Московский Авиационный Институт

(Национальный Исследовательский Университет)

Институт №8 “Компьютерные науки и прикладная математика”

Кафедра №806 “Вычислительная математика и программирование”

# Лабораторная работа №3 по курсу
# «Операционные системы»

Группа: М8О-213Б-23

Студент: Черников В.В.

Преподаватель: Бахарев В.Д.

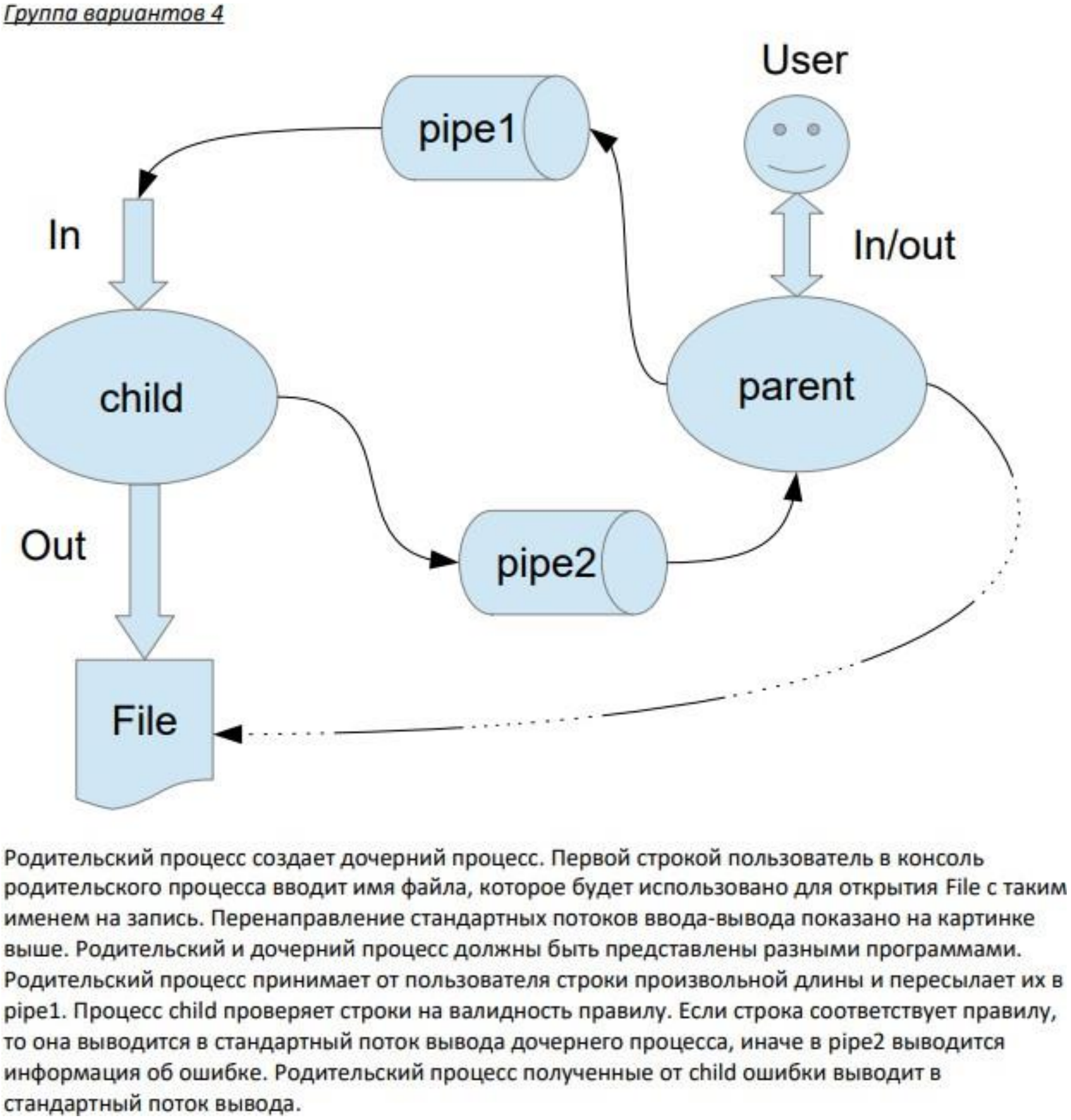
Оценка: ____________________

Дата: 25.11.24

Москва, 2024

# Постановка задачи

**Вариант 15.**



*Группа вариантов 4*

Родительский процесс создает дочерний процесс. Первой строкой пользователь в консоль родительского процесса вводит имя файла, которое будет использовано для открытия File с таким именем на запись. Перенаправление стандартных потоков ввода-вывода показано на картинке выше. Родительский и дочерний процесс должны быть представлены разными программами. Родительский процесс принимает от пользователя строки произвольной длины и пересылает их в pipe1. Процесс child проверяет строки на валидность правилу. Если строка соответствует правилу, то она выводится в стандартный поток вывода дочернего процесса, иначе в pipe2 выводится информация об ошибке. Родительский процесс полученные от child ошибки выводит в стандартный поток вывода.

Правило проверки: строка должна начинаться с заглавной буквы. Также вместо каналов необходимо использовать shared memory.

# Общий метод и алгоритм решения

**Использованные системные вызовы:**

- **GetStdHandle** — используется для получения дескрипторов стандартных потоков ввода и вывода;
- **WriteConsole** — выводит строки в консоль, заменяя стандартный printf. Используется для вывода сообщений, считанных строк и ошибок;
- **CloseHandle** — закрывает дескрипторы объекта;
- **SetConsoleCtrlHandler** — регистрирует обработчик для обработки событий

консоли (например, нажатия Ctrl+C). В данном случае используется для завершения дочернего процесса корректно при прерывании программы;

- **CreateProcess** — создает новый процесс и его основной поток; используется для запуска дочернего процесса;
- **CreateFile** — открывает или создает файл для записи данных, введенных пользователем. Используется для сохранения строк в файл;
- **TerminateProcess и WaitForSingleObject** — завершают и ожидают завершения дочернего процесса для корректного завершения работы программы.
- **CreateFileMapping** — создает объект отображения файла для использования в общей памяти;
- **MapViewOfFile** — создает представление файла в адресном пространстве процесса, что позволяет разделять память между процессами;
- **UnmapViewOfFile** — освобождает представление файла из адресного пространства процесса;
- **FlushViewOfFile** — записывает измененные страницы отображаемого файла в диск;
- **ReadConsole** — считывает данные из стандартного потока ввода консоли;

**Алгоритм решения:**

Родительский процесс сначала запрашивает у пользователя имя файла, в который будут записываться строки, прошедшие проверку по условию. Далее родительский процесс создает объект общей памяти с помощью функции **CreateFileMapping**, который позволяет обоим процессам (родительскому и дочернему) обмениваться данными через общую память. После этого родительский процесс создает дочерний процесс через вызов **CreateProcess**, при этом перенаправляя стандартные потоки ввода, вывода и ошибок так, чтобы дочерний процесс мог считывать строки и передавать результаты обратно родительскому процессу через общую память.

Родительский процесс принимает от пользователя строки через стандартный поток ввода, после чего записывает их в общую память, которая доступна как ему, так и дочернему процессу. Дочерний процесс, получив доступ к общей памяти, проверяет строки на соответствие правилу: строка должна начинаться с заглавной буквы. Если строка проходит проверку, дочерний процесс выводит её в свой стандартный поток вывода. В случае, если строка не соответствует правилу, дочерний процесс записывает сообщение об ошибке в общую память, чтобы родительский процесс мог его обработать.

Родительский процесс получает сообщение об ошибке из общей памяти и выводит его на экран. Если же строка прошла проверку, родительский процесс записывает её в указанный файл. Процесс продолжается до тех пор, пока пользователь не завершит работу программы, например, с помощью нажатия комбинации клавиш CTRL+C или слова ‘exit’. После завершения программы все дескрипторы файлов и общей памяти закрываются, а родительский процесс ожидает завершения дочернего процесса с помощью вызова **WaitForSingleObject.**

## Код программы

**parent.c**

```
#include <windows.h>
#include <string.h>

#define BUFFER_SIZE 1024
```

```
#define SHARED_MEMORY_NAME "SharedMemoryExample"
#define EVENT_WRITE_NAME "WriteEvent"
#define EVENT_READ_NAME "ReadEvent"

HANDLE hMapFile;
LPVOID lpBuffer;
HANDLE hWriteEvent, hReadEvent;
HANDLE hFile;

void cleanup() {
    if (lpBuffer != NULL) {
        UnmapViewOfFile(lpBuffer);
        lpBuffer = NULL;
    }
    if (hMapFile != NULL) {
        CloseHandle(hMapFile);
        hMapFile = NULL;
    }
    if (hWriteEvent != NULL) {
        CloseHandle(hWriteEvent);
        hWriteEvent = NULL;
    }
    if (hReadEvent != NULL) {
        CloseHandle(hReadEvent);
        hReadEvent = NULL;
    }
    if (hFile != INVALID_HANDLE_VALUE) {
        CloseHandle(hFile);
        hFile = INVALID_HANDLE_VALUE;
    }
}

int main() {
    char input[BUFFER_SIZE];
    STARTUPINFO si;
    PROCESS_INFORMATION pi;
    DWORD bytes_written;

    WriteConsole(GetStdHandle(STD_OUTPUT_HANDLE), "Enter the file name to write the correct lines: ", 50, NULL, NULL);
    DWORD bytes_read;
    ReadConsole(GetStdHandle(STD_INPUT_HANDLE), input, BUFFER_SIZE, &bytes_read, NULL);
    input[bytes_read - 2] = '\0';

    hFile = CreateFile(input, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL);
    if (hFile == INVALID_HANDLE_VALUE) {
        WriteConsole(GetStdHandle(STD_ERROR_HANDLE), "Error when opening a file for recording\r\n", 42, NULL, NULL);
        return 1;
    }
    hMapFile = CreateFileMapping(INVALID_HANDLE_VALUE, NULL, PAGE_READWRITE, 0,
BUFFER_SIZE, SHARED_MEMORY_NAME);
    if (hMapFile == NULL) {
       cleanup();
       return 1;
    }

    lpBuffer = MapViewOfFile(hMapFile, FILE_MAP_ALL_ACCESS, 0, 0, BUFFER_SIZE);
    if (lpBuffer == NULL) {
       cleanup();
       return 1;
    }

    hWriteEvent = CreateEvent(NULL, FALSE, FALSE, EVENT_WRITE_NAME);
    hReadEvent = CreateEvent(NULL, FALSE, FALSE, EVENT_READ_NAME);
    if (hWriteEvent == NULL || hReadEvent == NULL) {
       cleanup();
       return 1;
    }

    ZeroMemory(&si, sizeof(si));
    si.cb = sizeof(si);
    ZeroMemory(&pi, sizeof(pi));

    if (!CreateProcess(NULL, "child.exe", NULL, NULL, TRUE, 0, NULL, NULL, &si, &pi)) {
       WriteConsole(GetStdHandle(STD_ERROR_HANDLE), "Error when starting a child
process\r\n", 44, NULL, NULL);
       cleanup();
       return 1;
    }

    while (1) {
       WriteConsole(GetStdHandle(STD_OUTPUT_HANDLE), "Enter the line (to exit, enter
'exit'): ", 17, NULL, NULL);
       ReadConsole(GetStdHandle(STD_INPUT_HANDLE), input, BUFFER_SIZE, &bytes_read,
NULL);
       input[bytes_read - 2] = '\0';

       if (strcmp(input, "exit") == 0) {
          strcpy((char*)lpBuffer, "EXIT");
          SetEvent(hWriteEvent);
          break;
       }

       strcpy((char*)lpBuffer, input);

       SetEvent(hWriteEvent);

       WaitForSingleObject(hReadEvent, INFINITE);

       if (strncmp((char*)lpBuffer, "ERROR", 5) == 0) {
            WriteConsole(GetStdHandle(STD_OUTPUT_HANDLE), (char*)lpBuffer,
strlen((char*)lpBuffer), NULL, NULL);
        } else {
            WriteFile(hFile, (char*)lpBuffer, strlen((char*)lpBuffer), &bytes_written, NULL);
            WriteFile(hFile, "\r\n", 2, &bytes_written, NULL);
        }
    }

    cleanup();
    return 0;
}
```

**child.c**

```
#include <windows.h>
#include <string.h>
#include <ctype.h>

#define BUFFER_SIZE 1024
#define SHARED_MEMORY_NAME "SharedMemoryExample"
#define EVENT_WRITE_NAME "WriteEvent"
#define EVENT_READ_NAME "ReadEvent"

int main() {
    HANDLE hMapFile;
    LPVOID lpBuffer;
    HANDLE hWriteEvent, hReadEvent;

    hMapFile = OpenFileMapping(FILE_MAP_ALL_ACCESS, FALSE,
SHARED_MEMORY_NAME);
    if (hMapFile == NULL) {
        return 1;
    }

    lpBuffer = MapViewOfFile(hMapFile, FILE_MAP_ALL_ACCESS, 0, 0, BUFFER_SIZE);
    if (lpBuffer == NULL) {
        CloseHandle(hMapFile);
        return 1;
    }

    hWriteEvent = OpenEvent(EVENT_ALL_ACCESS, FALSE, EVENT_WRITE_NAME);
    hReadEvent = OpenEvent(EVENT_ALL_ACCESS, FALSE, EVENT_READ_NAME);
    if (hWriteEvent == NULL || hReadEvent == NULL) {
        UnmapViewOfFile(lpBuffer);
        CloseHandle(hMapFile);
        return 1;
    }

    while (1) {
        WaitForSingleObject(hWriteEvent, INFINITE);

        char *line = (char*)lpBuffer;
        if (strcmp(line, "EXIT") == 0) {
            break;
        }

        if (isupper(line[0])) {
            strcpy((char*)lpBuffer, line);
        } else {
            strcpy((char*)lpBuffer, "ERROR: the line must start with a capital letter\r\n");
        }

        SetEvent(hReadEvent);
    }

    UnmapViewOfFile(lpBuffer);
    CloseHandle(hMapFile);
    CloseHandle(hWriteEvent);
    CloseHandle(hReadEvent);

    return 0;
}
```

# Протокол работы программы

**Тестирование:**

```
PS D:\lab3_OC> ./parent.exe
Enter the file name to write the correct lines: output.txt
Enter the line: hello
ERROR: the line must start with a capital letter
Enter the line: 123321312
ERROR: the line must start with a capital letter
Enter the line: привет
ERROR: the line must start with a capital letter
Enter the line: Привет
ERROR: the line must start with a capital letter
Enter the line: Hello
Enter the line: World
Enter the line: Privet
Enter the line: exit
```

**NTTrace:**

**parent_log.txt**

```
    [14956] Process 14956 starting at 0000000000000000 with command line:
""D:\lab3_OC\parent.exe""

    D:\lab3_OC\parent.exe

    [14956] Loaded DLL at 00007FFF43D30000 C:\WINDOWS\SYSTEM32\ntdll.dll

    [14956] Loaded DLL at 00007FFF432B0000 C:\WINDOWS\System32\KERNEL32.DLL

    [14956] Loaded DLL at 00007FFF41030000 C:\WINDOWS\System32\KERNELBASE.dll
```

```
[14956] Loaded DLL at 00007FFF416C0000 C:\WINDOWS\System32\ucrtbase.dll

[14956] Created thread: 2724 at 00007FFF43E072A0

[14956] NtTestAlert() => 0

[14956] Initial breakpoint

[14956] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0x30d6bffdb8, Length=4, ReturnLength=null) => 0

[14956] Thread 2724 exit code: 0

[14956] NtDeviceIoControlFile(FileHandle=0x20, Event=0x00000030d69ff620, ApcRoutine=null, ApcContext=0x3000000000, IoStatusBlock=0x30d69ff580 [0/0xc], IoControlCode=0x00500016, InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtCreateFile(FileHandle=0x30d69ff6a0 [0xb4], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0x50:"output.txt", IoStatusBlock=0x30d69ff6a8 [0/3], AllocationSize=null, FileAttributes=0x80, ShareAccess=0, CreateDisposition=5, CreateOptions=0x60, EaBuffer=null, EaLength=0) => 0

[14956] NtCreateSection(SectionHandle=0x30d69ff750 [0x5c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x7, ObjectAttributes=0x78:"SharedMemoryExample", SectionSize=0x30d69ff740 [1024], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

[14956] NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x30d69ff7a8 [0x0000015e323d0000], ZeroBits=0, CommitSize=0, SectionOffset=0x30d69ff7a0 [0], ViewSize=0x30d69ff7b0 [0x1000], InheritDisposition=1 [ViewShare], AllocationType=0, Protect=4) => 0

[14956] NtCreateEvent(EventHandle=0x30d69ff7a0 [0xb8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x78:"WriteEvent", EventType=1 [SynchronizationEvent], InitialState=false) => 0

[14956] NtCreateEvent(EventHandle=0x30d69ff7a0 [0xbc], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x78:"ReadEvent", EventType=1 [SynchronizationEvent], InitialState=false) => 0

[14956] NtQueryAttributesFile(ObjectAttributes="\??\D:\lab3_OC\child.exe", Attributes=0x30d69fd800 [ARCHIVE]) => 0

[14956] NtQueryAttributesFile(ObjectAttributes="\??\D:\lab3_OC\child.exe", Attributes=0x30d69fdbd8 [ARCHIVE]) => 0

[14956] NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0x30d69fd060) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']
```

```
[14956] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x2a [ThreadDynamicCodePolicyInfo], ThreadInformation=0x30d69fd060, Length=4, ReturnLength=null) => 0

[14956] NtOpenSection(SectionHandle=0x30d69fcff8 [0xc0], DesiredAccess=0xd, ObjectAttributes=0x44:"sechost.dll") => 0

[14956] Loaded DLL at 00007FFF420B0000 C:\WINDOWS\System32\sechost.dll

[14956] NtMapViewOfSection(SectionHandle=0xc0, ProcessHandle=-1, BaseAddress=0x15e323ff560 [0x00007fff420b0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15e323f8418 [0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

[14956] NtQueryPerformanceCounter(Counter=0x30d69fce50 [2.30904e+11], Freq=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fcde0 [0x00007fff42152000], Size=0x30d69fcdd8 [0x1000], NewProtect=2, OldProtect=0x30d69fcdd0 [4]) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fce60 [0x00007fff43ecb000], Size=0x30d69fce58 [0x4000], NewProtect=4, OldProtect=0x30d69fce50 [2]) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fce60 [0x00007fff43ecb000], Size=0x30d69fce58 [0x4000], NewProtect=2, OldProtect=0x30d69fce50 [4]) => 0

[14956] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7fff420b0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x30d69fcb88, Length=0x30, ReturnLength=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fcea0 [0x00007fff4212c000], Size=0x30d69fcea8 [0x2000], NewProtect=4, OldProtect=0x15e323f8400 [2]) => 0

[14956] NtOpenSection(SectionHandle=0x30d69fc898 [0xc4], DesiredAccess=0xd, ObjectAttributes=0x44:"bcrypt.dll") => 0

[14956] Loaded DLL at 00007FFF417E0000 C:\WINDOWS\System32\bcrypt.dll

[14956] NtMapViewOfSection(SectionHandle=0xc4, ProcessHandle=-1, BaseAddress=0x15e323ff7a0 [0x00007fff417e0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15e323f7fb8 [0x00028000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

[14956] NtQueryPerformanceCounter(Counter=0x30d69fc6f0 [2.30904e+11], Freq=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fc680 [0x00007fff41805000], Size=0x30d69fc678 [0x1000], NewProtect=2, OldProtect=0x30d69fc670 [4]) => 0
```

```
[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fc700 [0x00007fff43ecb000], Size=0x30d69fc6f8 [0x4000], NewProtect=4, OldProtect=0x30d69fc6f0 [2]) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fc700 [0x00007fff43ecb000], Size=0x30d69fc6f8 [0x4000], NewProtect=2, OldProtect=0x30d69fc6f0 [4]) => 0

[14956] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7fff417e0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x30d69fc428, Length=0x30, ReturnLength=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fc740 [0x00007fff417fc000], Size=0x30d69fc748 [0x1000], NewProtect=4, OldProtect=0x15e323f7fa0 [2]) => 0

[14956] NtClose(Handle=0xc4) => 0

[14956] NtClose(Handle=0xc0) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15e323f7f80 [0x00007fff417fc000], Size=0x15e323f7f88 [0x1000], NewProtect=2, OldProtect=0x30d69fcde0 [4]) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15e323f83e0 [0x00007fff4212c000], Size=0x15e323f83e8 [0x2000], NewProtect=2, OldProtect=0x30d69fcde0 [4]) => 0

[14956] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

[14956] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

[14956] NtTraceControl(CtrlCode=0xf, InputBuffer=0x30d69fcbb8, InputBufferLength=0xa0, OutputBuffer=0x30d69fcbb8, OutputBufferLength=0xa0, ReturnLength=0x30d69fcbb0 [0xa0]) => 0

[14956] NtTraceControl(CtrlCode=0xf, InputBuffer=0x30d69fcc18, InputBufferLength=0xa0, OutputBuffer=0x30d69fcc18, OutputBufferLength=0xa0, ReturnLength=0x30d69fcc10 [0xa0]) => 0

[14956] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x56 [ProcessEnclaveInformation], ProcessInformation=0x30d69fcca0, Length=0xb0, ReturnLength=null) => 0xc0000003 [87 '╧рЁрьхЄЁ чрфрэ эхтхЁэю.']

[14956] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0 [ProcessBasicInformation], ProcessInformation=0x30d69fcc20, Length=0x40, ReturnLength=null) => 0

[14956] NtTraceControl(CtrlCode=0xf, InputBuffer=0x30d69fcbc8, InputBufferLength=0xa0, OutputBuffer=0x30d69fcbc8, OutputBufferLength=0xa0, ReturnLength=0x30d69fcbc0 [0xa0]) => 0
```

[14956] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x30d69fcc18, InputBufferLength=0x18, OutputBuffer=0x30d69fcc30, OutputBufferLength=0x78, ReturnLength=0x30d69fcc10 [0]) => 0

[14956] NtCreateSemaphore(SemaphoreHandle=0x30d69fcbd8 [0xcc], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0

[14956] NtCreateSemaphore(SemaphoreHandle=0x30d69fcbe8 [0xd0], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0

[14956] NtCreateEvent(EventHandle=0x30d69fcbd8 [0xd4], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

[14956] NtOpenFile(FileHandle=0x7fff418027a0 [0xd8], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes="\Device\KsecDD", IoStatusBlock=0x30d69fcb20 [0/0], ShareAccess=7, OpenOptions=0x20) => 0

[14956] NtDeviceIoControlFile(FileHandle=0xd8, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69fcbc0 [0/0], IoControlCode=0x00390400, InputBuffer=0x30d69fcca0, InputBufferLength=0x68, OutputBuffer=0x30d69fcbd0, OutputBufferLength=8) => 0

[14956] NtTraceControl(CtrlCode=0xf, InputBuffer=0x30d69fcb78, InputBufferLength=0xa0, OutputBuffer=0x30d69fcb78, OutputBufferLength=0xa0, ReturnLength=0x30d69fcb70 [0xa0]) => 0

[14956] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x30d69fcbc8, InputBufferLength=0x18, OutputBuffer=0x30d69fcbe0, OutputBufferLength=0x78, ReturnLength=0x30d69fcbc0 [0]) => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69fc580 [0x0000015e32403000], ZeroBits=0, pSize=0x30d69fc628 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

[14956] NtTraceControl(CtrlCode=0xf, InputBuffer=0x30d69fcb78, InputBufferLength=0xa0, OutputBuffer=0x30d69fcb78, OutputBufferLength=0xa0, ReturnLength=0x30d69fcb70 [0xa0]) => 0

[14956] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x30d69fcbc8, InputBufferLength=0x18, OutputBuffer=0x30d69fcbe0, OutputBufferLength=0x78, ReturnLength=0x30d69fcbc0 [0]) => 0

[14956] NtTraceControl(CtrlCode=0xf, InputBuffer=0x30d69fcba8, InputBufferLength=0xa0, OutputBuffer=0x30d69fcba8, OutputBufferLength=0xa0, ReturnLength=0x30d69fcba0 [0xa0]) => 0

[14956] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x30d69fcbf8, InputBufferLength=0x18, OutputBuffer=0x30d69fcc10, OutputBufferLength=0x78, ReturnLength=0x30d69fcbf0 [0]) => 0

```
        [14956] NtSetEvent(EventHandle=0x48, PrevState=null) => 0

        [14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fd538
[0x00007fff413b7000], Size=0x30d69fd530 [0x1000], NewProtect=4, OldProtect=0x30d69fd548
[2]) => 0

        [14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fd538
[0x00007fff413b7000], Size=0x30d69fd530 [0x1000], NewProtect=2, OldProtect=0x30d69fd548
[4]) => 0

        [14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69fd240
[0x0000015e32405000], ZeroBits=0, pSize=0x30d69fd2e8 [0x3000], flAllocationType=0x1000,
flProtect=4) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fdaa8 [0xe8], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options") => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fdb90, DesiredAccess=0x9,
ObjectAttributes=0xe8:"child.exe") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtOpenKey(KeyHandle=0x30d69fdb70, DesiredAccess=0x101,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Wow64\x86\xtajit") => 0xc0000034 [2
'═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtCreateUserProcess(ProcessHandle=0x30d69fdd20 [0xf0],
ThreadHandle=0x30d69fdda0 [0xec], ProcessDesiredAccess=MAXIMUM_ALLOWED,
ThreadDesiredAccess=MAXIMUM_ALLOWED, ProcessObjectAttributes=null,
ThreadObjectAttributes=null, ProcessFlags=0x204, ThreadFlags=1,
ProcessParameters=0x15e32403380 ["D:\lab3_OC\child.exe"], CreateInfo=0x30d69fe070,
AttributeList=0x30d69fe510) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fdc38, DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session
Manager\AppCertDlls") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0xa,
TokenHandle=0x30d69fd8f0 [0xfc]) => 0

        [14956] NtQueryInformationToken(TokenHandle=0xfc, TokenInformationClass=1
[TokenUser], TokenInformation=0x30d69fdb40, Length=0x90, ReturnLength=0x30d69fd918
[0x2c]) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd910, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtOpenKey(KeyHandle=0x30d69fd8d8 [0x100], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers"
) => 0

        [14956] NtQueryValueKey(KeyHandle=0x100, ValueName="TransparentEnabled",
KeyValueInformationClass=2 [KeyValuePartialInformation],
KeyValueInformation=0x30d69fda20, Length=0x50, ResultLength=0x30d69fd8d0) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtQueryValueKey(KeyHandle=0x100, ValueName="AuthenticodeEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x30d69fda20, Length=0x50, ResultLength=0x30d69fd8d0 [0x10]) => 0

[14956] NtClose(Handle=0x100) => 0

[14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd800, Length=0x58, ReturnLength=0x30d69fd7f8 [0x2c]) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd8d8, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtClose(Handle=0xfc) => 0

[14956] NtTraceControl(CtrlCode=0xf, InputBuffer=0x30d69fd998, InputBufferLength=0xa0, OutputBuffer=0x30d69fd998, OutputBufferLength=0xa0, ReturnLength=0x30d69fd990 [0xa0]) => 0

[14956] NtQueryInformationProcess(ProcessHandle=0xf0, ProcessInformationClass=0x3c [ProcessCommandLineInformation], ProcessInformation=0x15e32401550, Length=0x400, ReturnLength=0x30d69fd8c0 [0x24]) => 0

[14956] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0x30d69fd3a0, Length=0x24, ReturnLength=null) => 0

[14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd540, Length=0x54, ReturnLength=0x30d69fd520 [0x2c]) => 0

[14956] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0x30d69fd330, Length=0x24, ReturnLength=null) => 0

[14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd6e0, Length=0x58, ReturnLength=0x30d69fd6d8 [0x2c]) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd858 [0x104], DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders") => 0

[14956] NtQueryValueKey(KeyHandle=0x104, ValueName="Cache", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x15e32405220, Length=0x208, ResultLength=0x30d69fd850 [0x92]) => 0

[14956] NtClose(Handle=0x104) => 0
```

```
[14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd6e0, Length=0x58, ReturnLength=0x30d69fd6d8 [0x2c]) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd800 [0x108], DesiredAccess=0x8, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Microsoft\Windows NT\CurrentVersion") => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd808 [0x100], DesiredAccess=0x101, ObjectAttributes=0x108:"AppCompatFlags\Layers") => 0

[14956] NtQueryValueKey(KeyHandle=0x100, ValueName="D:\lab3_OC\child.exe", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x30d69fd868, Length=0x10, ResultLength=0x30d69fd810) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtClose(Handle=0x100) => 0

[14956] NtApphelpCacheControl(ServiceClass=0xb, ServiceData="") => 0

[14956] NtQueryInformationProcess(ProcessHandle=0xf0, ProcessInformationClass=0 [ProcessBasicInformation], ProcessInformation=0x30d69fdb60, Length=0x40, ReturnLength=null) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd910 [0x100], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide") => 0

[14956] NtQueryValueKey(KeyHandle=0x100, ValueName="PreferExternalManifest", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x30d69fd960, Length=0x14, ResultLength=0x30d69fd918) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtClose(Handle=0x100) => 0

[14956] NtQueryVolumeInformationFile(FileHandle=0xf4, IoStatusBlock=0x30d69fd970 [0/8], FsInformation=0x30d69fd9a0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

[14956] NtGetMUIRegistryInfo(Flags=0, BufferLength=0x30d69fd790 [0x4d0], Buffer=null) => 0

[14956] NtGetMUIRegistryInfo(Flags=0, BufferLength=0x30d69fd790 [0x4d0], Buffer=0x15e32403380) => 0

[14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd5c0, Length=0x58, ReturnLength=0x30d69fd5b8 [0x2c]) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd7a8 [0x100], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0
```

```
[14956] NtOpenKey(KeyHandle=0x30d69fd7a0, DesiredAccess=KEY_READ, ObjectAttributes=0x100:"Control Panel\Desktop\MuiCached\MachineLanguageConfiguration") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtClose(Handle=0x100) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd638, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd4d0, Length=0x58, ReturnLength=0x30d69fd4c8 [0x2c]) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd640 [0x100], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd648, DesiredAccess=KEY_READ, ObjectAttributes=0x100:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtOpenKey(KeyHandle=0x30d69fd638, DesiredAccess=KEY_READ, ObjectAttributes=0x100:"Control Panel\Desktop\LanguageConfiguration") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtClose(Handle=0x100) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd5d8, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd440, Length=0x58, ReturnLength=0x30d69fd438 [0x2c]) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd5d0 [0x10c], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0

[14956] NtOpenKey(KeyHandle=0x30d69fd500, DesiredAccess=KEY_READ, ObjectAttributes=0x10c:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtOpenKey(KeyHandle=0x30d69fd5c8 [0x110], DesiredAccess=KEY_READ, ObjectAttributes=0x10c:"Control Panel\Desktop") => 0

[14956] NtQueryValueKey(KeyHandle=0x110, ValueName="PreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x15e323fe710, Length=0xc, ResultLength=0x30d69fd598) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtClose(Handle=0x110) => 0
```

```
        [14956] NtClose(Handle=0x10c) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd5d8, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034
[2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1
[TokenUser], TokenInformation=0x30d69fd440, Length=0x58, ReturnLength=0x30d69fd438
[0x2c]) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd5d0 [0x10c],
DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-
2409479645-3338554513-3479048774-1001") => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd5c8 [0x110], DesiredAccess=KEY_READ,
ObjectAttributes=0x10c:"Control Panel\Desktop\MuiCached") => 0

        [14956] NtQueryValueKey(KeyHandle=0x110,
ValueName="MachinePreferredUILanguages", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x15e323fe7d0, Length=0xc,
ResultLength=0x30d69fd598) => 0x80000005 [234 '╚ьх■Єё  фюяюыэшЄхы№э√х фрээ√х.']

        [14956] NtQueryValueKey(KeyHandle=0x110,
ValueName="MachinePreferredUILanguages", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x15e323fe6b0, Length=0x18,
ResultLength=0x30d69fd598 [0x18]) => 0

        [14956] NtClose(Handle=0x110) => 0

        [14956] NtClose(Handle=0x10c) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd678, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034
[2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1
[TokenUser], TokenInformation=0x30d69fd4e0, Length=0x58, ReturnLength=0x30d69fd4d8
[0x2c]) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd670 [0x10c],
DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-
2409479645-3338554513-3479048774-1001") => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd5a0, DesiredAccess=KEY_READ,
ObjectAttributes=0x10c:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2
'═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtOpenKey(KeyHandle=0x30d69fd668 [0x100], DesiredAccess=KEY_READ,
ObjectAttributes=0x10c:"Control Panel\Desktop") => 0

        [14956] NtQueryValueKey(KeyHandle=0x100, ValueName="PreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation],
KeyValueInformation=0x15e323fe7f0, Length=0xc, ResultLength=0x30d69fd638) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtClose(Handle=0x100) => 0

        [14956] NtClose(Handle=0x10c) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd6b8, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x30d69fd550, Length=0x58, ReturnLength=0x30d69fd548 [0x2c]) => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd6c0 [0x100], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0

        [14956] NtOpenKey(KeyHandle=0x30d69fd6c8, DesiredAccess=KEY_READ, ObjectAttributes=0x100:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtOpenKey(KeyHandle=0x30d69fd6b8, DesiredAccess=KEY_READ, ObjectAttributes=0x100:"Control Panel\Desktop\LanguageConfiguration") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        [14956] NtClose(Handle=0x100) => 0

        [14956] NtAlpcSendWaitReceivePort(PortHandle=0x68, SendFlags=0x00020000, SendMessage=0x30d69fe900 [2 [LPC_REPLY] (560b)], InMessageBuffer=null, ReceiveBuffer=0x30d69fe900, ReceiveBufferSize=0x30d69fdc10 [0x258], OutMessageBuffer=null, Timeout=null) => 0

        [14956] NtQueryLicenseValue(Name="Kernel-OneCore-DeviceFamilyID", Type=0x30d69fd828 [4], Buffer=0x30d69fd820, Length=4, ReturnedLength=0x30d69fd870 [4]) => 0

        [14956] NtAllocateVirtualMemory(ProcessHandle=0xf0, lpAddress=0x30d69fdfc8 [0x000002d0cc280000], ZeroBits=0, pSize=0x30d69fe180 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

        [14956] NtWriteVirtualMemory(ProcessHandle=0xf0, BaseAddress=0x2d0cc280000, Buffer=0x15e32403860, BufferLength=0x11c0, ReturnedLength=null) => 0

        [14956] NtWriteVirtualMemory(ProcessHandle=0xf0, BaseAddress=0xd12ef642d8, Buffer=0x30d69fdfc8, BufferLength=8, ReturnedLength=null) => 0

        [14956] NtResumeThread(ThreadHandle=0xec, SuspendCount=null) => 0

        [14956] NtClose(Handle=0xf4) => 0

        [14956] NtClose(Handle=0xf8) => 0
```

```
        [14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x11], IoControlCode=0x00500016,
InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff580 [0/7], IoControlCode=0x00500016,
InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

        [14956] NtWaitForSingleObject(Handle=0xbc, Alertable=false, Timeout=null) => 0

        [14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x32], IoControlCode=0x00500016,
InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x11], IoControlCode=0x00500016,
InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff580 [0/0xb], IoControlCode=0x00500016,
InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

        [14956] NtWaitForSingleObject(Handle=0xbc, Alertable=false, Timeout=null) => 0

        [14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x32], IoControlCode=0x00500016,
InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x11], IoControlCode=0x00500016,
InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0x30d69ff580 [0/8], IoControlCode=0x00500016,
InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0)
=> 0

        [14956] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

        [14956] NtWaitForSingleObject(Handle=0xbc, Alertable=false, Timeout=null) => 0
```

```
[14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x32], IoControlCode=0x00500016, InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x11], IoControlCode=0x00500016, InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff580 [0/8], IoControlCode=0x00500016, InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[14956] NtWaitForSingleObject(Handle=0xbc, Alertable=false, Timeout=null) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x32], IoControlCode=0x00500016, InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x11], IoControlCode=0x00500016, InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff580 [0/7], IoControlCode=0x00500016, InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[14956] NtWaitForSingleObject(Handle=0xbc, Alertable=false, Timeout=null) => 0

[14956] NtWriteFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff800 [0/5], Buffer=0x15e323d0000, Length=5, ByteOffset=null, Key=null) => 0

[14956] NtWriteFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff800 [0/2], Buffer=0x7ff736c040da, Length=2, ByteOffset=null, Key=null) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x11], IoControlCode=0x00500016, InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff580 [0/7], IoControlCode=0x00500016,
InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[14956] NtWaitForSingleObject(Handle=0xbc, Alertable=false, Timeout=null) => 0

[14956] NtWriteFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff800 [0/5], Buffer=0x15e323d0000, Length=5, ByteOffset=null, Key=null) => 0

[14956] NtWriteFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff800 [0/2], Buffer=0x7ff736c040da, Length=2, ByteOffset=null, Key=null) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff640 [0/0x11], IoControlCode=0x00500016, InputBuffer=0x30d69ff650, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x30d69ff580 [0/6], IoControlCode=0x00500016, InputBuffer=0x30d69ff590, InputBufferLength=0x60, OutputBuffer=null, OutputBufferLength=0) => 0

[14956] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[14956] NtUnmapViewOfSectionEx(ProcessHandle=-1, BaseAddress=0x15e323d0000, Flags=0) => 0

[14956] NtClose(Handle=0x5c) => 0

[14956] NtClose(Handle=0xb8) => 0

[14956] NtClose(Handle=0xbc) => 0

[14956] NtClose(Handle=0xb4) => 0

[14956] NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0x30d69ff880) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

[14956] NtOpenSection(SectionHandle=0x30d69ff818, DesiredAccess=0xd, ObjectAttributes=0x44:"kernel.appcore.dll") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtQueryAttributesFile(ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", Attributes=0x30d69ff5d8 [ARCHIVE]) => 0

[14956] NtOpenFile(FileHandle=0x30d69ff5e0 [0xf8], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0x30d69ff648 [0/1], ShareAccess=5, OpenOptions=0x60) => 0
```

```
[14956] NtCreateSection(SectionHandle=0x30d69ff5e8 [0x5c], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xf8) => 0

[14956] Loaded DLL at 00007FFF400C0000 C:\WINDOWS\SYSTEM32\kernel.appcore.dll

[14956] NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x15e323f83a0 [0x00007fff400c0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15e323faca8 [0x00018000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

[14956] NtQueryPerformanceCounter(Counter=0x30d69ff460 [2.31089e+11], Freq=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69ff3f0 [0x00007fff400d5000], Size=0x30d69ff3e8 [0x1000], NewProtect=2, OldProtect=0x30d69ff3e0 [4]) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69ff470 [0x00007fff43ecb000], Size=0x30d69ff468 [0x4000], NewProtect=4, OldProtect=0x30d69ff460 [2]) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69ff470 [0x00007fff43ecb000], Size=0x30d69ff468 [0x4000], NewProtect=2, OldProtect=0x30d69ff460 [4]) => 0

[14956] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7fff400c0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x30d69ff198, Length=0x30, ReturnLength=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69ff4b0 [0x00007fff400ca000], Size=0x30d69ff4b8 [0x2000], NewProtect=4, OldProtect=0x15e323fac90 [2]) => 0

[14956] NtOpenSection(SectionHandle=0x30d69feea8 [0xf4], DesiredAccess=0xd, ObjectAttributes=0x44:"msvcrt.dll") => 0

[14956] Loaded DLL at 00007FFF41B10000 C:\WINDOWS\System32\msvcrt.dll

[14956] NtMapViewOfSection(SectionHandle=0xf4, ProcessHandle=-1, BaseAddress=0x15e323fb000 [0x00007fff41b10000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15e323fa5b8 [0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

[14956] NtQueryPerformanceCounter(Counter=0x30d69fed00 [2.31089e+11], Freq=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fed10 [0x00007fff43ecb000], Size=0x30d69fed08 [0x4000], NewProtect=4, OldProtect=0x30d69fed00 [2]) => 0
```

```
[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fed10 [0x00007fff43ecb000], Size=0x30d69fed08 [0x4000], NewProtect=2, OldProtect=0x30d69fed00 [4]) => 0

[14956] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7fff41b10000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x30d69fea38, Length=0x30, ReturnLength=null) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x30d69fed50 [0x00007fff41b8e000], Size=0x30d69fed58 [0x1000], NewProtect=4, OldProtect=0x15e323fa5a0 [2]) => 0

[14956] NtClose(Handle=0xf4) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15e323fac70 [0x00007fff400ca000], Size=0x15e323fac78 [0x2000], NewProtect=2, OldProtect=0x30d69ff2b0 [4]) => 0

[14956] NtClose(Handle=0x5c) => 0

[14956] NtClose(Handle=0xf8) => 0

[14956] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15e323fa580 [0x00007fff41b8e000], Size=0x15e323fa588 [0x1000], NewProtect=2, OldProtect=0x30d69ff600 [4]) => 0

[14956] NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0x30d69ff560, Length=0x28) => 0

[14956] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

[14956] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69ff230 [0x0000015e325c0000], ZeroBits=0, pSize=0x30d69ff238 [0x001d0000], flAllocationType=0x2000, flProtect=4) => 0

[14956] NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69ff230 [0x0000015e325c0000], pSize=0x30d69ff228 [0x001c0000], flFreeType=0x8000) => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69ff218 [0x0000015e32780000], ZeroBits=0, pSize=0x30d69ff210 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

[14956] NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0x30d69ff500 [0/8], FsInformation=0x30d69ff520, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

[14956] NtQueryVolumeInformationFile(FileHandle=0x60, IoStatusBlock=0x30d69ff500 [0/8], FsInformation=0x30d69ff520, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
```

```
[14956] NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0x30d69ff500 [0/8], FsInformation=0x30d69ff520, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69ff130 [0x0000015e32782000], ZeroBits=0, pSize=0x30d69ff1d8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69fecd0 [0x0000015e32783000], ZeroBits=0, pSize=0x30d69fed78 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

[14956] NtOpenKey(KeyHandle=0x30d69fefa0 [0x114], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

[14956] NtQueryValueKey(KeyHandle=0x114, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x30d69fefe0, Length=0x18, ResultLength=0x30d69fefa8) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[14956] NtClose(Handle=0x114) => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69ff0f8 [0x0000015e325c0000], ZeroBits=0, pSize=0x30d69ff100 [0x00062000], flAllocationType=0x2000, flProtect=4) => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69ff0f8 [0x0000015e325c0000], ZeroBits=0, pSize=0x30d69ff108 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

[14956] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x30d69ff130 [0x0000015e32785000], ZeroBits=0, pSize=0x30d69ff1d8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

[14956] NtSetEvent(EventHandle=0x48, PrevState=null) => 0

[14956] NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0x30d69ff820, Length=0x330, ReturnLength=0x30d69ff7d8) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

[14956] NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0x30d69ff820, Length=0x330, ReturnLength=0x30d69ff7d8) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

[14956] NtTerminateProcess(ProcessHandle=0, ExitStatus=0) => 0

[14956] NtClose(Handle=0xe4) => 0

[14956] NtClose(Handle=0xdc) => 0

[14956] NtClose(Handle=0xe0) => 0

[14956] NtClose(Handle=0xc4) => 0
```

```
[14956] NtClose(Handle=0xc8) => 0

[14956] NtClose(Handle=0x6c) => 0

[14956] NtClose(Handle=0x98) => 0

[14956] NtClose(Handle=0x94) => 0

[14956] NtQueryWnfStateData(StateName=0x30d69ff7f0 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x30d69fe73c [0xa40b], Buffer=0x30d69fe790, BufferSize=0x30d69fe738 [0xffe]) => 0

[14956] NtClose(Handle=0x84) => 0

[14956] NtClose(Handle=0x70) => 0

[14956] Process 14956 exit code: 0
```

**child_log.txt**

```
[18056] Process 18056 starting at 0000000000000000 with command line: "child.exe"

D:\lab3_OC\child.exe

[18056] Loaded DLL at 00007FFF43D30000 C:\WINDOWS\SYSTEM32\ntdll.dll

[18056] Created thread: 16768 at 00007FFF43D65580

[18056] Loaded DLL at 00007FFF432B0000 C:\WINDOWS\System32\KERNEL32.DLL

[18056] Loaded DLL at 00007FFF41030000 C:\WINDOWS\System32\KERNELBASE.dll

[18056] Loaded DLL at 00007FFF416C0000 C:\WINDOWS\System32\ucrtbase.dll

[18056] Created thread: 20076 at 00007FFF43E072A0

[18056] NtTestAlert() => 0

[18056] Initial breakpoint

[18056] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xa6097ffd98, Length=4, ReturnLength=null) => 0

[18056] Thread 20076 exit code: 0

[18056] NtWaitForSingleObject(Handle=0x000000a6093ffb80, Alertable=false, Timeout=null) => 0

[18056] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[18056] NtWaitForSingleObject(Handle=0xb4, Alertable=false, Timeout=null) => 0

[18056] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[18056] NtWaitForSingleObject(Handle=0xb4, Alertable=false, Timeout=null) => 0

[18056] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0
```

```
[18056] NtWaitForSingleObject(Handle=0xb4, Alertable=false, Timeout=null) => 0

[18056] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[18056] NtWaitForSingleObject(Handle=0xb4, Alertable=false, Timeout=null) => 0

[18056] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[18056] NtWaitForSingleObject(Handle=0xb4, Alertable=false, Timeout=null) => 0

[18056] NtSetEvent(EventHandle=0xb8, PrevState=null) => 0

[18056] NtWaitForSingleObject(Handle=0xb4, Alertable=false, Timeout=null) => 0

[18056] NtUnmapViewOfSectionEx(ProcessHandle=-1, BaseAddress=0x27a2ec80000, Flags=0) => 0

[18056] NtClose(Handle=0xb0) => 0

[18056] NtClose(Handle=0xb4) => 0

[18056] NtClose(Handle=0xb8) => 0

[18056] NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0xa6093ff6e0) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

[18056] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x2a [ThreadDynamicCodePolicyInfo], ThreadInformation=0xa6093ff6e0, Length=4, ReturnLength=null) => 0

[18056] NtOpenSection(SectionHandle=0xa6093ff678, DesiredAccess=0xd, ObjectAttributes=0x44:"kernel.appcore.dll") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[18056] NtQueryAttributesFile(ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", Attributes=0xa6093ff438 [ARCHIVE]) => 0

[18056] NtOpenFile(FileHandle=0xa6093ff440 [0xb0], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0xa6093ff4a8 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

[18056] NtCreateSection(SectionHandle=0xa6093ff448 [0xb4], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xb0) => 0

[18056] Loaded DLL at 00007FFF400C0000 C:\WINDOWS\SYSTEM32\kernel.appcore.dll

[18056] NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x27a2eb38380 [0x00007fff400c0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x27a2eb3ac88 [0x00018000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
```

```
[18056] NtQueryPerformanceCounter(Counter=0xa6093ff2c0 [2.34149e+11], Freq=null) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa6093ff250 [0x00007fff400d5000], Size=0xa6093ff248 [0x1000], NewProtect=2, OldProtect=0xa6093ff240 [4]) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa6093ff2d0 [0x00007fff43ecb000], Size=0xa6093ff2c8 [0x4000], NewProtect=4, OldProtect=0xa6093ff2c0 [2]) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa6093ff2d0 [0x00007fff43ecb000], Size=0xa6093ff2c8 [0x4000], NewProtect=2, OldProtect=0xa6093ff2c0 [4]) => 0

[18056] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7fff400c0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xa6093feff8, Length=0x30, ReturnLength=null) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa6093ff310 [0x00007fff400ca000], Size=0xa6093ff318 [0x2000], NewProtect=4, OldProtect=0x27a2eb3ac70 [2]) => 0

[18056] NtOpenSection(SectionHandle=0xa6093fed08 [0xb8], DesiredAccess=0xd, ObjectAttributes=0x44:"msvcrt.dll") => 0

[18056] Loaded DLL at 00007FFF41B10000 C:\WINDOWS\System32\msvcrt.dll

[18056] NtMapViewOfSection(SectionHandle=0xb8, ProcessHandle=-1, BaseAddress=0x27a2eb3f750 [0x00007fff41b10000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x27a2eb3f6d8 [0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

[18056] NtQueryPerformanceCounter(Counter=0xa6093feb60 [2.3415e+11], Freq=null) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa6093feb70 [0x00007fff43ecb000], Size=0xa6093feb68 [0x4000], NewProtect=4, OldProtect=0xa6093feb60 [2]) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa6093feb70 [0x00007fff43ecb000], Size=0xa6093feb68 [0x4000], NewProtect=2, OldProtect=0xa6093feb60 [4]) => 0

[18056] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7fff41b10000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xa6093fe898, Length=0x30, ReturnLength=null) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa6093febb0 [0x00007fff41b8e000], Size=0xa6093febb8 [0x1000], NewProtect=4, OldProtect=0x27a2eb3f6c0 [2]) => 0

[18056] NtClose(Handle=0xb8) => 0
```

```
[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x27a2eb3ac50 [0x00007fff400ca000], Size=0x27a2eb3ac58 [0x2000], NewProtect=2, OldProtect=0xa6093ff110 [4]) => 0

[18056] NtClose(Handle=0xb4) => 0

[18056] NtClose(Handle=0xb0) => 0

[18056] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x27a2eb3f6a0 [0x00007fff41b8e000], Size=0x27a2eb3f6a8 [0x1000], NewProtect=2, OldProtect=0xa6093ff460 [4]) => 0

[18056] NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0xa6093ff3c0, Length=0x28) => 0

[18056] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

[18056] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093ff090 [0x0000027a2ec80000], ZeroBits=0, pSize=0xa6093ff098 [0x000b0000], flAllocationType=0x2000, flProtect=4) => 0

[18056] NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093ff090 [0x0000027a2ec80000], pSize=0xa6093ff088 [0x000a0000], flFreeType=0x8000) => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093ff078 [0x0000027a2ed20000], ZeroBits=0, pSize=0xa6093ff070 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

[18056] NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0xa6093ff360 [0/8], FsInformation=0xa6093ff380, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

[18056] NtQueryVolumeInformationFile(FileHandle=0x60, IoStatusBlock=0xa6093ff360 [0/8], FsInformation=0xa6093ff380, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

[18056] NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0xa6093ff360 [0/8], FsInformation=0xa6093ff380, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093fefc0 [0x0000027a2eb42000], ZeroBits=0, pSize=0xa6093ff068 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093fef90 [0x0000027a2ed22000], ZeroBits=0, pSize=0xa6093ff038 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093feb30 [0x0000027a2ed23000], ZeroBits=0, pSize=0xa6093febd8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
```

```
[18056] NtOpenKey(KeyHandle=0xa6093fee00 [0xb0], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

[18056] NtQueryValueKey(KeyHandle=0xb0, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xa6093fee40, Length=0x18, ResultLength=0xa6093fee08) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

[18056] NtClose(Handle=0xb0) => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093fef58 [0x0000027a2ec80000], ZeroBits=0, pSize=0xa6093fef60 [0x00062000], flAllocationType=0x2000, flProtect=4) => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093fef58 [0x0000027a2ec80000], ZeroBits=0, pSize=0xa6093fef68 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

[18056] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa6093fef90 [0x0000027a2ed25000], ZeroBits=0, pSize=0xa6093ff038 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

[18056] NtSetEvent(EventHandle=0x48, PrevState=null) => 0

[18056] NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xa6093ff680, Length=0x330, ReturnLength=0xa6093ff638) => 0xc0000225 [1168 '█ ыхьхэЄ эх эрщфхэ.']

[18056] NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xa6093ff680, Length=0x330, ReturnLength=0xa6093ff638) => 0xc0000225 [1168 '█ ыхьхэЄ эх эрщфхэ.']

[18056] NtTerminateProcess(ProcessHandle=0, ExitStatus=0) => 0

[18056] Thread 16768 exit code: 0

[18056] NtClose(Handle=0x5c) => 0

[18056] NtClose(Handle=0x94) => 0

[18056] NtClose(Handle=0x90) => 0

[18056] NtQueryWnfStateData(StateName=0xa6093ff650 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xa6093fe59c [0xa40b], Buffer=0xa6093fe5f0, BufferSize=0xa6093fe598 [0xffe]) => 0

[18056] NtClose(Handle=0x80) => 0

[18056] NtClose(Handle=0x6c) => 0

[18056] Process 18056 exit code: 0
```

# Вывод

**В ходе работы изначальная задача была выполнена, а также решены проблемы с передачей данных между процессами через общую память. Были устранены ошибки завершения программы и корректной обработки строк, что обеспечило правильную работу с файлами и вывод информации об ошибках. Также была решена проблема записи данных в конечный файл, обеспечив успешную передачу и сохранение результатов корректных строк в файл, указанный пользователем в начале работы программы.**