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.

Оценка: _____

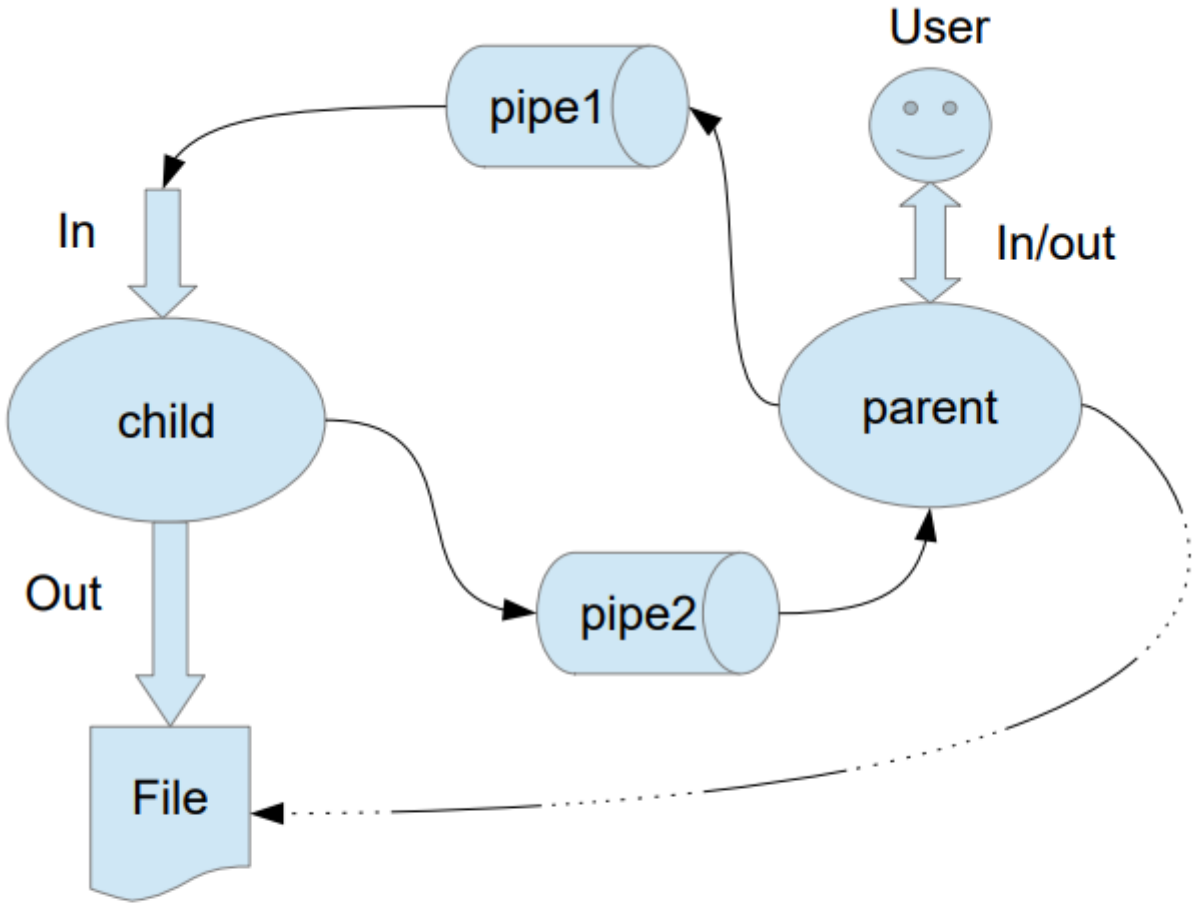
Дата: 16.10.24

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:

- **GetStdHandle** — используется для получения дескрипторов стандартных потоков ввода и вывода;
- **ReadFile** — считывает данные из pipe (канала связи между процессами) в буфер. Если нет данных или произошла ошибка, возвращает FALSE;
- **WriteFile** — записывает данные в pipe, который в родительском процессе воспринимается как стандартный поток ошибок. Используется для отправки сообщений об ошибках;

- **WriteConsole** — выводит строки в консоль, заменяя стандартный printf. Используется для вывода сообщений, считанных строк и ошибок.
- **CloseHandle** — закрывает дескрипторы pipe для завершения взаимодействия между процессами;
- **SetConsoleCtrlHandler** — регистрирует обработчик для обработки событий консоли (например, нажатия Ctrl+C). В данном случае используется для завершения дочернего процесса корректно при прерывании программы.
- **CreatePipe** — создает неименованные каналы (pipes) для межпроцессного взаимодействия;
- **CreateProcess** — запускает дочерний процесс child.exe, перенаправляя стандартный ввод на первый pipe, стандартный вывод на консоль, а стандартный поток ошибок на второй pipe;
- **CreateFile** — открывает или создает файл для записи данных, введенных пользователем. Используется для сохранения строк в файл;
- **FlushFileBuffers** — сбрасывает буферы файлового ввода/вывода, чтобы убедиться, что все данные записаны в файл или pipe;
- **TerminateProcess и WaitForSingleObject** — завершают и ожидают завершения дочернего процесса для корректного завершения работы программы.

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 <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) {
        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) {
        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)) {
        return 1;
    }

    const char *prompt = "Enter the file name for writing: ";
```

```
    WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), prompt, strlen(prompt), NULL, NULL);
    DWORD bytes_read;
    ReadFile(GetStdHandle(STD_INPUT_HANDLE), filename, BUFFER_SIZE - 1, &bytes_read,
NULL);
    filename[bytes_read - 1] = '\0';

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

    if (!CreatePipe(&pipe1_read, &pipe1_write, &sa, 0)) {
        return 1;
    }

    if (!CreatePipe(&pipe2_read, &pipe2_write, &sa, 0)) {
        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)) {
        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) {
        cleanup();
        return 1;
    }

    while (running) {
        const char *input_prompt = "Enter a string (type 'exit' to quit): ";
        WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), input_prompt, strlen(input_prompt),
NULL, NULL);
        ReadFile(GetStdHandle(STD_INPUT_HANDLE), input, BUFFER_SIZE - 1, &bytes_read,
NULL);
        input[bytes_read - 1] = '\0';

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

```
        if (input[0] < 'A' || input[0] > 'Z') {
            const char *error_message = "Error: The string must start with an uppercase letter.\n";
            WriteFile(GetStdHandle(STD_ERROR_HANDLE), error_message, strlen(error_message),
NULL, NULL);
            continue;
        }

        DWORD bytes_written;
        success = WriteFile(pipe1_write, input, strlen(input), &bytes_written, NULL);
        if (!success || bytes_written != strlen(input)) {
            break;
        }

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

        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);

        const char *success_message = "The line has been successfully written to the file.\n";
        WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), success_message,
strlen(success_message), NULL, NULL);
    }

    cleanup();

    return 0;
}
```

child.c

```
#include <windows.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;
                }

                DWORD bytes_written;
                char message[BUFFER_SIZE * 2];
                int message_len = wsprintfA(message, "Чтение строки: '%s'\r\n",
line);
                WriteConsole(GetStdHandle(STD_OUTPUT_HANDLE), message, message_len,
&bytes_written, NULL);

                if (line_pos > 0 && isupper(line[0])) {
                    WriteConsole(GetStdHandle(STD_OUTPUT_HANDLE), line, line_pos,
&bytes_written, NULL);
                    WriteConsole(GetStdHandle(STD_OUTPUT_HANDLE), "\r\n", 2,
&bytes_written, NULL);
                } else if (line_pos > 0) {
                    const char *error_message = "Ошибка: строка должна начинаться с
заглавной буквы\r\n";
                    DWORD bytes_written;
                    success = WriteFile(pipe2_write, error_message,
strlen(error_message), &bytes_written, NULL);
                    if (!success) {
                        char err_msg[] = "Ошибка при записи в pipe2\r\n";
                        WriteConsole(GetStdHandle(STD_ERROR_HANDLE), err_msg,
strlen(err_msg), &bytes_written, NULL);
                        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:\lab0001> .\parent.exe
Введите имя файла для записи: outputik.txt
Введите строку (для выхода введите 'exit'): hello world
Чтение строки: 'hello world'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): 76518
Чтение строки: '76518'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): -?
Чтение строки: '-?'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): %
Чтение строки: '%'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): Hello World Bro
Чтение строки: 'Hello World Bro'
Hello World Bro

Получен сигнал завершения. Завершение работы...
PS D:\lab0001> .\parent.exe
Введите имя файла для записи: output
Введите строку (для выхода введите 'exit'): привет
Чтение строки: '��'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): Привет
Чтение строки: '��'
Ошибка: строка должна начинаться с заглавной буквы
Введите строку (для выхода введите 'exit'): exit
PS D:\lab0001>
```

NTTrace:

parent_log.txt

```
[1768] Process 1768 starting at 0000000000000000 with command line: ""D:\lab0001\parent.exe""
D:\lab0001\parent.exe
[1768] Loaded DLL at 00007FF801910000 C:\WINDOWS\SYSTEM32\ntdll.dll
[1768] Loaded DLL at 0000000076F90000 C:\WINDOWS\SYSTEM32\ntdll.dll
[1768] Loaded DLL at 00007FF800520000 C:\WINDOWS\System32\wow64.dll
[1768] Loaded DLL at 00007FF800600000 C:\WINDOWS\System32\wow64base.dll
[1768] Loaded DLL at 00007FF801840000 C:\WINDOWS\System32\wow64win.dll
[1768] Loaded DLL at 00007FF800950000 C:\WINDOWS\System32\wow64con.dll
[1768] Loaded DLL at 0000000076F80000 C:\WINDOWS\System32\wow64cpu.dll
[1768] Loaded DLL at 00000000761A0000 C:\WINDOWS\System32\KERNEL32.DLL
[1768] Loaded DLL at 0000000076CF0000 C:\WINDOWS\System32\KERNELBASE.dll
[1768] Loaded DLL at 0000000076320000 C:\WINDOWS\System32\msvcrt.dll
[1768] Loaded DLL at 0000000076750000 C:\WINDOWS\System32\USER32.dll
[1768] Loaded DLL at 0000000076C90000 C:\WINDOWS\System32\win32u.dll
[1768] Loaded DLL at 00000000752F0000 C:\WINDOWS\System32\GDI32.dll
[1768] Loaded DLL at 0000000075200000 C:\WINDOWS\System32\gdi32full.dll
[1768] Loaded DLL at 0000000076590000 C:\WINDOWS\System32\msvcp_win.dll
[1768] Loaded DLL at 0000000076B70000 C:\WINDOWS\System32\ucrtbase.dll
[1768] Loaded DLL at 0000000076CC0000 C:\WINDOWS\System32\IMM32.DLL
[1768] Created thread: 3480 at 00007FF8019E71E0
[1768] NtTestAlert() => 0
```

[1768] Initial breakpoint
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0x7afc58, Length=4, ReturnLength=null) => 0
[1768] Thread 3480 exit code: 0
[1768] NtOpenFile(FileHandle=0x9e448 [0x11c], DesiredAccess=SYNCHRONIZE|GENERIC_READ, ObjectAttributes="\Device\NamedPipe\", IoStatusBlock=0x9e3e8 [0/1], ShareAccess=3, OpenOptions=0x20) => 0
[1768] NtQueryObject(ObjectHandle=0x11c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e0b0, Length=0x210, ReturnLength=null) => 0
[1768] NtCreateNamedPipeFile(NamedPipeHandle=0x9e3d8 [0x120], DesiredAccess=SYNCHRONIZE|GENERIC_READ|0x100, ObjectAttributes=0x11c:"", IoStatusBlock=0x9e3f0 [0/2], ShareAccess=3, CreateDisposition=2, CreateOptions=0x20, MessageType=false, MessageRead=false, NonBlocking=false, MaxInstances=1, InBufferSize=0x1000, OutBufferSize=0x1000, Timeout=0x61ee18 [-1.2e+09]) => 0
[1768] NtQueryObject(ObjectHandle=0x120, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e110, Length=0x210, ReturnLength=null) => 0xc0000039 [161 '   .']
[1768] NtQueryDebugFilterState(Component=0x68, Level=1) => 0
[1768] NtOpenFile(FileHandle=0x9e448 [0x124], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0x120:"", IoStatusBlock=0x9e3e8 [0/1], ShareAccess=3, OpenOptions=0x60) => 0
[1768] NtQueryObject(ObjectHandle=0x11c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e0b0, Length=0x210, ReturnLength=null) => 0
[1768] NtCreateNamedPipeFile(NamedPipeHandle=0x9e3d8 [0x128], DesiredAccess=SYNCHRONIZE|GENERIC_READ|0x100, ObjectAttributes=0x11c:"", IoStatusBlock=0x9e3f0 [0/2], ShareAccess=3, CreateDisposition=2, CreateOptions=0x20, MessageType=false, MessageRead=false, NonBlocking=false, MaxInstances=1, InBufferSize=0x1000, OutBufferSize=0x1000, Timeout=0x61ee18 [-1.2e+09]) => 0
[1768] NtQueryObject(ObjectHandle=0x128, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e110, Length=0x210, ReturnLength=null) => 0xc0000039 [161 '   .']
[1768] NtQueryDebugFilterState(Component=0x68, Level=1) => 0
[1768] NtOpenFile(FileHandle=0x9e448 [0x12c], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0x128:"", IoStatusBlock=0x9e3e8 [0/1], ShareAccess=3, OpenOptions=0x60) => 0
[1768] NtQueryAttributesFile(ObjectAttributes="\??\D:\lab0001\child.exe", Attributes=0x9e3d8 [ARCHIVE]) => 0
[1768] NtQueryAttributesFile(ObjectAttributes="\??\D:\lab0001\child.exe", Attributes=0x9e3d8 [ARCHIVE]) => 0
[1768] NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0x9e440) => 0xc000007c [1008 '   .']
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x2a [ThreadDynamicCodePolicyInfo], ThreadInformation=0x61d56c, Length=4, ReturnLength=null) => 0
[1768] NtQueryObject(ObjectHandle=0x9c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e150, Length=0x210, ReturnLength=null) => 0
[1768] NtOpenSection(SectionHandle=0x9e448 [0x130], DesiredAccess=0xd, ObjectAttributes=0x9c:"sechost.dll") => 0
[1768] Loaded DLL at 0000000076610000 C:\WINDOWS\SysWOW64\sechost.dll
[1768] NtMapViewOfSection(SectionHandle=0x130, ProcessHandle=-1, BaseAddress=0x9e400 [0x76610000], ZeroBits=0x7ffeffff, CommitSize=0, SectionOffset=null, ViewSize=0x9e3f8 [0x00085000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[1768] NtQuerySection(SectionHandle=0x130, SectionInformationClass=1 [SectionImageInformation], SectionInformation=0x9e320, Length=0x40, ReturnLength=null) => 0

[1768] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x76610000, MemoryInformationClass=6 [MemoryImageInformation], MemoryInformation=0x9e2c0, Length=0x18, ReturnLength=null) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x7668d000], Size=0x9e3f8 [0x1000], NewProtect=2, OldProtect=0x9e3c4 [4]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x770c2000], Size=0x9e3f8 [0x3000], NewProtect=4, OldProtect=0x9e3c4 [2]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x770c2000], Size=0x9e3f8 [0x3000], NewProtect=2, OldProtect=0x9e3c4 [4]) => 0
[1768] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x76610000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x9e370, Length=0x30, ReturnLength=0x9e3e8 [0x30]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x7668a000], Size=0x9e3f8 [0x1000], NewProtect=4, OldProtect=0x9e3c4 [2]) => 0
[1768] NtQueryObject(ObjectHandle=0x9c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e150, Length=0x210, ReturnLength=null) => 0
[1768] NtOpenSection(SectionHandle=0x9e448 [0x134], DesiredAccess=0xd, ObjectAttributes=0x9c:"bcrypt.dll") => 0
[1768] Loaded DLL at 0000000076550000 C:\WINDOWS\SysWOW64\bcrypt.dll
[1768] NtMapViewOfSection(SectionHandle=0x134, ProcessHandle=-1, BaseAddress=0x9e400 [0x76550000], ZeroBits=0x7ffeffff, CommitSize=0, SectionOffset=null, ViewSize=0x9e3f8 [0x0001a000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0
[1768] NtQuerySection(SectionHandle=0x134, SectionInformationClass=1 [SectionImageInformation], SectionInformation=0x9e320, Length=0x40, ReturnLength=null) => 0
[1768] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x76550000, MemoryInformationClass=6 [MemoryImageInformation], MemoryInformation=0x9e2c0, Length=0x18, ReturnLength=null) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x76567000], Size=0x9e3f8 [0x1000], NewProtect=2, OldProtect=0x9e3c4 [4]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x770c2000], Size=0x9e3f8 [0x3000], NewProtect=4, OldProtect=0x9e3c4 [2]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x770c2000], Size=0x9e3f8 [0x3000], NewProtect=2, OldProtect=0x9e3c4 [4]) => 0
[1768] NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x76550000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x9e370, Length=0x30, ReturnLength=0x9e3e8 [0x30]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x76566000], Size=0x9e3f8 [0x1000], NewProtect=4, OldProtect=0x9e3c4 [2]) => 0
[1768] Created thread: 20136 at 0000000076FCEF40
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0xbbfd24, Length=0x2cc, ReturnLength=null) => 0
[1768] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0xbbfd24, Length=0x2cc) => 0
[1768] NtTestAlert() => 0
[1768] NtWaitForWorkViaWorkerFactory(WorkerFactoryHandle=0xe8, MiniPacket=0x7aeea0) => 0
[1768] Created thread: 20748 at 0000000076FCEF40
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x76566000], Size=0x9e3f8 [0x1000], NewProtect=2, OldProtect=0x9e3c4 [4]) => 0
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0xdbfd24, Length=0x2cc, ReturnLength=null) => 0
[1768] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0xdbfd24, Length=0x2cc) => 0
[1768] NtTestAlert() => 0

[1768] NtWaitForWorkViaWorkerFactory(WorkerFactoryHandle=0xe8, MiniPacket=0x7eeea0) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ae7d0 [0x7668a000], Size=0x7ae7c8 [0x1000], NewProtect=2, OldProtect=0x7ae794 [4]) => 0
[1768] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[1768] NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
[1768] NtTraceControl(CtrlCode=0x8000000f, InputBuffer=0x61d298, InputBufferLength=0xa0, OutputBuffer=0x61d298, OutputBufferLength=0xa0, ReturnLength=0x61d28c [0xa0]) => 0
[1768] NtTraceControl(CtrlCode=0x8000000f, InputBuffer=0x61d2e0, InputBufferLength=0xa0, OutputBuffer=0x61d2e0, OutputBufferLength=0xa0, ReturnLength=0x61d2d4 [0xa0]) => 0
[1768] NtTraceControl(CtrlCode=0x8000000f, InputBuffer=0x61d2b8, InputBufferLength=0xa0, OutputBuffer=0x61d2b8, OutputBufferLength=0xa0, ReturnLength=0x61d2ac [0xa0]) => 0
[1768] NtTraceControl(CtrlCode=0x8000001e, InputBuffer=0x61d380, InputBufferLength=0x18, OutputBuffer=0x61d308, OutputBufferLength=0x78, ReturnLength=0x61d300 [0]) => 0
[1768] NtCreateSemaphore(SemaphoreHandle=0x9e448 [0x13c], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0
[1768] NtCreateSemaphore(SemaphoreHandle=0x9e448 [0x140], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0
[1768] NtCreateEvent(EventHandle=0x9e448 [0x144], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
[1768] NtOpenFile(FileHandle=0x9e448 [0x148], DesiredAccess=SYNCHRONIZE|0x3, ObjectAttributes="\Device\KsecDD", IoStatusBlock=0x9e3e8 [0/0], ShareAccess=7, OpenOptions=0x20) => 0
[1768] NtTraceControl(CtrlCode=0x8000000f, InputBuffer=0x61d278, InputBufferLength=0xa0, OutputBuffer=0x61d278, OutputBufferLength=0xa0, ReturnLength=0x61d26c [0xa0]) => 0
[1768] NtTraceControl(CtrlCode=0x8000001e, InputBuffer=0x61d340, InputBufferLength=0x18, OutputBuffer=0x61d2c8, OutputBufferLength=0x78, ReturnLength=0x61d2c0 [0]) => 0
[1768] NtTraceControl(CtrlCode=0x8000000f, InputBuffer=0x61d280, InputBufferLength=0xa0, OutputBuffer=0x61d280, OutputBufferLength=0xa0, ReturnLength=0x61d274 [0xa0]) => 0
[1768] NtTraceControl(CtrlCode=0x8000001e, InputBuffer=0x61d348, InputBufferLength=0x18, OutputBuffer=0x61d2d0, OutputBufferLength=0x78, ReturnLength=0x61d2c8 [0]) => 0
[1768] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x9e400 [0x008d4000], ZeroBits=0, pSize=0x9e3f0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[1768] NtTraceControl(CtrlCode=0x8000000f, InputBuffer=0x61d278, InputBufferLength=0xa0, OutputBuffer=0x61d278, OutputBufferLength=0xa0, ReturnLength=0x61d26c [0xa0]) => 0
[1768] NtTraceControl(CtrlCode=0x8000001e, InputBuffer=0x61d340, InputBufferLength=0x18, OutputBuffer=0x61d2c8, OutputBufferLength=0x78, ReturnLength=0x61d2c0 [0]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x76f37000], Size=0x9e3f8 [0x1000], NewProtect=4, OldProtect=0x9e3c4 [2]) => 0
[1768] NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x9e400 [0x76f37000], Size=0x9e3f8 [0x1000], NewProtect=2, OldProtect=0x9e3c4 [4]) => 0
[1768] NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x9e400 [0x008d6000], ZeroBits=0, pSize=0x9e3f0 [0x3000], flAllocationType=0x1000, flProtect=4) => 0
[1768] NtQueryObject(ObjectHandle=0xac, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0xac, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=0x9, ObjectAttributes=0xac:"child.exe", OpenOptions=0) => 0xc0000034 [2 '   .']
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=0x101, ObjectAttributes="\Registry\Machine\Software\Microsoft\Wow64\x86\xtajit", OpenOptions=0) => 0xc0000034 [2 '   .']

[1768] NtCreateUserProcess(ProcessHandle=0x9e210 [0x15c], ThreadHandle=0x9e248 [0x158], ProcessDesiredAccess=MAXIMUM_ALLOWED, ThreadDesiredAccess=MAXIMUM_ALLOWED, ProcessObjectAttributes=null, ThreadObjectAttributes=null, ProcessFlags=0x204, ThreadFlags=1, ProcessParameters=0x7391c0 ["D:\lab0001\child.exe"], CreateInfo=0x9e3a0, AttributeList=0x9eba0) => 0
[1768] NtQueryInformationProcess(ProcessHandle=0x15c, ProcessInformationClass=0x1a [ProcessWow64Information], ProcessInformation=0x9e110, Length=8, ReturnLength=null) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls", OpenOptions=0) => 0xc0000034 [2 '   .']
[1768] NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0xa, TokenHandle=0x9e440 [0x168]) => 0
[1768] NtQueryInformationToken(TokenHandle=0x168, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec40, Length=0x90, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=0x3, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option", OpenOptions=0) => 0xc0000034 [2 '   .']
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x16c], DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x16c, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtQueryValueKey(KeyHandle=0x16c, ValueName="TransparentEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x61da60, Length=0x50, ResultLength=0x61d98c) => 0xc0000034 [2 '   .']
[1768] NtQueryValueKey(KeyHandle=0x16c, ValueName="AuthenticodeEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x61da60, Length=0x50, ResultLength=0x61d98c [0x10]) => 0
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers", OpenOptions=0) => 0xc0000034 [2 '   .']
[1768] NtTraceControl(CtrlCode=0x8000000f, InputBuffer=0x61da98, InputBufferLength=0xa0, OutputBuffer=0x61da98, OutputBufferLength=0xa0, ReturnLength=0x61da8c [0xa0]) => 0
[1768] NtQueryInformationProcess(ProcessHandle=0x15c, ProcessInformationClass=0x3c [ProcessCommandLineInformation], ProcessInformation=0x9e8c0, Length=0x408, ReturnLength=0x61d9e4 [0x24]) => 0
[1768] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0x9eca0, Length=0x24, ReturnLength=0x9e400 [0x24]) => 0
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x54, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0x9eca0, Length=0x24, ReturnLength=0x9e400 [0x24]) => 0
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x170], DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x170, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0

[1768] NtQueryValueKey(KeyHandle=0x170, ValueName="Cache",
KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x8d62a8,
Length=0x208, ResultLength=0x61d9b8 [0x92]) => 0
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x168], DesiredAccess=0x8,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-
1001\Software\Microsoft\Windows NT\CurrentVersion", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x168, KeySetInformationClass=5
[KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtQueryObject(ObjectHandle=0x168, ObjectInformationClass=1
[ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x168, KeyInformationClass=7 [KeyHandleTagsInformation],
KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x174], DesiredAccess=0x101,
ObjectAttributes=0x168:"AppCompatFlags\Layers", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x174, KeySetInformationClass=5
[KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtQueryValueKey(KeyHandle=0x174, ValueName="D:\lab0001\child.exe",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x738930,
Length=0x10, ResultLength=0x61d998) => 0xc0000034 [2 ' .']
[1768] NtApphelpCacheControl(ServiceClass=0xb, ServiceData="") => 0
[1768] NtQueryInformationProcess(ProcessHandle=0x15c, ProcessInformationClass=0
[ProcessBasicInformation], ProcessInformation=0x9e320, Length=0x40, ReturnLength=null) => 0
[1768] NtQueryInformationProcess(ProcessHandle=0x15c, ProcessInformationClass=0x1a
[ProcessWow64Information], ProcessInformation=0x9e2e0, Length=8, ReturnLength=null) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x174], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\MACHINE\Software\WOW6432Node\Microsoft\Windows\CurrentV
ersion\SideBySide", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x174, KeySetInformationClass=5
[KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtQueryValueKey(KeyHandle=0x174, ValueName="PreferExternalManifest",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x61daa8,
Length=0x14, ResultLength=0x61da80) => 0xc0000034 [2 ' .']
[1768] NtQueryVolumeInformationFile(FileHandle=0x160, IoStatusBlock=0x9e418 [0/8],
FsInformation=0x61dab8, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
[1768] NtQueryLicenseValue(Name="WindowsExcludedProcs", Type=0x61d9b8, Buffer=null,
Length=0, ReturnedLength=0x61d9bc) => 0xc0000034 [2 ' .']
[1768] NtQueryLicenseValue(Name="WindowsExcludedProcs", Type=0x61d9b8, Buffer=null,
Length=0x76fdc63e, ReturnedLength=0x61d9bc) => 0xc000000d [87 ' .']
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Number-Allowed", Type=0x61d9b8,
Buffer=null, Length=0, ReturnedLength=0x61d9bc) => 0xc0000023 [122 ' ,
, .']
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Number-Allowed", Type=0x61d9b8 [4],
Buffer=0x8cf8e8, Length=4, ReturnedLength=0x61d9bc [4]) => 0
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Language-Allowed", Type=0x61d9b8,
Buffer=null, Length=0, ReturnedLength=0x61d9bc) => 0xc0000023 [122 ' ,
, .']
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Language-Allowed", Type=0x61d9b8 [1],
Buffer=0x8c1270, Length=0xc, ReturnedLength=0x61d9bc [0xc]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x174], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CustomLocale"
, OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x174, KeySetInformationClass=5
[KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0

[1768] NtQueryValueKey(KeyHandle=0x174, ValueName="EMPTY",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x61d780,
Length=0x78, ResultLength=0x61d774) => 0xc0000034 [2 ' .']
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Language-Disallowed", Type=0x61d9b8,
Buffer=null, Length=0, ReturnedLength=0x61d9bc) => 0xc0000023 [122 ' ,
, .']
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Language-Disallowed", Type=0x61d9b8 [1],
Buffer=0x8c1270, Length=0xc, ReturnedLength=0x61d9bc [0xc]) => 0
[1768] NtQueryValueKey(KeyHandle=0x174, ValueName="EMPTY",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x61d780,
Length=0x78, ResultLength=0x61d774) => 0xc0000034 [2 ' .']
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Language-SKU", Type=0x61d9b8,
Buffer=null, Length=0, ReturnedLength=0x61d9bc) => 0xc0000023 [122 ' ,
, .']
[1768] NtQueryLicenseValue(Name="Kernel-MUI-Language-SKU", Type=0x61d9b8 [1],
Buffer=0x8d2688, Length=0x302, ReturnedLength=0x61d9bc [0x302]) => 0
[1768] NtIsUILanguageComitted() => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x178], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\NLS\Language",
OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x178, KeySetInformationClass=5
[KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtQueryValueKey(KeyHandle=0x178, ValueName="InstallLanguageFallback",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8d27e8,
Length=0x164, ResultLength=0x61d944 [0x18]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x178], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\MUI\UILanguages",
OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x178, KeySetInformationClass=5
[KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtEnumerateKey(KeyHandle=0x178, Index=0, KeyInformationClass=0
[KeyBasicInformation], KeyInformation=0x61d780, Length=0x200, ResultLength=0x61d744
[0x1a]) => 0
[1768] NtQueryObject(ObjectHandle=0x178, ObjectInformationClass=1
[ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x178, KeyInformationClass=7 [KeyHandleTagsInformation],
KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=KEY_READ,
ObjectAttributes=0x178:"en-US", OpenOptions=0) => 0
[1768] NtQueryValueKey(KeyHandle=0x17c, ValueName="Type", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x8c1300, Length=0x10,
ResultLength=0x61d704 [0x10]) => 0
[1768] NtQueryValueKey(KeyHandle=0x17c, ValueName="AlternateCodePage",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8c1378,
Length=0xc, ResultLength=0x61d684) => 0xc0000034 [2 ' .']
[1768] NtEnumerateKey(KeyHandle=0x178, Index=1, KeyInformationClass=0
[KeyBasicInformation], KeyInformation=0x61d780, Length=0x200, ResultLength=0x61d744
[0x1a]) => 0
[1768] NtQueryObject(ObjectHandle=0x178, ObjectInformationClass=1
[ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x178, KeyInformationClass=7 [KeyHandleTagsInformation],
KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=KEY_READ,
ObjectAttributes=0x178:"ru-RU", OpenOptions=0) => 0

[1768] NtQueryValueKey(KeyHandle=0x17c, ValueName="Type", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8c1300, Length=0x10, ResultLength=0x61d704 [0x10]) => 0
[1768] NtQueryValueKey(KeyHandle=0x17c, ValueName="DefaultFallback", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8c98f0, Length=0xb6, ResultLength=0x61d204 [0x18]) => 0
[1768] NtQueryValueKey(KeyHandle=0x17c, ValueName="en-US", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x61d3e0, Length=0x200, ResultLength=0x61d26c [0x24]) => 0
[1768] NtEnumerateValueKey(KeyHandle=0x17c, Index=0, KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x61d3e0, Length=0x200, ResultLength=0x61d234 [0x44]) => 0
[1768] NtEnumerateValueKey(KeyHandle=0x17c, Index=1, KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x61d3e0, Length=0x200, ResultLength=0x61d234 [0x24]) => 0
[1768] NtEnumerateValueKey(KeyHandle=0x17c, Index=2, KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x61d3e0, Length=0x200, ResultLength=0x61d234 [0x24]) => 0
[1768] NtEnumerateValueKey(KeyHandle=0x17c, Index=3, KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x61d3e0, Length=0x200, ResultLength=0x61d234 [0x24]) => 0
[1768] NtEnumerateValueKey(KeyHandle=0x17c, Index=4, KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x61d3e0, Length=0x200, ResultLength=0x61d234) => 0x8000001a [259 ' .']
[1768] NtQueryValueKey(KeyHandle=0x17c, ValueName="AlternateCodePage", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8c1270, Length=0xc, ResultLength=0x61d684) => 0xc0000034 [2 ' .']
[1768] NtEnumerateKey(KeyHandle=0x178, Index=2, KeyInformationClass=0 [KeyBasicInformation], KeyInformation=0x61d780, Length=0x200, ResultLength=0x61d744) => 0x8000001a [259 ' .']
[1768] NtIsUILanguageComitted() => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\MUI\UILanguages\PendingDelete", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Policies\Microsoft\MUI\Settings", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x178], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001", OpenOptions=0) => 0
[1768] NtQueryObject(ObjectHandle=0x178, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x178, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x178, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes=0x178:"Control Panel\Desktop\MuiCached\MachineLanguageConfiguration", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration", OpenOptions=0) => 0xc0000034 [2 ' .']

[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Policies\Microsoft\MUI\Settings", OpenOptions=0) => 0xc0000034 [2 '.']
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001", OpenOptions=0) => 0
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Software\Policies\Microsoft\Control Panel\Desktop", OpenOptions=0) => 0xc0000034 [2 '.']
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Control Panel\Desktop\LanguageConfiguration", OpenOptions=0) => 0xc0000034 [2 '.']
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Policies\Microsoft\MUI\Settings", OpenOptions=0) => 0xc0000034 [2 '.']
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001", OpenOptions=0) => 0
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Software\Policies\Microsoft\Control Panel\Desktop", OpenOptions=0) => 0xc0000034 [2 '.']
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x178], DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Control Panel\Desktop", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x178, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0

[1768] NtQueryValueKey(KeyHandle=0x178, ValueName="PreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8c1378, Length=0xc, ResultLength=0x61d904) => 0xc0000034 [2 ' .']
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Policies\Microsoft\MUI\Settings", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001", OpenOptions=0) => 0
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x178], DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Control Panel\Desktop\MuiCached", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x178, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtQueryValueKey(KeyHandle=0x178, ValueName="MachinePreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8c1270, Length=0xc, ResultLength=0x61d904) => 0x80000005 [234 ' .']
[1768] NtQueryValueKey(KeyHandle=0x178, ValueName="MachinePreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8d1e48, Length=0x18, ResultLength=0x61d904 [0x18]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Policies\Microsoft\MUI\Settings", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001", OpenOptions=0) => 0
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Software\Policies\Microsoft\Control Panel\Desktop", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x178], DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Control Panel\Desktop", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x178, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0

[1768] NtQueryValueKey(KeyHandle=0x178, ValueName="PreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x8c1270, Length=0xc, ResultLength=0x61d92c) => 0xc0000034 [2 ' .']
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Policies\Microsoft\MUI\Settings", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001", OpenOptions=0) => 0
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Software\Policies\Microsoft\Control Panel\Desktop", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtQueryObject(ObjectHandle=0x17c, ObjectInformationClass=1 [ObjectNameInformation], ObjectInformation=0x9e140, Length=0x210, ReturnLength=null) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=7 [KeyHandleTagsInformation], KeyInformation=0x9e348, Length=4, ResultLength=0x9e358 [4]) => 0
[1768] NtQueryKey(KeyHandle=0x17c, KeyInformationClass=3 [KeyNameInformation], KeyInformation=0x7391e0, Length=0x818, ResultLength=0x9e2d8 [0x7e]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378, DesiredAccess=KEY_READ, ObjectAttributes=0x17c:"Control Panel\Desktop\LanguageConfiguration", OpenOptions=0) => 0xc0000034 [2 ' .']
[1768] NtAlpcSendWaitReceivePort(PortHandle=0xb4, SendFlags=0x00020000, SendMessage=0x9dd80 [2 [LPC_REPLY] (560b)], InMessageBuffer=null, ReceiveBuffer=0x9dd80, ReceiveBufferSize=0x9dd30 [0x258], OutMessageBuffer=null, Timeout=null) => 0
[1768] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0x9eca0, Length=0x24, ReturnLength=0x9e400 [0x24]) => 0
[1768] NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x9ec70, Length=0x58, ReturnLength=0x9e400 [0x2c]) => 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x17c], DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x17c, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[1768] NtQueryValueKey(KeyHandle=0x17c, ValueName="Cache", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x8d4790, Length=0x208, ResultLength=0x61da18 [0x92]) => 0
[1768] NtApphelpCacheControl(ServiceClass=0, ServiceData="") => 0
[1768] NtQueryLicenseValue(Name="Kernel-OneCore-DeviceFamilyID", Type=0x61d8e8 [4], Buffer=0x61d8d8, Length=4, ReturnedLength=0x61d8ec [4]) => 0
[1768] NtAllocateVirtualMemory(ProcessHandle=0x15c, lpAddress=0x61dfd0 [0x000b0000], ZeroBits=0, pSize=0x61de68 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
[1768] NtWriteVirtualMemory(ProcessHandle=0x15c, BaseAddress=0xb0000, Buffer=0x8d46d8, BufferLength=0x11c0, ReturnedLength=null) => 0
[1768] NtWriteVirtualMemory(ProcessHandle=0x15c, BaseAddress=0x3a22d8, Buffer=0x61dfd0, BufferLength=8, ReturnedLength=null) => 0

[1768] NtWriteVirtualMemory(ProcessHandle=0x15c, BaseAddress=0x3a31e8, Buffer=0x61dee8, BufferLength=4, ReturnedLength=null) => 0
[1768] NtSetInformationProcess(ProcessHandle=0x15c, ProcessInformationClass=0x30 [ProcessTokenVirtualizationEnabled], ProcessInformation=0x61dc10, Length=4) => 0
[1768] NtCreateFile(FileHandle=0x9e3d8 [0x17c], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0xa8:"outputik.txt", IoStatusBlock=0x9e3f0 [0/3], AllocationSize=null, FileAttributes=0x80, ShareAccess=0, CreateDisposition=5, CreateOptions=0x60, EaBuffer=null, EaLength=0) => 0
[1768] Created thread: 27376 at 0000000076EF5200
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0xfbfd24, Length=0x2cc, ReturnLength=null) => 0
[1768] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0xfbfd24, Length=0x2cc) => 0
[1768] NtTestAlert() => 0
[1768] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=3 [ThreadBasePriority], ThreadInformation=0xfbfed4, Length=4) => 0
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0x82e250, Length=0x2cc, ReturnLength=null) => 0
[1768] Exception: 40010005 at 0000000076EF536C (first chance)
[1768] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x22 [ProcessExecuteFlags], ProcessInformation=0xfbf998, Length=4, ReturnLength=null) => 0
[1768] NtDuplicateObject(SourceProcess=-1, SourceHandle=0x15c, TargetProcess=-1, TargetHandle=0x82e810 [0x180], DesiredAccess=0x1000, InheritMode=false, Options=0) => 0
[1768] NtQueryInformationProcess(ProcessHandle=0x180, ProcessInformationClass=0 [ProcessBasicInformation], ProcessInformation=0x82e6b8, Length=0x30, ReturnLength=null) => 0
[1768] NtQueryInformationProcess(ProcessHandle=0x180, ProcessInformationClass=0x1a [ProcessWow64Information], ProcessInformation=0x82e6b0, Length=8, ReturnLength=null) => 0
[1768] NtQueryInformationProcess(ProcessHandle=0x180, ProcessInformationClass=0x2b [ProcessImageFileNameWin32], ProcessInformation=0x82ee80, Length=0x218, ReturnLength=null) => 0xc0000001 [31 '   .']
[1768] NtFlushBuffersFile(FileHandle=0x17c, IoStatusBlock=0x9e420 [0/0]) => 0
[1768] NtFlushBuffersFile(FileHandle=0x17c, IoStatusBlock=0x82e7f0 [0/0]) => 0
[1768] NtFlushBuffersFile(FileHandle=0x17c, IoStatusBlock=0x9e420 [0/0]) => 0
[1768] Exception raised by attempted close of an invalid handle
[1768] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x22 [ProcessExecuteFlags], ProcessInformation=0x61e8b0, Length=4, ReturnLength=null) => 0
[1768] NtFlushBuffersFile(FileHandle=0x124, IoStatusBlock=0x82e7f0 [0/0]) => 0
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xfbfe1c, Length=4, ReturnLength=null) => 0
[1768] Thread 27376 exit code: 0
[1768] NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=7 [ProcessDebugPort], ProcessInformation=0x9ecc0, Length=8, ReturnLength=0x9e400 [8]) => 0
[1768] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0x61e98c, Length=0x2cc) => 0
[1768] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0x9de80, Length=0x2cc, ReturnLength=null) => 0
[1768] Ignoring unhandled exception from close of an invalid handle
[1768] Thread 20748 exit code: 0
[1768] Thread 20136 exit code: 0
[1768] NtOpenKeyEx(KeyHandle=0x9e378 [0x104], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize", OpenOptions=0) => 0
[1768] NtSetInformationKey(KeyHandle=0x104, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0

[1768] NtQueryValueKey(KeyHandle=0x104, ValueName="DisableMetaFiles", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x738930, Length=0x14, ResultLength=0x61f54c) => 0xc0000034 [2 ' .']
[1768] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0xa [ThreadZeroTlsCell], ThreadInformation=0x61f538, Length=4) => 0
[1768] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0xa [ThreadZeroTlsCell], ThreadInformation=0x61fcb8, Length=4) => 0
[1768] NtQueryWnfStateData(StateName=0x61fbb4 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x61eb90 [0x8c74], Buffer=0x61eb98, BufferSize=0x61eb94 [0x948]) => 0
[1768] Process 1768 exit code: 0

child_log.txt

[24828] Process 24828 starting at 0000000000000000 with command line: "child.exe" D:\lab0001\child.exe
[24828] Loaded DLL at 00007FF801910000 C:\WINDOWS\SYSTEM32\ntdll.dll
[24828] Loaded DLL at 0000000076F90000 C:\WINDOWS\SYSTEM32\ntdll.dll
[24828] Created thread: 24872 at 0000000076FCEF40
[24828] Created thread: 24880 at 0000000076FCEF40
[24828] Created thread: 25096 at 0000000076FCEF40
[24828] Loaded DLL at 00007FF800520000 C:\WINDOWS\System32\wow64.dll
[24828] Loaded DLL at 00007FF800600000 C:\WINDOWS\System32\wow64base.dll
[24828] Loaded DLL at 00007FF801840000 C:\WINDOWS\System32\wow64win.dll
[24828] Loaded DLL at 00007FF800950000 C:\WINDOWS\System32\wow64con.dll
[24828] Loaded DLL at 0000000076F80000 C:\WINDOWS\System32\wow64cpu.dll
[24828] Loaded DLL at 00000000761A0000 C:\WINDOWS\System32\KERNEL32.DLL
[24828] Loaded DLL at 0000000076CF0000 C:\WINDOWS\System32\KERNELBASE.dll
[24828] Loaded DLL at 0000000076320000 C:\WINDOWS\System32\msvcrt.dll
[24828] Loaded DLL at 0000000076750000 C:\WINDOWS\System32\USER32.dll
[24828] Loaded DLL at 0000000076C90000 C:\WINDOWS\System32\win32u.dll
[24828] Loaded DLL at 00000000752F0000 C:\WINDOWS\System32\GDI32.dll
[24828] Loaded DLL at 0000000075200000 C:\WINDOWS\System32\gdi32full.dll
[24828] Loaded DLL at 0000000076590000 C:\WINDOWS\System32\msvcp_win.dll
[24828] Loaded DLL at 0000000076B70000 C:\WINDOWS\System32\ucrtbase.dll
[24828] Loaded DLL at 0000000076CC0000 C:\WINDOWS\System32\IMM32.DLL
[24828] Created thread: 12476 at 00007FF8019E71E0
[24828] NtTestAlert() => 0
[24828] Initial breakpoint
[24828] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xf7fc58, Length=4, ReturnLength=null) => 0
[24828] Thread 12476 exit code: 0
[24828] Created thread: 20512 at 0000000076EF5200
[24828] NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0x295fd24, Length=0x2cc, ReturnLength=null) => 0
[24828] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0x1d [ThreadWow64Context], ThreadInformation=0x295fd24, Length=0x2cc) => 0
[24828] NtTestAlert() => 0
[24828] Thread 25096 exit code: 0
[24828] Thread 24872 exit code: 0
[24828] Thread 20512 exit code: 0
[24828] Thread 24880 exit code: 0
[24828] NtOpenKeyEx(KeyHandle=0x9e378 [0x11c], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\WOW6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize", OpenOptions=0) => 0

[24828] NtSetInformationKey(KeyHandle=0x11c, KeySetInformationClass=5 [KeySetHandleTagsInformation], KeyInformation=0x9e370, Length=4) => 0
[24828] NtQueryValueKey(KeyHandle=0x11c, ValueName="DisableMetaFiles", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x197960, Length=0x14, ResultLength=0x61f54c) => 0xc0000034 [2 ' .']
[24828] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0xa [ThreadZeroTlsCell], ThreadInformation=0x61f538, Length=4) => 0
[24828] NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0xa [ThreadZeroTlsCell], ThreadInformation=0x61fcb8, Length=4) => 0
[24828] NtQueryWnfStateData(StateName=0x61fbb4 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x61eb90 [0x8c74], Buffer=0x61eb98, BufferSize=0x61eb94 [0x948]) => 0
[24828] Process 24828 exit code: 0

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.