.exe","21104","Thread Exit","","SUCCESS","Thread ID: 22580, User Time: 0.0000000, Kernel Time: 0.0000000"
2:10:06,5633408,"program2.exe","21104","Thread Exit","","SUCCESS","Thread ID: 22112, User Time: 0.0000000, Kernel Time: 0.0000000"
2:10:06,5633965,"program2.exe","21104","Thread Exit","","SUCCESS","Thread ID: 11696, User Time: 0.0000000, Kernel Time: 0.0000000"
2:10:06,5637280,"program2.exe","21104","Process Exit","","SUCCESS","Exit Status: -1073741510, User Time: 0.0000000 seconds, Kernel Time: 0.0000000 seconds, Private Bytes: 798 720, Peak Private Bytes: 798 720, Working Set: 3 518 464, Peak Working Set: 3 522 560"
2:10:06,5637759,"program2.exe","21104","RegOpenKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS","Desired Access: All Access"
2:10:06,5638064,"program2.exe","21104","RegQueryValue","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001\\Device\HarddiskVolume3\Users\Xiaomi\Desktop\ll4\build\bin\program2.exe","NAME NOT FOUND","Length: 40"
2:10:06,5638434,"program2.exe","21104","RegCloseKey","HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-615703858-2741458157-3452826841-1001","SUCCESS",""
2:10:06,5640489,"program2.exe","21104","RegCloseKey","HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions","SUCCESS",""
2:10:06,5640594,"program2.exe","21104","RegCloseKey","HKLM\System\CurrentControlSet\Control\Session Manager","SUCCESS",""
```

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



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.