Московский Авиационный Институт

(Национальный Исследовательский Университет)

Институт №8 “Компьютерные науки и прикладная математика”

Кафедра №806 “Вычислительная математика и программирование”

# Лабораторная работа №1 по курсу

# «Операционные системы»

Группа: М8О-213Б-23

Студент: Черников В.В.

Преподаватель: Бахарев В.Д. (ФИИТ)

Оценка: _____

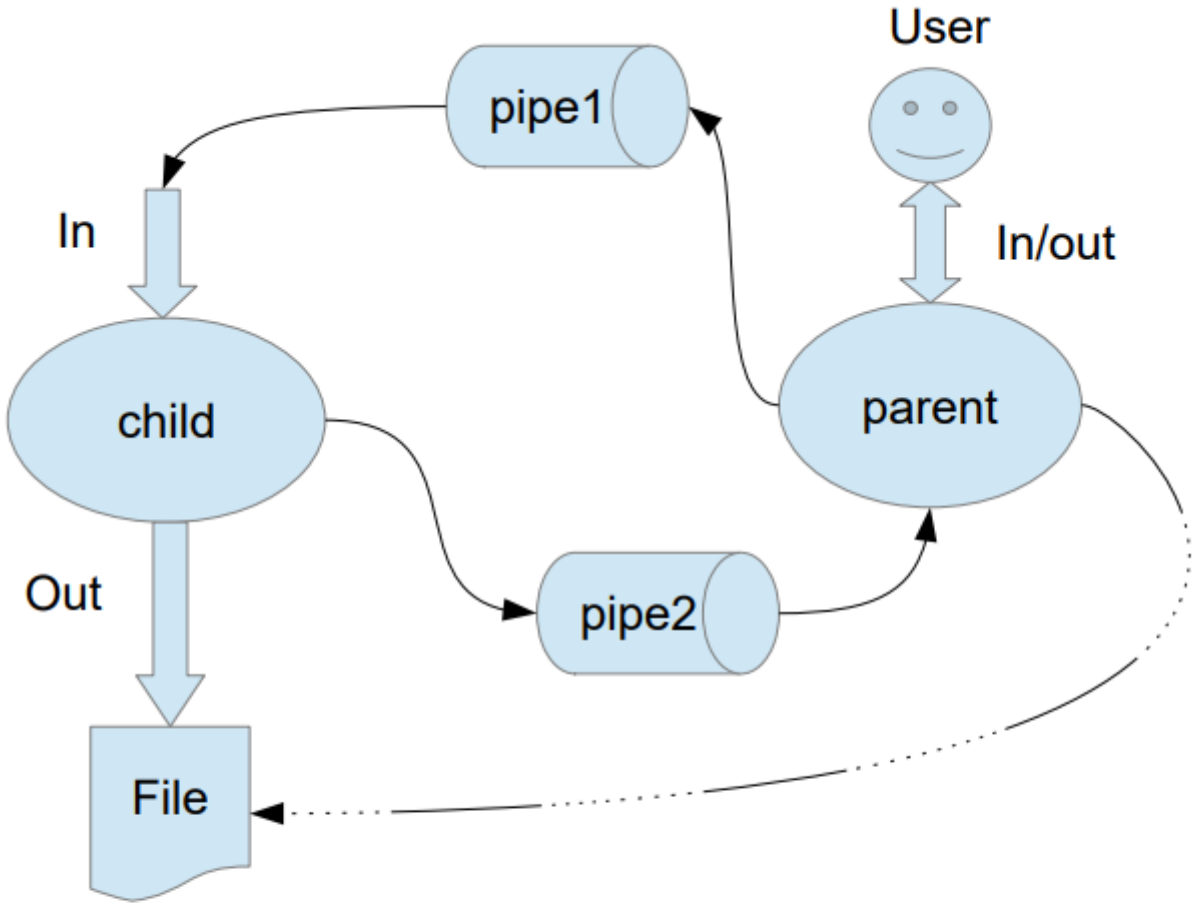
Дата: 16.10.24

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

# Общий метод и алгоритм решения

**Использованные системные вызовы:**

- **SetConsoleOutputCP(CP_UTF8)** - устанавливает кодировку UTF-8 для вывода в консоль;
- **CreatePipe(&pipe1_read, &pipe1_write, &sa, 0)** - создает канал для передачи данных между процессами;
- **CreatePipe(&pipe2_read, &pipe2_write, &sa, 0)** - создает второй канал для передачи данных обратно в родительский процесс;

- **GetStdHandle(STD_OUTPUT_HANDLE)** - возвращает дескриптор стандартного вывода консоли;
- **CreateProcess(NULL, "child.exe", NULL, NULL, TRUE, 0, NULL, NULL, &si, &pi)** - создает новый дочерний процесс для выполнения программы child.exe;
- **WriteFile(pipe1_write, input, strlen(input), &bytes_written, NULL)** - записывает данные в канал для передачи их дочернему процессу.
- **ReadFile(pipe2_read, error_message, BUFFER_SIZE - 1, &bytes_read, NULL)** - читает данные из канала, полученные от дочернего процесса;
- **CreateFile(filename, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL)** - открывает или создает файл для записи;
- **CloseHandle(pipe1_read) / CloseHandle(pipe2_write)** - закрывает дескриптор канала после использования;
- **WaitForSingleObject(pi.hProcess, INFINITE)** - ожидает завершения дочернего процесса;
- **GetStdHandle(STD_INPUT_HANDLE)** - возвращает дескриптор стандартного ввода (канал pipe1 от родительского процесса);
- **GetStdHandle(STD_ERROR_HANDLE)** - возвращает дескриптор стандартного вывода ошибок (канал pipe2 для передачи ошибок обратно в родительский процесс);
- **ReadFile(pipe1_read, buffer, BUFFER_SIZE - 1, &bytes_read, NULL)** - читает данные, переданные через канал родительским процессом;
- **WriteFile(pipe2_write, error_message, strlen(error_message), &bytes_written, NULL)** - записывает сообщение об ошибке в канал для передачи его родительскому процессу.
- **void cleanup()** – завершение работы программы и освобождение всех ресурсов, задействованных в работе.

**Алгоритм решения:**

Родительский процесс создает два канала для передачи данных: один для отправки строк дочернему процессу, а другой для получения сообщений об ошибках.

Дочерний процесс считывает строки из первого канала, проверяет, начинается ли строка с заглавной буквы, и выводит её, если проверка пройдена. В противном случае отправляет сообщение об ошибке через второй канал.

Родительский процесс считывает эти сообщения, выводит их на экран и записывает корректные строки в файл, который пользователь указывает в начале работы. Цикл продолжается до тех пор, пока пользователь не завершит работу программы (например, нажатием горячих клавиш CTRL + C). После завершения работы все дескрипторы закрываются, а родительский процесс ожидает завершения дочернего процесса.

# Код программы

**parent.c**

```
#include <windows.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <signal.h>

#define BUFFER_SIZE 1024

BOOL running = TRUE;
```

```
HANDLE file_handle = INVALID_HANDLE_VALUE;
HANDLE pipe1_write = INVALID_HANDLE_VALUE;
HANDLE pipe2_read = INVALID_HANDLE_VALUE;
PROCESS_INFORMATION pi = {0};
char last_input[BUFFER_SIZE] = {0};

void cleanup() {
    if (pi.hProcess != NULL) {
        WaitForSingleObject(pi.hProcess, INFINITE);
        TerminateProcess(pi.hProcess, 0);
        CloseHandle(pi.hProcess);
        pi.hProcess = NULL;
    }
    if (pi.hThread != NULL) {
        CloseHandle(pi.hThread);
        pi.hThread = NULL;
    }
    if (file_handle != INVALID_HANDLE_VALUE) {
        // Убираем дублирующую запись строки в файл
        FlushFileBuffers(file_handle);
        CloseHandle(file_handle);
        file_handle = INVALID_HANDLE_VALUE;
    }
    if (pipe1_write != INVALID_HANDLE_VALUE) {
        FlushFileBuffers(pipe1_write);
        CloseHandle(pipe1_write);
        pipe1_write = INVALID_HANDLE_VALUE;
    }
    if (pipe2_read != INVALID_HANDLE_VALUE) {
        CloseHandle(pipe2_read);
        pipe2_read = INVALID_HANDLE_VALUE;
    }
}

BOOL WINAPI CtrlHandler(DWORD fdwCtrlType) {
    if (fdwCtrlType == CTRL_C_EVENT) {
        printf("\nПолучен сигнал завершения. Завершение работы...\n");
        running = FALSE;
        const char *exit_signal = "EXIT\n";
        WriteFile(pipe1_write, exit_signal, strlen(exit_signal), NULL, NULL);
        cleanup();
        return TRUE;
    }
    return FALSE;
}

int main() {
    SetConsoleOutputCP(CP_UTF8);

    HANDLE pipe1_read = INVALID_HANDLE_VALUE;
    HANDLE pipe2_write = INVALID_HANDLE_VALUE;
    SECURITY_ATTRIBUTES sa = {0};
    STARTUPINFO si = {0};
    BOOL success;
    char filename[BUFFER_SIZE];
    char input[BUFFER_SIZE];
    char error_message[BUFFER_SIZE];

    if (!SetConsoleCtrlHandler(CtrlHandler, TRUE)) {
        printf("ERROR: Could not set control handler\n");
        return 1;
    }

    printf("Введите имя файла для записи: ");
    fgets(filename, BUFFER_SIZE, stdin);
    filename[strcspn(filename, "\n")] = '\0';

    sa.nLength = sizeof(SECURITY_ATTRIBUTES);
    sa.bInheritHandle = TRUE;
    sa.lpSecurityDescriptor = NULL;
```

```
    if (!CreatePipe(&pipe1_read, &pipe1_write, &sa, 0)) {
        fprintf(stderr, "Ошибка при создании pipe1\n");
        return 1;
    }

    if (!CreatePipe(&pipe2_read, &pipe2_write, &sa, 0)) {
        fprintf(stderr, "Ошибка при создании pipe2\n");
        CloseHandle(pipe1_read);
        CloseHandle(pipe1_write);
        return 1;
    }

    si.cb = sizeof(si);
    si.hStdInput = pipe1_read;
    si.hStdOutput = GetStdHandle(STD_OUTPUT_HANDLE);
    si.hStdError = pipe2_write;
    si.dwFlags |= STARTF_USESTDHANDLES;

    if (!CreateProcess(NULL, "child.exe", NULL, NULL, TRUE, 0, NULL, NULL, &si, &pi)) {
        fprintf(stderr, "Ошибка при создании дочернего процесса\n");
        cleanup();
        return 1;
    }

    CloseHandle(pipe1_read);
    CloseHandle(pipe2_write);

    file_handle = CreateFile(filename, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL, NULL);
    if (file_handle == INVALID_HANDLE_VALUE) {
        fprintf(stderr, "Ошибка при открытии файла: %d\n", GetLastError());
        cleanup();
        return 1;
    }

    while (running) {
        printf("Введите строку (для выхода введите 'exit'): ");
        fgets(input, BUFFER_SIZE, stdin);
        input[strcspn(input, "\n")] = '\0';

        if (strcmp(input, "exit") == 0) {
            const char *exit_signal = "EXIT\n";
            WriteFile(pipe1_write, exit_signal, strlen(exit_signal), NULL, NULL);
            break;
        }

        DWORD bytes_written;
        success = WriteFile(pipe1_write, input, strlen(input), &bytes_written, NULL);
        if (!success || bytes_written != strlen(input)) {
            fprintf(stderr, "Ошибка при записи в pipe1\n");
            break;
        }

        WriteFile(pipe1_write, "\n", 1, &bytes_written, NULL);

        DWORD bytes_read;
        success = ReadFile(pipe2_read, error_message, BUFFER_SIZE - 1, &bytes_read, NULL);
        if (success && bytes_read > 0) {
            error_message[bytes_read] = '\0';
            printf("%s", error_message);
        } else {
            strncpy(last_input, input, BUFFER_SIZE);
            last_input[BUFFER_SIZE - 1] = '\0';
            DWORD bytes_written_to_file;
            WriteFile(file_handle, input, strlen(input), &bytes_written_to_file, NULL);
            WriteFile(file_handle, "\n", 1, &bytes_written_to_file, NULL);
            FlushFileBuffers(file_handle);
        }
    }

    cleanup();
```

```
    return 0;
}
```

**child.c**

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

#define BUFFER_SIZE 1024

int main() {
    HANDLE pipe1_read, pipe2_write;
    BOOL success;
    char buffer[BUFFER_SIZE];
    char line[BUFFER_SIZE];
    int line_pos = 0;

    pipe1_read = GetStdHandle(STD_INPUT_HANDLE);
    pipe2_write = GetStdHandle(STD_ERROR_HANDLE);

    while (1) {
        DWORD bytes_read;
        success = ReadFile(pipe1_read, buffer, BUFFER_SIZE - 1, &bytes_read, NULL);
        if (!success || bytes_read == 0)
            break;

        buffer[bytes_read] = '\0';

        for (int i = 0; i < bytes_read; i++) {
            if (buffer[i] == '\n' || line_pos == BUFFER_SIZE - 1) {
                line[line_pos] = '\0';

                if (strcmp(line, "EXIT") == 0) {
                    goto exit_loop;
                }

                printf("Чтение строки: '%s'\n", line);

                if (line_pos > 0 && isupper(line[0])) {
                    printf("%s\n", line);
                } else if (line_pos > 0) {
                    const char *error_message = "Ошибка: строка должна начинаться с
 заглавной буквы\n";
                    DWORD bytes_written;
                    success = WriteFile(pipe2_write, error_message,
 strlen(error_message), &bytes_written, NULL);
                    if (!success) {
                        fprintf(stderr, "Ошибка при записи в pipe2\n");
                        return 1;
                    }
                }

                line_pos = 0;
            } else {
                line[line_pos++] = buffer[i];
            }
        }
    }

exit_loop:
    CloseHandle(pipe1_read);
    CloseHandle(pipe2_write);

    return 0;
}
```

# Протокол работы программы

**Тестирование:**

PS D:\source> .\parent.exe
Введите имя файла для записи: outputs.txt
Введите строку (для выхода введите 'exit'): hello
Чтение строки: 'hello'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): Hello woorld
Чтение строки: 'Hello woorld'
Hello woorld

Получен сигнал завершения. Завершение работы...
PS D:\source> .\parent.exe
Введите имя файла для записи: hello
Введите строку (для выхода введите 'exit'): hello
Чтение строки: 'hello'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): Hello
Чтение строки: 'Hello'
Hello

Получен сигнал завершения. Завершение работы...
PS D:\source> .\parent.exe
Введите имя файла для записи: hello
Введите строку (для выхода введите 'exit'): hello
Чтение строки: 'hello'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): Hello
Чтение строки: 'Hello'
Hello

Получен сигнал завершения. Завершение работы...
PS D:\source> .\parent.exe
Введите имя файла для записи: hello.txt
Введите строку (для выхода введите 'exit'): 732
Чтение строки: '732'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): &32
Чтение строки: '&32'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): Е
Чтение строки: '  '
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): У
Чтение строки: '  '
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): Е
Чтение строки: 'Е'
Е

Получен сигнал завершения. Завершение работы...
PS D:\source> .\parent.exe
Введите имя файла для записи: hello.txt

Введите строку (для выхода введите 'exit'): hihihi
Чтение строки: 'hihihi'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): exit
PS D:\source>

**NTTrace:**

**parent_log.txt**

[7172] Process 7172 starting at 0000000000000000 with command line: ""D:\source\parent.exe""
D:\source\parent.exe
[7172] Loaded DLL at 00007FF801910000 C:\WINDOWS\SYSTEM32\ntdll.dll
[7172] Loaded DLL at 00007FF800610000 C:\WINDOWS\System32\KERNEL32.DLL
[7172] Loaded DLL at 00007FFFFEC00000 C:\WINDOWS\System32\KERNELBASE.dll
[7172] Loaded DLL at 00007FFFFF100000 C:\WINDOWS\System32\ucrtbase.dll
[7172] Created thread: 2024 at 00007FF8019E71E0
[7172] NtTestAlert() => 0
[7172] Initial breakpoint
[7172] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc
[ThreadAmILastThread], ThreadInformation=0x10071ffed8, Length=4, ReturnLength=null) => 0
[7172] Thread 2024 exit code: 0
[7172] NtReadFile(FileHandle=0, Event=0x1010, ApcRoutine=0x200b4a03f60,
ApcContext=0x7ffffec42f43, IoStatusBlock=0x1006ffee40 [0/7], Buffer=0x200b4a115b0,
Length=0x1000, ByteOffset=null, Key=null) => 0
[7172] NtOpenFile(FileHandle=0x1006ffef88 [0xb4],
DesiredAccess=SYNCHRONIZE|GENERIC_READ, ObjectAttributes="\Device\NamedPipe\",
IoStatusBlock=0x1006ffefa0 [0/1], ShareAccess=3, OpenOptions=0x20) => 0
[7172] NtCreateNamedPipeFile(NamedPipeHandle=0x1006ffef40 [0xb8],
DesiredAccess=SYNCHRONIZE|GENERIC_READ|0x100, ObjectAttributes=0xb4:"",
IoStatusBlock=0x1006ffefa0 [0/2], ShareAccess=3, CreateDisposition=2, CreateOptions=0x20,
MessageType=false, MessageRead=false, NonBlocking=false, MaxInstances=1,
InBufferSize=0x1000, OutBufferSize=0x1000, Timeout=0x1006ffef90 [-1.2e+09]) => 0
[7172] NtOpenFile(FileHandle=0x1006ffef98 [0xbc],
DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0xb8:"",
IoStatusBlock=0x1006ffefa0 [0/1], ShareAccess=3, OpenOptions=0x60) => 0
[7172] NtCreateNamedPipeFile(NamedPipeHandle=0x1006ffef40 [0xc0],
DesiredAccess=SYNCHRONIZE|GENERIC_READ|0x100, ObjectAttributes=0xb4:"",
IoStatusBlock=0x1006ffefa0 [0/2], ShareAccess=3, CreateDisposition=2, CreateOptions=0x20,
MessageType=false, MessageRead=false, NonBlocking=false, MaxInstances=1,
InBufferSize=0x1000, OutBufferSize=0x1000, Timeout=0x1006ffef90 [-1.2e+09]) => 0
[7172] NtOpenFile(FileHandle=0x1006ffef98 [0xc4],
DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0xc0:"",
IoStatusBlock=0x1006ffefa0 [0/1], ShareAccess=3, OpenOptions=0x60) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006ffce70
[0x00000200b4a13000], ZeroBits=0, pSize=0x1006ffcf18 [0x1000], flAllocationType=0x1000,
flProtect=4) => 0
[7172] NtQueryAttributesFile(ObjectAttributes="\??\D:\source\child.exe",
Attributes=0x1006ffcfb0 [ARCHIVE]) => 0
[7172] NtQueryAttributesFile(ObjectAttributes="\??\D:\source\child.exe",
Attributes=0x1006ffd388 [ARCHIVE]) => 0
[7172] NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c,
OpenAsSelf=false, TokenHandle=0x1006ffc810) => 0xc000007c [1008 '  .']

[7172] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x2a [ThreadDynamicCodePolicyInfo], ThreadInformation=0x1006ffc810, Length=4, ReturnLength=null) => 0
[7172] NtOpenSection(SectionHandle=0x1006ffc7a8 [0xc8], DesiredAccess=0xd, ObjectAttributes=0x44:"sechost.dll") => 0
[7172] Loaded DLL at 00007FF8006E0000 C:\WINDOWS\System32\sechost.dll
[7172] NtMapViewOfSection(SectionHandle=0xc8, ProcessHandle=-1, BaseAddress=0x200b4a08150 [0x00007ff8006e0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x200b4a0aa58 [0x000a8000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[7172] NtQueryPerformanceCounter(Counter=0x1006ffc600 [5.51839e+11], Freq=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffc590 [0x00007ff800783000], Size=0x1006ffc588 [0x1000], NewProtect=2, OldProtect=0x1006ffc580 [4]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffc610 [0x00007ff801aab000], Size=0x1006ffc608 [0x4000], NewProtect=4, OldProtect=0x1006ffc600 [2]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffc610 [0x00007ff801aab000], Size=0x1006ffc608 [0x4000], NewProtect=2, OldProtect=0x1006ffc600 [4]) => 0
[7172] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff8006e0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x1006ffc338, Length=0x30, ReturnLength=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffc650 [0x00007ff80075d000], Size=0x1006ffc658 [0x2000], NewProtect=4, OldProtect=0x200b4a0aa40 [2]) => 0
[7172] NtOpenSection(SectionHandle=0x1006ffc048 [0xcc], DesiredAccess=0xd, ObjectAttributes=0x44:"bcrypt.dll") => 0
[7172] Loaded DLL at 00007FFFFF030000 C:\WINDOWS\System32\bcrypt.dll
[7172] NtMapViewOfSection(SectionHandle=0xcc, ProcessHandle=-1, BaseAddress=0x200b4a138e0 [0x00007fffff030000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x200b4a07d68 [0x00028000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[7172] NtQueryPerformanceCounter(Counter=0x1006ffbea0 [5.51839e+11], Freq=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffbe30 [0x00007fffff055000], Size=0x1006ffbe28 [0x1000], NewProtect=2, OldProtect=0x1006ffbe20 [4]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffbeb0 [0x00007ff801aab000], Size=0x1006ffbea8 [0x4000], NewProtect=4, OldProtect=0x1006ffbea0 [2]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffbeb0 [0x00007ff801aab000], Size=0x1006ffbea8 [0x4000], NewProtect=2, OldProtect=0x1006ffbea0 [4]) => 0
[7172] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7fffff030000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x1006ffbbd8, Length=0x30, ReturnLength=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffbef0 [0x00007fffff04c000], Size=0x1006ffbef8 [0x1000], NewProtect=4, OldProtect=0x200b4a07d50 [2]) => 0
[7172] NtClose(Handle=0xcc) => 0
[7172] NtClose(Handle=0xc8) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x200b4a07d30 [0x00007fffff04c000], Size=0x200b4a07d38 [0x1000], NewProtect=2, OldProtect=0x1006ffc590 [4]) => 0

[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x200b4a0aa20 [0x00007ff80075d000], Size=0x200b4a0aa28 [0x2000], NewProtect=2, OldProtect=0x1006ffc590 [4]) => 0
[7172] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[7172] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[7172] NtTraceControl(CtrlCode=0xf, InputBuffer=0x1006ffc368, InputBufferLength=0xa0, OutputBuffer=0x1006ffc368, OutputBufferLength=0xa0, ReturnLength=0x1006ffc360 [0xa0]) => 0
[7172] NtTraceControl(CtrlCode=0xf, InputBuffer=0x1006ffc3c8, InputBufferLength=0xa0, OutputBuffer=0x1006ffc3c8, OutputBufferLength=0xa0, ReturnLength=0x1006ffc3c0 [0xa0]) => 0
[7172] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x56 [ProcessEnclaveInformation], ProcessInformation=0x1006ffc450, Length=0xb0, ReturnLength=null) => 0xc0000003 [87 '                    .']
[7172] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0 [ProcessBasicInformation], ProcessInformation=0x1006ffc3d0, Length=0x40, ReturnLength=null) => 0
[7172] NtTraceControl(CtrlCode=0xf, InputBuffer=0x1006ffc378, InputBufferLength=0xa0, OutputBuffer=0x1006ffc378, OutputBufferLength=0xa0, ReturnLength=0x1006ffc370 [0xa0]) => 0
[7172] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x1006ffc3c8, InputBufferLength=0x18, OutputBuffer=0x1006ffc3e0, OutputBufferLength=0x78, ReturnLength=0x1006ffc3c0 [0]) => 0
[7172] NtCreateSemaphore(SemaphoreHandle=0x1006ffc388 [0xd8], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0
[7172] NtCreateSemaphore(SemaphoreHandle=0x1006ffc398 [0xdc], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0
[7172] NtCreateEvent(EventHandle=0x1006ffc388 [0xe0], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
[7172] NtOpenFile(FileHandle=0x7fffff0527a0 [0xe4], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes="\Device\KsecDD", IoStatusBlock=0x1006ffc2d0 [0/0], ShareAccess=7, OpenOptions=0x20) => 0
[7172] NtDeviceIoControlFile(FileHandle=0xe4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffc370 [0/0], IoControlCode=0x00390400, InputBuffer=0x1006ffc450, InputBufferLength=0x68, OutputBuffer=0x1006ffc380, OutputBufferLength=8) => 0
[7172] NtTraceControl(CtrlCode=0xf, InputBuffer=0x1006ffc328, InputBufferLength=0xa0, OutputBuffer=0x1006ffc328, OutputBufferLength=0xa0, ReturnLength=0x1006ffc320 [0xa0]) => 0
[7172] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x1006ffc378, InputBufferLength=0x18, OutputBuffer=0x1006ffc390, OutputBufferLength=0x78, ReturnLength=0x1006ffc370 [0]) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006ffbd30 [0x00000200b4a14000], ZeroBits=0, pSize=0x1006ffbdd8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtTraceControl(CtrlCode=0xf, InputBuffer=0x1006ffc328, InputBufferLength=0xa0, OutputBuffer=0x1006ffc328, OutputBufferLength=0xa0, ReturnLength=0x1006ffc320 [0xa0]) => 0
[7172] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x1006ffc378, InputBufferLength=0x18, OutputBuffer=0x1006ffc390, OutputBufferLength=0x78, ReturnLength=0x1006ffc370 [0]) => 0
[7172] NtTraceControl(CtrlCode=0xf, InputBuffer=0x1006ffc358, InputBufferLength=0xa0, OutputBuffer=0x1006ffc358, OutputBufferLength=0xa0, ReturnLength=0x1006ffc350 [0xa0]) => 0
[7172] NtTraceControl(CtrlCode=0x1e, InputBuffer=0x1006ffc3a8, InputBufferLength=0x18, OutputBuffer=0x1006ffc3c0, OutputBufferLength=0x78, ReturnLength=0x1006ffc3a0 [0]) => 0

[7172] NtSetEvent(EventHandle=0x48, PrevState=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffcce8 [0x00007ffffef85000], Size=0x1006ffcce0 [0x1000], NewProtect=4, OldProtect=0x1006ffccf8 [2]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffcce8 [0x00007ffffef85000], Size=0x1006ffcce0 [0x1000], NewProtect=2, OldProtect=0x1006ffccf8 [4]) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006ffc9f0 [0x00000200b4a16000], ZeroBits=0, pSize=0x1006ffca98 [0x3000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffd258 [0xf4], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffd340, DesiredAccess=0x9, ObjectAttributes=0xf4:"child.exe") => 0xc0000034 [2 '  .']
[7172] NtOpenKey(KeyHandle=0x1006ffd320, DesiredAccess=0x101, ObjectAttributes="\Registry\Machine\Software\Microsoft\Wow64\x86\xtajit") => 0xc0000034 [2 ' .']
[7172] NtCreateUserProcess(ProcessHandle=0x1006ffd4d0 [0xfc], ThreadHandle=0x1006ffd550 [0xf8], ProcessDesiredAccess=MAXIMUM_ALLOWED, ThreadDesiredAccess=MAXIMUM_ALLOWED, ProcessObjectAttributes=null, ThreadObjectAttributes=null, ProcessFlags=0x204, ThreadFlags=1, ProcessParameters=0x200b4a14f20 ["D:\source\child.exe"], CreateInfo=0x1006ffd820, AttributeList=0x1006ffdcc0) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffd3e8, DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls") => 0xc0000034 [2 '  .']
[7172] NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0xa, TokenHandle=0x1006ffd0a0 [0xc8]) => 0
[7172] NtQueryInformationToken(TokenHandle=0xc8, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffd2f0, Length=0x90, ReturnLength=0x1006ffd0c8 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffd0c0, DesiredAccess=0x3, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") => 0xc0000034 [2 '  .']
[7172] NtOpenKey(KeyHandle=0x1006ffd088 [0xb0], DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0
[7172] NtQueryValueKey(KeyHandle=0xb0, ValueName="TransparentEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1006ffd1d0, Length=0x50, ResultLength=0x1006ffd080) => 0xc0000034 [2 '  .']
[7172] NtQueryValueKey(KeyHandle=0xb0, ValueName="AuthenticodeEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1006ffd1d0, Length=0x50, ResultLength=0x1006ffd080 [0x10]) => 0
[7172] NtClose(Handle=0xb0) => 0
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffcfb0, Length=0x58, ReturnLength=0x1006ffcfa8 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffd088, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 ' .']
[7172] NtClose(Handle=0xc8) => 0
[7172] NtTraceControl(CtrlCode=0xf, InputBuffer=0x1006ffd148, InputBufferLength=0xa0, OutputBuffer=0x1006ffd148, OutputBufferLength=0xa0, ReturnLength=0x1006ffd140 [0xa0]) => 0

[7172] NtQueryInformationProcess(ProcessHandle=0xfc, ProcessInformationClass=0x3c [ProcessCommandLineInformation], ProcessInformation=0x200b4a16970, Length=0x400, ReturnLength=0x1006ffd070 [0x24]) => 0
[7172] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0x1006ffcb50, Length=0x24, ReturnLength=null) => 0
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffccf0, Length=0x54, ReturnLength=0x1006ffccd0 [0x2c]) => 0
[7172] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0x1006ffcae0, Length=0x24, ReturnLength=null) => 0
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffce90, Length=0x58, ReturnLength=0x1006ffce88 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffd008 [0xb0], DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders") => 0
[7172] NtQueryValueKey(KeyHandle=0xb0, ValueName="Cache", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x200b4a16d80, Length=0x208, ResultLength=0x1006ffd000 [0x92]) => 0
[7172] NtClose(Handle=0xb0) => 0
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffce90, Length=0x58, ReturnLength=0x1006ffce88 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcfb0 [0xb0], DesiredAccess=0x8, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Microsoft\Windows NT\CurrentVersion") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcfb8 [0x108], DesiredAccess=0x101, ObjectAttributes=0xb0:"AppCompatFlags\Layers") => 0
[7172] NtQueryValueKey(KeyHandle=0x108, ValueName="D:\source\child.exe", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1006ffd018, Length=0x10, ResultLength=0x1006ffcfc0) => 0xc0000034 [2 '  .']
[7172] NtClose(Handle=0x108) => 0
[7172] NtApphelpCacheControl(ServiceClass=0xb, ServiceData="") => 0
[7172] NtQueryInformationProcess(ProcessHandle=0xfc, ProcessInformationClass=0 [ProcessBasicInformation], ProcessInformation=0x1006ffd310, Length=0x40, ReturnLength=null) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffd0c0 [0x108], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide") => 0
[7172] NtQueryValueKey(KeyHandle=0x108, ValueName="PreferExternalManifest", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1006ffd110, Length=0x14, ResultLength=0x1006ffd0c8) => 0xc0000034 [2 '  .']
[7172] NtClose(Handle=0x108) => 0
[7172] NtQueryVolumeInformationFile(FileHandle=0x100, IoStatusBlock=0x1006ffd120 [0/8], FsInformation=0x1006ffd150, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
[7172] NtGetMUIRegistryInfo(Flags=0, BufferLength=0x1006ffcf40 [0x4d0], Buffer=null) => 0
[7172] NtGetMUIRegistryInfo(Flags=0, BufferLength=0x1006ffcf40 [0x4d0], Buffer=0x200b4a14f20) => 0
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffcd70, Length=0x58, ReturnLength=0x1006ffcd68 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcf58 [0x108], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcf50, DesiredAccess=KEY_READ, ObjectAttributes=0x108:"Control Panel\Desktop\MuiCached\MachineLanguageConfiguration") => 0xc0000034 [2 '  .']

[7172] NtClose(Handle=0x108) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcde8, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '  .']
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffcc80, Length=0x58, ReturnLength=0x1006ffcc78 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcdf0 [0x108], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcdf8, DesiredAccess=KEY_READ, ObjectAttributes=0x108:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 '  .']
[7172] NtOpenKey(KeyHandle=0x1006ffcde8, DesiredAccess=KEY_READ, ObjectAttributes=0x108:"Control Panel\Desktop\LanguageConfiguration") => 0xc0000034 [2 '  .']
[7172] NtClose(Handle=0x108) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcd88, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '  .']
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffcbf0, Length=0x58, ReturnLength=0x1006ffcbe8 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcd80 [0x108], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffccb0, DesiredAccess=KEY_READ, ObjectAttributes=0x108:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 '  .']
[7172] NtOpenKey(KeyHandle=0x1006ffcd78 [0x10c], DesiredAccess=KEY_READ, ObjectAttributes=0x108:"Control Panel\Desktop") => 0
[7172] NtQueryValueKey(KeyHandle=0x10c, ValueName="PreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x200b4a0e0e0, Length=0xc, ResultLength=0x1006ffcd48) => 0xc0000034 [2 '  .']
[7172] NtClose(Handle=0x10c) => 0
[7172] NtClose(Handle=0x108) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcd88, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '  .']
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffcbf0, Length=0x58, ReturnLength=0x1006ffcbe8 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcd80 [0x110], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcd78 [0x114], DesiredAccess=KEY_READ, ObjectAttributes=0x110:"Control Panel\Desktop\MuiCached") => 0
[7172] NtQueryValueKey(KeyHandle=0x114, ValueName="MachinePreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x200b4a0e040, Length=0xc, ResultLength=0x1006ffcd48) => 0x80000005 [234 '  .']
[7172] NtQueryValueKey(KeyHandle=0x114, ValueName="MachinePreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x200b4a0de80, Length=0x18, ResultLength=0x1006ffcd48 [0x18]) => 0
[7172] NtClose(Handle=0x114) => 0
[7172] NtClose(Handle=0x110) => 0

[7172] NtOpenKey(KeyHandle=0x1006ffce28, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '  .']
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffcc90, Length=0x58, ReturnLength=0x1006ffcc88 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffce20 [0x118], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffcd50, DesiredAccess=KEY_READ, ObjectAttributes=0x118:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 '  .']
[7172] NtOpenKey(KeyHandle=0x1006ffce18 [0x11c], DesiredAccess=KEY_READ, ObjectAttributes=0x118:"Control Panel\Desktop") => 0
[7172] NtQueryValueKey(KeyHandle=0x11c, ValueName="PreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x200b4a0df40, Length=0xc, ResultLength=0x1006ffcde8) => 0xc0000034 [2 '  .']
[7172] NtClose(Handle=0x11c) => 0
[7172] NtClose(Handle=0x118) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffce68, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 '  .']
[7172] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x1006ffcd00, Length=0x58, ReturnLength=0x1006ffccf8 [0x2c]) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffce70 [0x118], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001") => 0
[7172] NtOpenKey(KeyHandle=0x1006ffce78, DesiredAccess=KEY_READ, ObjectAttributes=0x118:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 '  .']
[7172] NtOpenKey(KeyHandle=0x1006ffce68, DesiredAccess=KEY_READ, ObjectAttributes=0x118:"Control Panel\Desktop\LanguageConfiguration") => 0xc0000034 [2 '.']
[7172] NtClose(Handle=0x118) => 0
[7172] NtAlpcSendWaitReceivePort(PortHandle=0x68, SendFlags=0x00020000, SendMessage=0x1006ffe0b0 [2 [LPC_REPLY] (560b)], InMessageBuffer=null, ReceiveBuffer=0x1006ffe0b0, ReceiveBufferSize=0x1006ffd3c0 [0x258], OutMessageBuffer=null, Timeout=null) => 0
[7172] NtQueryLicenseValue(Name="Kernel-OneCore-DeviceFamilyID", Type=0x1006ffcfd8 [4], Buffer=0x1006ffcfd0, Length=4, ReturnedLength=0x1006ffd020 [4]) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=0xfc, lpAddress=0x1006ffd778 [0x000001baef690000], ZeroBits=0, pSize=0x1006ffd930 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtWriteVirtualMemory(ProcessHandle=0xfc, BaseAddress=0x1baef690000, Buffer=0x200b4a15400, BufferLength=0x11c0, ReturnedLength=null) => 0
[7172] NtWriteVirtualMemory(ProcessHandle=0xfc, BaseAddress=0x7fe132a2d8, Buffer=0x1006ffd778, BufferLength=8, ReturnedLength=null) => 0
[7172] NtResumeThread(ThreadHandle=0xf8, SuspendCount=null) => 0
[7172] NtClose(Handle=0x100) => 0
[7172] NtClose(Handle=0x104) => 0
[7172] NtClose(Handle=0xb8) => 0
[7172] NtClose(Handle=0xc4) => 0
[7172] NtCreateFile(FileHandle=0x1006ffee50 [0x120], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0x50:"hello",

IoStatusBlock=0x1006ffee58 [0/2], AllocationSize=null, FileAttributes=0x80, ShareAccess=0, CreateDisposition=5, CreateOptions=0x60, EaBuffer=null, EaLength=0) => 0
[7172] NtWriteFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffd410 [0/0x49], Buffer=0x1006ffd470, Length=0x49, ByteOffset=null, Key=null) => 0
[7172] NtDeviceIoControlFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffeca0 [0/0], IoControlCode=0x00500016, InputBuffer=0x1006ffecb0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0
[7172] NtReadFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffee40 [0/7], Buffer=0x200b4a115b0, Length=0x1000, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0 [0/5], Buffer=0x1006fff430, Length=5, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0 [0/1], Buffer=0x7ff6f43750bf, Length=1, ByteOffset=null, Key=null) => 0
[7172] NtReadFile(FileHandle=0xc0, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0 [0/0x5e], Buffer=0x1006fff030, Length=0x3ff, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffd410 [0/0x5f], Buffer=0x1006ffd470, Length=0x5f, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffd410 [0/0x49], Buffer=0x1006ffd470, Length=0x49, ByteOffset=null, Key=null) => 0
[7172] NtDeviceIoControlFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffeca0 [0/0], IoControlCode=0x00500016, InputBuffer=0x1006ffecb0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0
[7172] NtReadFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffee40 [0/7], Buffer=0x200b4a115b0, Length=0x1000, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0 [0/5], Buffer=0x1006fff430, Length=5, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0 [0/1], Buffer=0x7ff6f43750bf, Length=1, ByteOffset=null, Key=null) => 0
[7172] Created thread: 2260 at 00007FFFFED5CD10
[7172] NtDeviceIoControlFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x10071feda0, IoControlCode=0x00500016, InputBuffer=0x10071fedb0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '
.']
[7172] NtSetEvent(EventHandle=0x48, PrevState=null) => 0
[7172] NtTestAlert() => 0
[7172] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=3 [ThreadBasePriority], ThreadInformation=0x10071ffa38, Length=4) => 0
[7172] Exception: 40010005 at 00007FFFFED5CECE (first chance)
[7172] NtWriteFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x10071fe2e0 [0/0x5a], Buffer=0x10071fe340, Length=0x5a, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x10071ff9c0 [0/5], Buffer=0x7ff6f4375058, Length=5, ByteOffset=null, Key=null) => 0

[7172] NtReadFile(FileHandle=0xc0, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0, Buffer=0x1006fff030, Length=0x3ff, ByteOffset=null, Key=null) => 0xc000014b [109 '  .']
[7172] NtWriteFile(FileHandle=0x120, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0 [0/5], Buffer=0x1006fff430, Length=5, ByteOffset=null, Key=null) => 0
[7172] NtWriteFile(FileHandle=0x120, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x1006ffefb0 [0/1], Buffer=0x7ff6f43750bf, Length=1, ByteOffset=null, Key=null) => 0
[7172] NtWaitForSingleObject(Handle=0xfc, Alertable=false, Timeout=null) => 0
[7172] NtDuplicateObject(SourceProcess=-1, SourceHandle=0xfc, TargetProcess=-1, TargetHandle=0x10071fee30 [0xb8], DesiredAccess=0x1000, InheritMode=false, Options=0) => 0
[7172] NtQueryInformationProcess(ProcessHandle=0xb8, ProcessInformationClass=0 [ProcessBasicInformation], ProcessInformation=0x10071fedb0, Length=0x30, ReturnLength=null) => 0
[7172] NtQueryInformationProcess(ProcessHandle=0xb8, ProcessInformationClass=0x2b [ProcessImageFileNameWin32], ProcessInformation=0x10071fe7a0, Length=0x218, ReturnLength=null) => 0xc0000001 [31 '  .']
[7172] NtClose(Handle=0xb8) => 0
[7172] NtTerminateProcess(ProcessHandle=0xfc, ExitStatus=0) => 0xc000010a [5 '  .']
[7172] NtClose(Handle=0xfc) => 0
[7172] NtClose(Handle=0xf8) => 0
[7172] NtFlushBuffersFile(FileHandle=0x120, IoStatusBlock=0x1006ffefb0 [0/0]) => 0
[7172] NtFlushBuffersFile(FileHandle=0x120, IoStatusBlock=0x10071ff990 [0/0]) => 0
[7172] NtFlushBuffersFile(FileHandle=0x120, IoStatusBlock=0x1006ffef80 [0/0]) => 0
[7172] NtClose(Handle=0x120) => 0
[7172] Exception raised by attempted close of an invalid handle
[7172] NtFlushBuffersFile(FileHandle=0xbc, IoStatusBlock=0x10071ff990 [0/0]) => 0
[7172] NtClose(Handle=0xbc) => 0
[7172] NtClose(Handle=0xc0) => 0
[7172] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0x10071ffa38, Length=4, ReturnLength=null) => 0
[7172] NtSetEvent(EventHandle=0x48, PrevState=null) => 0
[7172] Thread 2260 exit code: 0
[7172] NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0x1006fff850) => 0xc000007c [1008 '  .']
[7172] NtOpenSection(SectionHandle=0x1006fff7e8, DesiredAccess=0xd, ObjectAttributes=0x44:"kernel.appcore.dll") => 0xc0000034 [2 '  .']
[7172] NtQueryAttributesFile(ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", Attributes=0x1006fff5a8 [ARCHIVE]) => 0
[7172] NtOpenFile(FileHandle=0x1006fff5b0 [0xbc], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0x1006fff618 [0/1], ShareAccess=5, OpenOptions=0x60) => 0
[7172] NtCreateSection(SectionHandle=0x1006fff5b8 [0x110], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xbc) => 0
[7172] Loaded DLL at 00007FFFFDCB0000 C:\WINDOWS\SYSTEM32\kernel.appcore.dll
[7172] NtMapViewOfSection(SectionHandle=0x110, ProcessHandle=-1, BaseAddress=0x200b4a0a2f0 [0x00007ffffdcb0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x200b4a0aa58 [0x00018000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[7172] NtQueryPerformanceCounter(Counter=0x1006fff430 [5.51928e+11], Freq=null) => 0

[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006fff3c0 [0x00007ffffdcc5000], Size=0x1006fff3b8 [0x1000], NewProtect=2, OldProtect=0x1006fff3b0 [4]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006fff440 [0x00007ff801aab000], Size=0x1006fff438 [0x4000], NewProtect=4, OldProtect=0x1006fff430 [2]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006fff440 [0x00007ff801aab000], Size=0x1006fff438 [0x4000], NewProtect=2, OldProtect=0x1006fff430 [4]) => 0
[7172] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffffdcb0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x1006fff168, Length=0x30, ReturnLength=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006fff480 [0x00007ffffdcba000], Size=0x1006fff488 [0x2000], NewProtect=4, OldProtect=0x200b4a0aa40 [2]) => 0
[7172] NtOpenSection(SectionHandle=0x1006ffee78 [0x114], DesiredAccess=0xd, ObjectAttributes=0x44:"msvcrt.dll") => 0
[7172] Loaded DLL at 00007FF801630000 C:\WINDOWS\System32\msvcrt.dll
[7172] NtMapViewOfSection(SectionHandle=0x114, ProcessHandle=-1, BaseAddress=0x200b4a0adb0 [0x00007ff801630000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x200b4a0f7e8 [0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[7172] NtQueryPerformanceCounter(Counter=0x1006ffecd0 [5.51928e+11], Freq=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffece0 [0x00007ff801aab000], Size=0x1006ffecd8 [0x4000], NewProtect=4, OldProtect=0x1006ffecd0 [2]) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffece0 [0x00007ff801aab000], Size=0x1006ffecd8 [0x4000], NewProtect=2, OldProtect=0x1006ffecd0 [4]) => 0
[7172] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff801630000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x1006ffea08, Length=0x30, ReturnLength=null) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1006ffed20 [0x00007ff8016ae000], Size=0x1006ffed28 [0x1000], NewProtect=4, OldProtect=0x200b4a0f7d0 [2]) => 0
[7172] NtClose(Handle=0x114) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x200b4a0aa20 [0x00007ffffdcba000], Size=0x200b4a0aa28 [0x2000], NewProtect=2, OldProtect=0x1006fff280 [4]) => 0
[7172] NtClose(Handle=0x110) => 0
[7172] NtClose(Handle=0xbc) => 0
[7172] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x200b4a0f7b0 [0x00007ff8016ae000], Size=0x200b4a0f7b8 [0x1000], NewProtect=2, OldProtect=0x1006fff5d0 [4]) => 0
[7172] NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0x1006fff530, Length=0x28) => 0
[7172] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[7172] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006fff200 [0x00000200b4bd0000], ZeroBits=0, pSize=0x1006fff208 [0x001b0000], flAllocationType=0x2000, flProtect=4) => 0
[7172] NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x1006fff200 [0x00000200b4bd0000], pSize=0x1006fff1f8 [0x001a0000], flFreeType=0x8000) => 0

[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006fff1e8 [0x00000200b4d70000], ZeroBits=0, pSize=0x1006fff1e0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0x1006fff4d0 [0/8], FsInformation=0x1006fff4f0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
[7172] NtQueryVolumeInformationFile(FileHandle=0x60, IoStatusBlock=0x1006fff4d0 [0/8], FsInformation=0x1006fff4f0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
[7172] NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0x1006fff4d0 [0/8], FsInformation=0x1006fff4f0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006ffeca0 [0x00000200b4d72000], ZeroBits=0, pSize=0x1006ffed48 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006ffeca0 [0x00000200b4d73000], ZeroBits=0, pSize=0x1006ffed48 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtOpenKey(KeyHandle=0x1006ffef70 [0xbc], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0
[7172] NtQueryValueKey(KeyHandle=0xbc, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1006ffefb0, Length=0x18, ResultLength=0x1006ffef78) => 0xc0000034 [2 '  .']
[7172] NtClose(Handle=0xbc) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006fff0c8 [0x00000200b4bd0000], ZeroBits=0, pSize=0x1006fff0d0 [0x00062000], flAllocationType=0x2000, flProtect=4) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006fff0c8 [0x00000200b4bd0000], ZeroBits=0, pSize=0x1006fff0d8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006fff100 [0x00000200b4d75000], ZeroBits=0, pSize=0x1006fff1a8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x1006fff0e0 [0x00000200b4d76000], ZeroBits=0, pSize=0x1006fff188 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[7172] NtSetEvent(EventHandle=0x48, PrevState=null) => 0
[7172] NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0x1006fff7f0, Length=0x330, ReturnLength=0x1006fff7a8) => 0xc0000225 [1168 '  .']
[7172] NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0x1006fff7f0, Length=0x330, ReturnLength=0x1006fff7a8) => 0xc0000225 [1168 '  .']
[7172] NtTerminateProcess(ProcessHandle=0, ExitStatus=0) => 0
[7172] NtClose(Handle=0xf0) => 0
[7172] NtClose(Handle=0xe8) => 0
[7172] NtClose(Handle=0xec) => 0
[7172] NtClose(Handle=0xcc) => 0
[7172] NtClose(Handle=0xd0) => 0
[7172] NtClose(Handle=0x5c) => 0
[7172] NtClose(Handle=0x94) => 0
[7172] NtClose(Handle=0x90) => 0
[7172] NtQueryWnfStateData(StateName=0x1006fff7c0 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x1006ffe70c [0x8c20], Buffer=0x1006ffe760, BufferSize=0x1006ffe708 [0x6c4]) => 0
[7172] NtClose(Handle=0x80) => 0

[7172] NtClose(Handle=0x6c) => 0
[7172] Process 7172 exit code: 0

child_log.txt

[11856] Process 11856 starting at 0000000000000000 with command line: "child.exe" D:\source\child.exe
[11856] Loaded DLL at 00007FF801910000 C:\WINDOWS\SYSTEM32\ntdll.dll
[11856] Loaded DLL at 00007FF800610000 C:\WINDOWS\System32\KERNEL32.DLL
[11856] Loaded DLL at 00007FFFFEC00000 C:\WINDOWS\System32\KERNELBASE.dll
[11856] Loaded DLL at 00007FFFFF100000 C:\WINDOWS\System32\ucrtbase.dll
[11856] Created thread: 14596 at 00007FF8019E71E0
[11856] NtTestAlert() => 0
[11856] Initial breakpoint
[11856] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xbf8fdffdb8, Length=4, ReturnLength=null) => 0
[11856] Thread 14596 exit code: 0
[11856] NtReadFile(FileHandle=0, Event=0x0000020269cd0060, ApcRoutine=0xbf8fbff158, ApcContext=null, IoStatusBlock=0xbf8fbff170 [0/5], Buffer=0xbf8fbff5d0, Length=0x3ff, ByteOffset=null, Key=null) => 0
[11856] NtReadFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbff170 [0/1], Buffer=0xbf8fbff5d0, Length=0x3ff, ByteOffset=null, Key=null) => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfe730 [0x0000020269cd1000], ZeroBits=0, pSize=0xbf8fbfe7d8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtWriteFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbfd5d0 [0/0x24], Buffer=0xbf8fbfd630, Length=0x24, ByteOffset=null, Key=null) => 0
[11856] NtWriteFile(FileHandle=0xc0, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbff170 [0/0x5e], Buffer=0x7ff73c694030, Length=0x5e, ByteOffset=null, Key=null) => 0
[11856] NtReadFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbff170 [0/5], Buffer=0xbf8fbff5d0, Length=0x3ff, ByteOffset=null, Key=null) => 0
[11856] NtReadFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbff170 [0/1], Buffer=0xbf8fbff5d0, Length=0x3ff, ByteOffset=null, Key=null) => 0
[11856] NtWriteFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbfd5d0 [0/0x24], Buffer=0xbf8fbfd630, Length=0x24, ByteOffset=null, Key=null) => 0
[11856] NtWriteFile(FileHandle=0x60, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbfda90 [0/7], Buffer=0xbf8fbfdaf0, Length=7, ByteOffset=null, Key=null) => 0
[11856] Created thread: 9088 at 00007FFFFED5CD10
[11856] NtReadFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fbff170 [0/5], Buffer=0xbf8fbff5d0, Length=0x3ff, ByteOffset=null, Key=null) => 0
[11856] NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xbf8fdfece0, IoControlCode=0x00500016, InputBuffer=0xbf8fdfecf0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '.']
[11856] NtSetEvent(EventHandle=0x50, PrevState=null) => 0
[11856] NtTestAlert() => 0

[11856] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=3 [ThreadBasePriority], ThreadInformation=0xbf8fdff978, Length=4) => 0
[11856] Exception: 40010005 at 00007FFFFED5CECE (first chance)
[11856] NtClose(Handle=0xb4) => 0
[11856] NtClose(Handle=0xc0) => 0
[11856] NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0xbf8fbff560) => 0xc000007c [1008 '                    .']
[11856] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x2a [ThreadDynamicCodePolicyInfo], ThreadInformation=0xbf8fbff560, Length=4, ReturnLength=null) => 0
[11856] NtOpenSection(SectionHandle=0xbf8fbff4f8, DesiredAccess=0xd, ObjectAttributes=0x4c:"kernel.appcore.dll") => 0xc0000034 [2 '                    .']
[11856] NtQueryAttributesFile(ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", Attributes=0xbf8fbff2b8 [ARCHIVE]) => 0
[11856] NtOpenFile(FileHandle=0xbf8fbff2c0 [0xc0], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0xbf8fbff328 [0/1], ShareAccess=5, OpenOptions=0x60) => 0
[11856] NtWaitForSingleObject(Handle=0x50, Alertable=false, Timeout=null) => 0
[11856] NtCreateSection(SectionHandle=0xbf8fbff2c8 [0xb4], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xc0) => 0
[11856] Loaded DLL at 00007FFFFDCB0000 C:\WINDOWS\SYSTEM32\kernel.appcore.dll
[11856] NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x20269cc8130 [0x00007ffffdcb0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x20269ccaa38 [0x00018000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[11856] NtQueryPerformanceCounter(Counter=0xbf8fbff140 [5.53203e+11], Freq=null) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbf8fbff0d0 [0x00007ffffdcc5000], Size=0xbf8fbff0c8 [0x1000], NewProtect=2, OldProtect=0xbf8fbff0c0 [4]) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbf8fbff150 [0x00007ff801aab000], Size=0xbf8fbff148 [0x4000], NewProtect=4, OldProtect=0xbf8fbff140 [2]) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbf8fbff150 [0x00007ff801aab000], Size=0xbf8fbff148 [0x4000], NewProtect=2, OldProtect=0xbf8fbff140 [4]) => 0
[11856] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffffdcb0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xbf8fbfee78, Length=0x30, ReturnLength=null) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbf8fbff190 [0x00007ffffdcba000], Size=0xbf8fbff198 [0x2000], NewProtect=4, OldProtect=0x20269ccaa20 [2]) => 0
[11856] NtOpenSection(SectionHandle=0xbf8fbfeb88 [0x14], DesiredAccess=0xd, ObjectAttributes=0x4c:"msvcrt.dll") => 0
[11856] Loaded DLL at 00007FF801630000 C:\WINDOWS\System32\msvcrt.dll
[11856] NtMapViewOfSection(SectionHandle=0x14, ProcessHandle=-1, BaseAddress=0x20269ccae20 [0x00007ff801630000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x20269ccada8 [0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[11856] NtQueryPerformanceCounter(Counter=0xbf8fbfe9e0 [5.53203e+11], Freq=null) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbf8fbfe9f0 [0x00007ff801aab000], Size=0xbf8fbfe9e8 [0x4000], NewProtect=4, OldProtect=0xbf8fbfe9e0 [2]) => 0

[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbf8fbfe9f0 [0x00007ff801aab000], Size=0xbf8fbfe9e8 [0x4000], NewProtect=2, OldProtect=0xbf8fbfe9e0 [4]) => 0
[11856] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff801630000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xbf8fbfe718, Length=0x30, ReturnLength=null) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbf8fbfea30 [0x00007ff8016ae000], Size=0xbf8fbfea38 [0x1000], NewProtect=4, OldProtect=0x20269ccad90 [2]) => 0
[11856] NtClose(Handle=0x14) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x20269ccaa00 [0x00007ffffdcba000], Size=0x20269ccaa08 [0x2000], NewProtect=2, OldProtect=0xbf8fbfef90 [4]) => 0
[11856] NtClose(Handle=0xb4) => 0
[11856] NtClose(Handle=0xc0) => 0
[11856] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x20269ccad70 [0x00007ff8016ae000], Size=0x20269ccad78 [0x1000], NewProtect=2, OldProtect=0xbf8fbff2e0 [4]) => 0
[11856] NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0x20269ccda00, Length=0x40) => 0
[11856] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[11856] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfef10 [0x0000020269e90000], ZeroBits=0, pSize=0xbf8fbfef18 [0x000b0000], flAllocationType=0x2000, flProtect=4) => 0
[11856] NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfef10 [0x0000020269e90000], pSize=0xbf8fbfef08 [0x000a0000], flFreeType=0x8000) => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfeef8 [0x0000020269f30000], ZeroBits=0, pSize=0xbf8fbfeef0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtQueryVolumeInformationFile(FileHandle=0xb4, IoStatusBlock=0xbf8fbff1e0, FsInformation=0xbf8fbff200, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0xc0000008 [6 '                    .']
[11856] NtQueryVolumeInformationFile(FileHandle=0x60, IoStatusBlock=0xbf8fbff1e0 [0/8], FsInformation=0xbf8fbff200, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
[11856] NtQueryVolumeInformationFile(FileHandle=0xc0, IoStatusBlock=0xbf8fbff1e0, FsInformation=0xbf8fbff200, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0xc0000008 [6 '                    .']
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfee40 [0x0000020269cd3000], ZeroBits=0, pSize=0xbf8fbfeee8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfe9b0 [0x0000020269f32000], ZeroBits=0, pSize=0xbf8fbfea58 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfe9b0 [0x0000020269f33000], ZeroBits=0, pSize=0xbf8fbfea58 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtOpenKey(KeyHandle=0xbf8fbfec80 [0xc0], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0
[11856] NtQueryValueKey(KeyHandle=0xc0, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xbf8fbfecc0, Length=0x18, ResultLength=0xbf8fbfec88) => 0xc0000034 [2 '                              .']
[11856] NtClose(Handle=0xc0) => 0

[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfedd8 [0x0000020269e90000], ZeroBits=0, pSize=0xbf8fbfede0 [0x00062000], flAllocationType=0x2000, flProtect=4) => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfedd8 [0x0000020269e90000], ZeroBits=0, pSize=0xbf8fbfede8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfee10 [0x0000020269f35000], ZeroBits=0, pSize=0xbf8fbfeeb8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbf8fbfedf0 [0x0000020269f36000], ZeroBits=0, pSize=0xbf8fbfee98 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[11856] NtSetEvent(EventHandle=0x50, PrevState=null) => 0
[11856] NtWaitForSingleObject(Handle=0x50, Alertable=false, Timeout=null) => 0
[11856] Thread 17896 exit code: 3221225786
[11856] NtTerminateProcess(ProcessHandle=0, ExitStatus=0xc000013a) => 0
[11856] NtClose(Handle=0x74) => 0
[11856] NtClose(Handle=0xa0) => 0
[11856] NtClose(Handle=0x9c) => 0
[11856] NtQueryWnfStateData(StateName=0xbf8fdff4c0 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xbf8fdfe40c [0x8c22], Buffer=0xbf8fdfe460, BufferSize=0xbf8fdfe408 [0x6d4]) => 0
[11856] NtClose(Handle=0x8c) => 0
[11856] NtClose(Handle=0x78) => 0
[11856] Process 11856 exit code: 3221225786

## Вывод

**В ходе работы изначальная задача была выполнена, а также решены проблемы с завершением программы и корректной обработкой данных между процессами через пайпы. Также были устранены ошибки записи данных в конечный файл, что обеспечило успешную передачу и сохранение результатов.**