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-214Б-23

Студент: Кондратенко А.С.

Преподаватель: Бахарев В.Д. (ФИИТ)

Оценка: _____

Дата: 20.11.24

Москва, 2024

Постановка задачи

Вариант 8.

В файле записаны команды вида: «число число число». Дочерний процесс производит деление первого числа команда, на последующие числа в команде, а результат выводит в стандартный поток вывода. Если происходит деление на 0, то тогда дочерний и родительский процесс завершают свою работу. Проверка деления на 0 должна осуществляться на стороне дочернего процесса. Числа имеют тип int. Количество чисел может быть произвольным.

Общий метод и алгоритм решения

Использованные системные вызовы:

- CreateNamedPipe – создает канал
- ConnectNamedPipe – позволяет работать с созданным ранее каналом
- ReadFile – читает данные из канала
- WriteFile – записывает данные в канал
- CloseHandle – закрывает дескриптор канала
- GetStdHandle – возвращает дескриптор по DWORD

Я реализовал собственные аналоги printf и fprintf(my_printf и file_printf соответственно). В них обрабатывается форматная строка, в результирующую строку подставляются переданные аргументы, и затем она выводится либо в консоль (с помощью WriteConsoleA) либо в файл (с помощью WriteFile). Также я создал функцию для перевода строки в LPWSTR.

В parent.cpp открывается файл, переданный в аргументах командной строки, в строку buffer записываются данные оттуда. Затем полученные данные отправляются в child.cpp, где они с помощью strtok разделяются по строкам. Далее строки разделяются по пробелам на числа, производится деление чисел, и результат передается в родительский процесс, откуда выводится в стандартный поток вывода.

Код программы

my_stdio.h

```
#include <windows.h>

#include <stdarg.h>

#include <string.h>



LPWSTR ConvertToWideString(const char* str);



void my_printf(const char* format, ...);



int file_printf(HANDLE fileHandle, const char* format, ...);
```

my_stdio.cpp

```
#pragma once
#define INITIAL_BUFFER_SIZE 128

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

LPWSTR ConvertToWideString(const char* str) {
    if (str == nullptr) return nullptr;
    int size_needed = MultiByteToWideChar(CP_UTF8, 0, str, -1, NULL, 0);
    LPWSTR wideString = new wchar_t[size_needed];
    MultiByteToWideChar(CP_UTF8, 0, str, -1, wideString, size_needed);
    return wideString;
}
void my_printf(const char* format, ...) {
    va_list args;
    va_start(args, format);

    char buffer[1024];
    char* buf_ptr = buffer;
    const char* fmt_ptr = format;
    int buffer_size = sizeof(buffer);

    while (*fmt_ptr) {
        if (*fmt_ptr == '%') {
            fmt_ptr++;
            switch (*fmt_ptr) {
            case 'd': {
                int value = va_arg(args, int);
```

```
    char num_buffer[20];
    char* num_ptr = num_buffer;
    if (value < 0) {
        *buf_ptr++ = '-';
        value = -value;
    }
    do {
        *num_ptr++ = (char)((value % 10) + '0');
        value /= 10;
    } while (value > 0);
    while (num_ptr > num_buffer) {
        *buf_ptr++ = *--num_ptr;
    }
    break;
}
case 's': {
    char* str = va_arg(args, char*);
    while (*str) {
        *buf_ptr++ = *str++;
    }
    break;
}
case 'c': {
    char ch = (char)va_arg(args, int);
    *buf_ptr++ = ch;
    break;
}
case '%': {
    *buf_ptr++ = '%';
    break;
```

```
            }
            default:
                *buf_ptr++ = *fmt_ptr;
                break;
            }
        }
        else {
            *buf_ptr++ = *fmt_ptr;
        }
        fmt_ptr++;
    }
    *buf_ptr = '\0';

    va_end(args);

    HANDLE hConsole = GetStdHandle(STD_OUTPUT_HANDLE);
    DWORD bytesWritten;
    WriteConsoleA(hConsole, buffer, (DWORD)(buf_ptr - buffer), &bytesWritten, NULL);
}


int file_printf(HANDLE fileHandle, const char* format, ...) {
    va_list args;
    va_start(args, format);

    char buffer[1024];
    char* buf_ptr = buffer;
    const char* fmt_ptr = format;
    int buffer_size = sizeof(buffer);
```

```
while (*fmt_ptr) {
    if (*fmt_ptr == '%') {
        fmt_ptr++;
        switch (*fmt_ptr) {
        case 'd': {
            int value = va_arg(args, int);
            char num_buffer[20];
            char* num_ptr = num_buffer;
            if (value < 0) {
                *buf_ptr++ = '-';
                value = -value;
            }
            do {
                *num_ptr++ = (char)((value % 10) + '0');
                value /= 10;
            } while (value > 0);
            while (num_ptr > num_buffer) {
                *buf_ptr++ = *--num_ptr;
            }
            break;
        }
        case 's': {
            const char* str = va_arg(args, const char*);
            while (*str) {
                *buf_ptr++ = *str++;
            }
            break;
        }
        case 'c': {
            char ch = (char)va_arg(args, int);
```

```
                *buf_ptr++ = ch;
                break;
            }
            case '%': {
                *buf_ptr++ = '%';
                break;
            }
            default:
                *buf_ptr++ = *fmt_ptr;
                break;
            }
        }
        else {
            *buf_ptr++ = *fmt_ptr;
        }
        fmt_ptr++;
    }
    *buf_ptr = '\0';
    DWORD bytesWritten;
    WriteFile(fileHandle, buffer, (DWORD)(buf_ptr - buffer), &bytesWritten, NULL);

    va_end(args);
    //CloseHandle(fileHandle);
    return 0;
}
```

parent.cpp

```
#define _CRT_SECURE_NO_WARNINGS
#include <windows.h>
#include <string.h>
#include "my_stdio.h"
```

```
//#include <stdio.h>
#define BUFFER_SIZE 1024

enum ret_type_t {
    SUCCESS,    //Successful end
    ERROR_ARGS_COUNT,    //Wrong args number
    ERROR_CREATE_PIPE,  //Failed to create a new pipeline
    ERROR_CREATE_CHILD_PROCESS, //Failed to create a child process
    ERROR_READ, //Failed to read from pipe
    ERROR_DEV_ZERO, //Devision by zero detected
    ERROR_FULL, //Overflow
    ERROR_OPEN_FILE,    //Error with file opening
    ERROR_CLOSE_FILE,   //Error with closing file
    ERROR_FILE_WRITE,   //Error with file writing
    ERROR_HANDLER_INHERITED, //Error handler reading
    ERROR_PIPE_WRITE,   //Failed to write smth in the pipe
    ERROR_HEAP,         //Failed to malloc
};

int main(int argc, char* argv[]) {

    //my_printf("1\n");

    if (argc != 2) {
        my_printf("Incorrect num args");
        return ERROR_ARGS_COUNT;
    }

    HANDLE hPipe1, hPipe2;
    char pipeName1[] = "\\\\.\\pipe\\Pipe1";
```

```
    char pipeName2[] = "\\\\.\\pipe\\Pipe2";

    char fileName[BUFFER_SIZE];

    char buffer[BUFFER_SIZE];

    DWORD bytesRead, bytesWritten;


    hPipe1 = CreateNamedPipe(ConvertToWideString(pipeName1), PIPE_ACCESS_OUTBOUND,
PIPE_TYPE_BYTE | PIPE_WAIT, 1, 0, 0, 0, NULL);

    if (hPipe1 == INVALID_HANDLE_VALUE) {

        my_printf("Failed to create named pipe");

        return ERROR_CREATE_PIPE;

    }


    hPipe2 = CreateNamedPipe(ConvertToWideString(pipeName2), PIPE_ACCESS_INBOUND,
PIPE_TYPE_BYTE | PIPE_WAIT, 1, 0, 0, 0, NULL);

    if (hPipe2 == INVALID_HANDLE_VALUE) {

        CloseHandle(hPipe1);

        my_printf("Failed to create named pipe");

        return ERROR_CREATE_PIPE;

    }


    //my_printf("2\n");


    HANDLE hFile = CreateFile(ConvertToWideString(argv[1]), GENERIC_READ, 0, NULL,
OPEN_EXISTING, 0, NULL);

    ReadFile(hFile, buffer, BUFFER_SIZE, &bytesRead, NULL);

    buffer[bytesRead] = '\0';

    //my_printf("bytes read %d\n", bytesRead);

    //my_printf("%s", buffer);


    STARTUPINFO si;

    PROCESS_INFORMATION pi;
```

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

    char cmdLine[] = "child.exe";

    if (!CreateProcess(NULL, ConvertToWideString(cmdLine), NULL, NULL, FALSE, 0, NULL,
NULL, &si, &pi)) {
        CloseHandle(hPipe1);
        CloseHandle(hPipe2);
        my_printf("Failed to create process");
        return ERROR_CREATE_CHILD_PROCESS;
    }

    ConnectNamedPipe(hPipe1, NULL);

    ConnectNamedPipe(hPipe2, NULL);
    WriteFile(hPipe1, buffer, bytesRead + 1, &bytesWritten, NULL);
    char response[BUFFER_SIZE] = { '\0' };
    ReadFile(hPipe2, response, BUFFER_SIZE, &bytesRead, NULL);
    if (!strcmp(response, "DIVIDE_BY_ZERO")) {
        my_printf("Zero division error");
        return ERROR_DEV_ZERO;
    }

    CloseHandle(hPipe1);
    CloseHandle(hPipe2);
    CloseHandle(pi.hProcess);
    CloseHandle(pi.hThread);
```

```
    return SUCCESS;
}
```

child.cpp

```
#pragma once
#define _CRT_SECURE_NO_WARNINGS
#include <windows.h>
#include <string.h>
//#include <stdio.h>
#include "my_stdio.h"

#define BUFFER_SIZE 1024

enum ret_type_t {
    SUCCESS,    //Successful end
    ERROR_ARGS_COUNT,    //Wrong args number
    ERROR_CREATE_PIPE,  //Failed to create a new pipeline
    ERROR_CREATE_CHILD_PROCESS, //Failed to create a child process
    ERROR_READ, //Failed to read from pipe
    ERROR_DEV_ZERO, //Devision by zero detected
    ERROR_FULL, //Overflow
    ERROR_OPEN_FILE,    //Error with file opening
    ERROR_CLOSE_FILE,   //Error with closing file
    ERROR_FILE_WRITE,   //Error with file writing
    ERROR_HANDLER_INHERITED, //Error handler reading
    ERROR_PIPE_WRITE,   //Failed to write smth in the pipe
    ERROR_HEAP,         //Failed to malloc
};

int main() {
    HANDLE hPipe1, hPipe2;
```

```
    char pipeName1[] = "\\\\.\\pipe\\Pipe1";
    char pipeName2[] = "\\\\.\\pipe\\Pipe2";
    char buffer[BUFFER_SIZE];
    DWORD bytesRead, bytesWritten;


    //my_printf("11\n");
    HANDLE hFile;


    hPipe1 = CreateFile(ConvertToWideString(pipeName1), GENERIC_READ, 0, NULL,
OPEN_EXISTING, 0, NULL);
    if (hPipe1 == INVALID_HANDLE_VALUE) {
        my_printf("Failed to create named pipe");
        return ERROR_CREATE_PIPE;
    }
    //my_printf("22\n");
    hPipe2 = CreateFile(ConvertToWideString(pipeName2), GENERIC_WRITE, 0, NULL,
OPEN_EXISTING, 0, NULL);
    if (hPipe2 == INVALID_HANDLE_VALUE) {
        CloseHandle(hPipe1);
        my_printf("Failed to create named pipe");
        return ERROR_CREATE_PIPE;
    }
    //my_printf("33\n");
    ReadFile(hPipe1, buffer, BUFFER_SIZE, &bytesRead, NULL);
    //my_printf("44\n");
    //my_printf("%s\n\n", buffer);
    int count = 0;
    char* token = strtok(buffer, "\n");
    //my_printf("start token: %s\n", token);
    while (token) {
        int i = 0, a, b, is_first = 1;
```

```
        char num[BUFFER_SIZE];
        char* ptc = token;
        while (1) {
            if (*ptc == ' ' || !(*ptc)) {
                if (is_first) {
                    num[i] = '\0';
                    a = atoi(num);
                    is_first = 0;
                }
                else {
                    num[i] = '\0';
                    b = atoi(num);
                    if (!b) {
                        WriteFile(hPipe2, "DIVIDE_BY_ZERO", strlen("DIVIDE_BY_ZERO"),
&bytesWritten, NULL);
                        return ERROR_DEV_ZERO;
                    }
                    my_printf("%d ", a / b);
                }
                i = 0;
                if (!(*ptc))
                    break;
            }
            else {
                num[i] = *ptc;
                i++;
            }
            ptc++;
        }
        my_printf("\n");
```

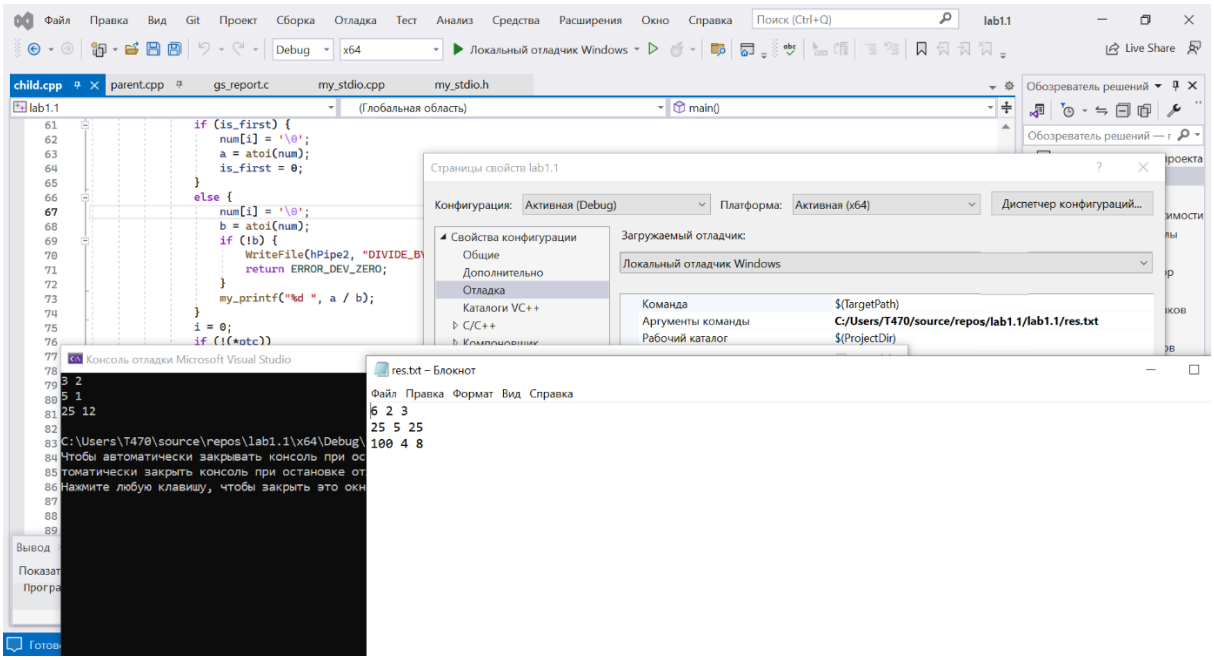
```
        token = strtok(NULL, "\n");
        //my_printf("token: %s\n", token);
    }

    CloseHandle(hPipe1);
    CloseHandle(hPipe2);

    return SUCCESS;
}
```

Протокол работы программы

Тестирование:



NtTrace:

C:\Users\T470\source\repos\lab1.1\lab1.1>NtTrace parent.exe

Process 7496 starting at 00007FF642E112E9 with command line: "parent.exe"

C:\Users\T470\source\repos\lab1.1\lab1.1\parent.exe

Loaded DLL at 00007FFA755F0000 C:\Windows\SYSTEM32\ntdll.dll

NtQueryPerformanceCounter(Counter=0xdfbd3f450 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3f498 [0x00007ffa75774000], Size=0xdfbd3f490 [0x1000], NewProtect=4, OldProtect=0xdfbd3f4d0 [8]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3f498 [0x00007ffa75774000], Size=0xdfbd3f490 [0x1000], NewProtect=8, OldProtect=0xdfbd3f4d0 [4]) => 0

NtCreateEvent(EventHandle=0x7ffa7575c478 [8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xdfbd3f400, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xdfbd3f128, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation], SystemInformation=0xdfbd3f000, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffa755f0000, MemoryInformationClass=6 [MemoryImageInformation], MemoryInformation=0xdfbd3ef10, Length=0x18, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4 [MemoryWorkingSetExInformation], MemoryInformation=0xdfbd3efd0, Length=0x50, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3f020 [0x00007ffa75771000], Size=0xdfbd3f018 [0x4000], NewProtect=2, OldProtect=0xdfbd3f010 [4]) => 0

NtOpenKey(KeyHandle=0xdfbd3dc60 [0xc], DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xc, ValueName="RaiseExceptionOnPossibleDeadlock", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xdfbd3dc70, Length=0x50, ResultLength=0xdfbd3dc68) => 0xc0000034 [2 '≔x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xc) => 0

NtOpenKey(KeyHandle=0xdfbd3dbf8 [0xc], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options") => 0

NtOpenKey(KeyHandle=0xdfbd3dce0, DesiredAccess=0x9, ObjectAttributes=0xc:"parent.exe") => 0xc0000034 [2 '≔x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xdfbd3dc40, DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap") => 0xc0000034 [2 '≔x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0x7ffa7575d230, Length=4, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xdfbd3efb8, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xdfbd3e9f0, Length=0x330, ReturnLength=0xdfbd3e9a8) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xdfbd3e9f0, Length=0x330, ReturnLength=0xdfbd3e9a8) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtOpenKey(KeyHandle=0xdfbd3ef30 [0x10], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x10, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xdfbd3ef70, Length=0x18, ResultLength=0xdfbd3ef38) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtClose(Handle=0x10) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xdfbd3f010, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xdfbd3efb0, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation], SystemInformation=0xdfbd3efe0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffa7575dc38 [0x00007ff5c37d0000], ZeroBits=0x0000000dfbd3ef60, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0xdfbd3eec8, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffa7575dc30 [0x00007ff5c57d0000], ZeroBits=0x0000000dfbd3ef68, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null, DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffa7575dca0 [0x00007ff4c37b0000], ZeroBits=0x0000000dfbd3ef10, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0xdfbd3ee78, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xdfbd3ee50, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3ea10 [0x0000015fd3eb0000], ZeroBits=0, pSize=0xdfbd3ea18 [0x001d0000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3ea10 [0x0000015fd3eb0000], pSize=0xdfbd3ea08 [0x000d0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e9f8 [0x0000015fd3f80000], ZeroBits=0, pSize=0xdfbd3e9f0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5 [SystemHypervisorSharedPageInformation], SystemInformation=0xdfbd3f1b8, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap], SystemInformation=0xdfbd3ec20, Length=0x408, ReturnLength=0xdfbd3f040 [0x18]) => 0

NtCreateEvent(EventHandle=0xdfbd3ee58 [0x10], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x15fd3f80b20 [0x14], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xdfbd3ebb0 [1], Alignment=4, SystemInformation=0x15fd3f80ed0, Length=0x50, ReturnLength=0xdfbd3eba8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x15fd3f80c00 [0x18], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, NumberOfConcurrentThreads=5) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x15fd3f80bf8 [0x1c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null, CompletionPortHandle=0x18, WorkerProcessHandle=-1, StartRoutine=0x7ffa7563d110, StartParameter=0x15fd3f80bc0, MaxThreadCount=0x200, StackReserve=0x00100000, StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x15fd3f80c50 [0x20], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x7ffa00000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x15fd3f80c58 [0x24], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x24, IoCompletionHandle=0x18, TargetObjectHandle=0x20, KeyContext=0x15fd3f80c60, ApcContext=0x15fd3f80c30, IoStatus=0, IoStatusInformation=1, AlreadySignaled=0xdfbd3eb70 [0]) => 0

NtCreateTimer2(TimerHandle=0x15fd3f80cc8 [0x28], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x15f00000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x15fd3f80cd0 [0x2c], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x2c, IoCompletionHandle=0x18, TargetObjectHandle=0x28, KeyContext=0x15fd3f80cd8, ApcContext=0x15fd3f80c30, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0xdfbd3eb70 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0xdfbd3ec78, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=0xe [WorkerFactoryThreadSoftMaximum], Buffer=0xdfbd3ec78, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=3 [WorkerFactoryBindingCount], Buffer=0xdfbd3ed98, BufferLength=4) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x14, IoCompletionHandle=0x18, TargetObjectHandle=0x10, KeyContext=0x15fd3f80b38, ApcContext=0x15fd3f809b0, IoStatus=0x0000015f00000000, IoStatusInformation=0, AlreadySignaled=0xdfbd3ede0 [0xd3f80b00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0xdfbd3ee98, InputBufferLength=4, OutputBuffer=null, OutputBufferLength=0, ReturnLength=0xdfbd3ee50 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xdfbd3eef8, InputBufferLength=0xa0, OutputBuffer=0xdfbd3eef8, OutputBufferLength=0xa0, ReturnLength=0xdfbd3eef0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xdfbd3eef8, InputBufferLength=0xa0, OutputBuffer=0xdfbd3eef8, OutputBufferLength=0xa0, ReturnLength=0xdfbd3eef0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xdfbd3eef8, InputBufferLength=0xa0, OutputBuffer=0xdfbd3eef8, OutputBufferLength=0xa0, ReturnLength=0xdfbd3eef0 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e860 [0x0000015fd3f82000], ZeroBits=0, pSize=0xdfbd3e908 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3f040 [0x0000015fd3e40000], pSize=0xdfbd3f048 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3f020 [0x00007ffa75771000], Size=0xdfbd3f018 [0x4000], NewProtect=4, OldProtect=0xdfbd3f010 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ffa75771298 [0x3c], DesiredAccess=0x3, ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3f020 [0x00007ffa75771000], Size=0xdfbd3f018 [0x4000], NewProtect=2, OldProtect=0xdfbd3f010 [4]) => 0

NtOpenSymbolicLinkObject(LinkHandle=0xdfbd3f178 [0x40], DesiredAccess=0x1, ObjectAttributes=0x3c:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x40, LinkTarget="C:\Windows\System32", ReturnedLength=0xdfbd3f12c [0x28]) => 0

NtClose(Handle=0x40) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eff0 [0x00007ffa75771000], Size=0xdfbd3efe8 [0x4000], NewProtect=4, OldProtect=0xdfbd3efe0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3f020 [0x00007ffa75771000], Size=0xdfbd3f018 [0x4000], NewProtect=2, OldProtect=0xdfbd3f010 [4]) => 0

NtCreateEvent(EventHandle=0x7ffa7575c380 [0x40], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ffa7575c3b0 [0x44], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3ef70 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3ef80 [0x00007ffa75771000], Size=0xdfbd3ef78 [0x4000], NewProtect=4, OldProtect=0xdfbd3ef70 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3ef80 [0x00007ffa75771000], Size=0xdfbd3ef78 [0x4000], NewProtect=2, OldProtect=0xdfbd3ef70 [4]) => 0

NtOpenFile(FileHandle=0xdfbd3f028 [0x48], DesiredAccess=SYNCHRONIZE|0x20, ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\lab1.1\", IoStatusBlock=0xdfbd3ef98 [0/1], ShareAccess=3, OpenOptions=0x21) => 0

NtQueryVolumeInformationFile(FileHandle=0x48, IoStatusBlock=0xdfbd3ef98 [0/8], FsInformation=0xdfbd3ef80, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtSetEvent(EventHandle=0x40, PrevState=null) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0xdfbd3ece0, Length=4) => 0

NtOpenSection(SectionHandle=0xdfbd3ecb8 [0x4c], DesiredAccess=0xd, ObjectAttributes=0x3c:"KERNEL32.DLL") => 0

Loaded DLL at 00007FFA74A60000 C:\Windows\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x4c, ProcessHandle=-1, BaseAddress=0x15fd3f83260 [0x00007ffa74a60000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15fd3f831c0 [0x000c2000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3eb30 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb48 [0x00007ffa74b1f000], Size=0xdfbd3eb40 [0x1000], NewProtect=2, OldProtect=0xdfbd3ebb0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb40 [0x00007ffa75771000], Size=0xdfbd3eb38 [0x4000], NewProtect=4, OldProtect=0xdfbd3eb30 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb40 [0x00007ffa75771000], Size=0xdfbd3eb38 [0x4000], NewProtect=2, OldProtect=0xdfbd3eb30 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb90 [0x00007ffa74ae3000], Size=0xdfbd3eb98 [0x4000], NewProtect=4, OldProtect=0x15fd3f831a8 [2]) => 0

NtOpenSection(SectionHandle=0xdfbd3e628 [0x5c], DesiredAccess=0xd, ObjectAttributes=0x3c:"KERNELBASE.dll") => 0

Loaded DLL at 00007FFA72FE0000 C:\Windows\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x15fd3f83940 [0x00007ffa72fe0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15fd3f838a0 [0x002fe000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3e4a0 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e4b8 [0x00007ffa732b3000], Size=0xdfbd3e4b0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e520 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e4b0 [0x00007ffa75771000], Size=0xdfbd3e4a8 [0x4000], NewProtect=4, OldProtect=0xdfbd3e4a0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e4b0 [0x00007ffa75771000], Size=0xdfbd3e4a8 [0x4000], NewProtect=2, OldProtect=0xdfbd3e4a0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e500 [0x00007ffa731ca000], Size=0xdfbd3e508 [0x3000], NewProtect=4, OldProtect=0x15fd3f83888 [2]) => 0

NtClose(Handle=0x5c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3f83188 [0x00007ffa74ae3000], Size=0x15fd3f83190 [0x4000], NewProtect=2, OldProtect=0xdfbd3ea80 [4]) => 0

NtClose(Handle=0x4c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3f83868 [0x00007ffa731ca000], Size=0x15fd3f83870 [0x3000], NewProtect=2, OldProtect=0xdfbd3eb80 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0xdfbd3eae0, Length=0x28) => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3eba0, VmInformation=0xdfbd3ec78, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation], SystemInformation=0xdfbd3e800, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x7ffa7329ee60, Length=0x40, ReturnLength=null) => 0

NtOpenSection(SectionHandle=0xdfbd3e5c0 [0x60], DesiredAccess=0x4, ObjectAttributes="\Sessions\21\Windows\SharedSection") => 0

NtCreateSection(SectionHandle=0xdfbd3e5e0 [0x64], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null, SectionSize=0xdfbd3e5d0 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ffa7575cc48 [0x68], PortName="\Sessions\21\Windows\ApiPort", SecurityQos=0xdfbd3e700, ClientView=0xdfbd3e5f8, ServerView=0xdfbd3e628,

MaxMsgLength=0xdfbd3e5f0 [0x3b8], ConnectionInfo=0xdfbd3e670, ConnectionInfoLength=0xdfbd3e5c8 [0x30]) => 0

NtClose(Handle=0x64) => 0

NtMapViewOfSection(SectionHandle=0x60, ProcessHandle=-1, BaseAddress=0xdfbd3e5d8 [0x00007ff4c36b0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xdfbd3e5e8 [0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x60) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3e40000, MemoryInformationClass=0 [MemoryBasicInformation], MemoryInformation=0xdfbd3e2b0, Length=0x30, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3dfc0 [0x0000015fd3f84000], ZeroBits=0, pSize=0xdfbd3e068 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtInitializeNlsFiles(BaseAddress=0xdfbd3e7a0 [0x0000015fd3eb0000], DefaultLocaleId=0x7ffa732a08e0 [0x419], DefaultCasingTableSize=null) => 0

NtCreateFile(FileHandle=0xdfbd3e808 [0x64], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f, ObjectAttributes=4:"\Connect", IoStatusBlock=0xdfbd3e1c0 [0/0x18], AllocationSize=null, FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20, EaBuffer=0x15fd3f847c0, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x64, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xdfbd3e750 [0/0], IoControlCode=0x00500023, InputBuffer=null, InputBufferLength=0, OutputBuffer=0xdfbd3e770, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31 [ProcessOwnerInformation], ProcessInformation=0xdfbd3e778, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x64, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xdfbd3e540, IoControlCode=0x00500016, InputBuffer=0xdfbd3e550, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '═x эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xdfbd3e668, InputBufferLength=0xa0, OutputBuffer=0xdfbd3e668, OutputBufferLength=0xa0, ReturnLength=0xdfbd3e660 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xdfbd3e6a8, InputBufferLength=0x18, OutputBuffer=0xdfbd3e6c0, OutputBufferLength=0x78, ReturnLength=0xdfbd3e6a0 [0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xdfbd3e6a0 [0x70]) => 0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0xc [TokenSessionId], TokenInformation=0xdfbd3dfc0, Length=4, ReturnLength=0xdfbd3dfa0 [4]) => 0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0x1d [TokenIsAppContainer], TokenInformation=0xdfbd3e008, Length=4, ReturnLength=0xdfbd3dfa0 [4]) => 0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0x2a [TokenPrivateNameSpace], TokenInformation=0xdfbd3dfa4, Length=4, ReturnLength=0xdfbd3dfa0 [4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0xdfbd3dfc8 [0x74], DesiredAccess=0xf, ObjectAttributes="\Sessions\21\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0x2c [TokenBnoIsolation], TokenInformation=0xdfbd3e2c0, Length=0x120, ReturnLength=0xdfbd3dfa0 [0x10]) => 0

NtClose(Handle=0x70) => 0

NtCreateMutant(MutantHandle=0xdfbd3e6f8 [0x78], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1, ObjectAttributes=0x74:"Local\SM0:7496:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x78, Alertable=false, Timeout=null) => 0

NtOpenSemaphore(SemaphoreHandle=0xdfbd3e4e8, DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x74:"Local\SM0:7496:304:WilStaging_02_p0") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtCreateSemaphore(SemaphoreHandle=0xdfbd3e3d8 [0x7c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x74:"Local\SM0:7496:304:WilStaging_02_p0", InitialCount=0x74fe123c, MaxCount=0x74fe123c) => 0

NtCreateSemaphore(SemaphoreHandle=0xdfbd3e3d8 [0x80], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x74:"Local\SM0:7496:304:WilStaging_02_p0h", InitialCount=0xaf, MaxCount=0xaf) => 0

NtReleaseMutant(MutantHandle=0x78, PreviousCount=null) => 0

NtQueryWnfStateData(StateName=0xdfbd3e750 [0xa3bc0875], TypeId=0xdfbd3e7f8, ExplicitScope=null, ChangeStamp=0xdfbd3e744 [0xb], Buffer=0xdfbd3d740, BufferSize=0xdfbd3e740 [8]) => 0

NtCreateEvent(EventHandle=0xdfbd3e6b0 [0x84], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3de70 [0x0000015fd3f85000], ZeroBits=0, pSize=0xdfbd3df18 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x15fd3f84f90 [0x88], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x84) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x88, IoCompletionHandle=0x18, TargetObjectHandle=0x84, KeyContext=0x15fd3f84fa8,

ApcContext=0x15fd3f84e20, IoStatus=0x0000015f00000000, IoStatusInformation=0, AlreadySignaled=0xdfbd3e630 [0xd3f80b00]) => 0

NtSubscribeWnfStateChange(StateName=0x15fd3f85120 [0xa3bc0875], ChangeStamp=0xb, EventMask=0x11, SubscriptionId=0xdfbd3e720 [0x000475f4]) => 0

NtQueryWnfStateData(StateName=0xdfbd3e890 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xdfbd3e888 [0], Buffer=null, BufferSize=0xdfbd3e88c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x15fd3f85450 [0xa3bc7c75], ChangeStamp=0, EventMask=0x11, SubscriptionId=0xdfbd3e700 [0x000475f5]) => 0

NtQueryWnfStateData(StateName=0xdfbd3e890 [0xa3bc88f5], TypeId=null, ExplicitScope=null, ChangeStamp=0xdfbd3e888 [0], Buffer=null, BufferSize=0xdfbd3e88c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x15fd3f85600 [0xa3bc88f5], ChangeStamp=0, EventMask=0x11, SubscriptionId=0xdfbd3e700 [0x000475f6]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3 [SystemFeatureConfigurationSectionInformation], QueryType=0xdfbd3e640 [0], Alignment=0x18, SystemInformation=0xdfbd3e660, Length=0x50, ReturnLength=null) => 0

NtMapViewOfSection(SectionHandle=0x70, ProcessHandle=-1, BaseAddress=0xdfbd3e610 [0x0000015fd3e50000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xdfbd3e618 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x60, ProcessHandle=-1, BaseAddress=0xdfbd3e610 [0x0000015fd4080000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xdfbd3e618 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x4c, ProcessHandle=-1, BaseAddress=0xdfbd3e610 [0x0000015fd4090000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xdfbd3e618 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0x70) => 0

NtClose(Handle=0x60) => 0

NtClose(Handle=0x4c) => 0

NtQueryWnfStateData(StateName=0xdfbd3e648 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xdfbd3e6d8 [0], Buffer=0xdfbd3e730, BufferSize=0xdfbd3e630 [0]) => 0

NtSetTimer2(TimerHandle=0x28, DueTime=0xdfbd3e6c0 [-3e+09], Period=null, Parameters=0xdfbd3e6c8) => 0

NtOpenKey(KeyHandle=0xdfbd3e890, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys") => 0xc0000034 [2 '≔x єфрхЄё эрщЄш єърчрээ∀щ Їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xdfbd3e8a8, InputBufferLength=0xa0, OutputBuffer=0xdfbd3e8a8, OutputBufferLength=0xa0, ReturnLength=0xdfbd3e8a0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xdfbd3e8e8, InputBufferLength=0x18, OutputBuffer=0xdfbd3e900, OutputBufferLength=0x78, ReturnLength=0xdfbd3e8e0 [0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e1c0 [0x0000015fd3f86000], ZeroBits=0, pSize=0xdfbd3e268 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xdfbd3e8d8, InputBufferLength=0xa0, OutputBuffer=0xdfbd3e8d8, OutputBufferLength=0xa0, ReturnLength=0xdfbd3e8d0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xdfbd3e918, InputBufferLength=0x18, OutputBuffer=0xdfbd3e930, OutputBufferLength=0x78, ReturnLength=0xdfbd3e910 [0]) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3ebe0, VmInformation=0xdfbd3ecb8, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtOpenKey(KeyHandle=0xdfbd3e7c0, DesiredAccess=0x9, ObjectAttributes=0xc:"parent.exe") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xdfbd3e6c8, InputBufferLength=0xa0, OutputBuffer=0xdfbd3e6c8, OutputBufferLength=0xa0, ReturnLength=0xdfbd3e6c0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xdfbd3e708, InputBufferLength=0x18, OutputBuffer=0xdfbd3e720, OutputBufferLength=0x78, ReturnLength=0xdfbd3e700 [0]) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x7ffa74b17aa0, Length=0x40, ReturnLength=null) => 0

NtSetEvent(EventHandle=0x40, PrevState=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=4, OldProtect=0xdfbd3e908 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e8f8 [0x00007ffa732b3000], Size=0xdfbd3e8f0 [0x1000], NewProtect=2, OldProtect=0xdfbd3e908 [4]) => 0

NtOpenKey(KeyHandle=0xdfbd3eee0, DesiredAccess=0x3, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xdfbd3eec0, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xdfbd3eeb8 [0x8c], DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0

NtQueryValueKey(KeyHandle=0x8c, ValueName="TransparentEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xdfbd3ef70, Length=0x50, ResultLength=0xdfbd3eeb0) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x8c) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0xdfbd3ee00, Length=0x58, ReturnLength=0xdfbd3edf8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xdfbd3eeb8, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-279210374-529612743-1025975986-1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xdfbd3efa0 [0x90], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x90, ValueName="LongPathsEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xdfbd3efe0, Length=0x14, ResultLength=0xdfbd3efa8 [0x10]) => 0

NtClose(Handle=0x90) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0xdfbd3ef80, Length=4) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xdfbd3ef00 [1], Alignment=4, SystemInformation=0x15fd3f83840, Length=0x50, ReturnLength=0xdfbd3eef8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x15fd3f86270 [0x94], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, NumberOfConcurrentThreads=5) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x15fd3f86268 [0x8c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null, CompletionPortHandle=0x94, WorkerProcessHandle=-1, StartRoutine=0x7ffa7563d110, StartParameter=0x15fd3f86230, MaxThreadCount=0x200, StackReserve=0x00100000, StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=0xd [WorkerFactoryFlags], Buffer=0xdfbd3efc8, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x15fd3f862c0 [0x98], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x15fd3f862c8 [0x90], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x90, IoCompletionHandle=0x94, TargetObjectHandle=0x98, KeyContext=0x15fd3f862d0, ApcContext=0x15fd3f862a0, IoStatus=0, IoStatusInformation=1, AlreadySignaled=0xdfbd3eec0 [0]) => 0

NtCreateTimer2(TimerHandle=0x15fd3f86338 [0x5c], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x15f00000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x15fd3f86340 [0x9c], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x9c, IoCompletionHandle=0x94, TargetObjectHandle=0x5c, KeyContext=0x15fd3f86348, ApcContext=0x15fd3f862a0, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0xdfbd3eec0 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=2 [WorkerFactoryIdleTimeout], Buffer=0xdfbd3efc8, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0xdfbd3efc8, BufferLength=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3efd0 [0x00007ff642e23000], Size=0xdfbd3efd8 [0x1000], NewProtect=4, OldProtect=0xdfbd3f368 [2]) => 0

NtOpenSection(SectionHandle=0xdfbd3ea68, DesiredAccess=0xd, ObjectAttributes=0x3c:"VCRUNTIME140D.dll") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtOpenSection(SectionHandle=0xdfbd3ea68, DesiredAccess=0xd, ObjectAttributes=0x3c:"ucrtbased.dll") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtQueryWnfStateData(StateName=0xdfbd3e860 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xdfbd3e8f8 [0], Buffer=0xdfbd3e950, BufferSize=0xdfbd3e850 [0]) => 0

NtQueryWnfStateData(StateName=0xdfbd3e700 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xdfbd3e798 [0], Buffer=0xdfbd3e7f0, BufferSize=0xdfbd3e6f0 [0]) => 0

NtOpenKey(KeyHandle=0xdfbd3ead0 [0xa0], DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xa0, ValueName="SafeDllSearchMode", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xdfbd3eae0, Length=0x10, ResultLength=0xdfbd3ead8) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e2b0 [0x0000015fd3f87000], ZeroBits=0, pSize=0xdfbd3e358 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\lab1.1\VCRUNTIME140D.dll", Attributes=0xdfbd3eb78) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\VCRUNTIME140D.dll", Attributes=0xdfbd3eb78 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0xdfbd3ec80 [0xa4], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\VCRUNTIME140D.dll", IoStatusBlock=0xdfbd3ece8 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xdfbd3ec88 [0xa8], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xa4) => 0

Loaded DLL at 00007FFA6C490000 C:\Windows\SYSTEM32\VCRUNTIME140D.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x15fd3f86470 [0x00007ffa6c490000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15fd3f836c0 [0x0002b000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3eb20 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb30 [0x00007ffa75771000], Size=0xdfbd3eb28 [0x4000], NewProtect=4, OldProtect=0xdfbd3eb20 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb30 [0x00007ffa75771000], Size=0xdfbd3eb28 [0x4000], NewProtect=2, OldProtect=0xdfbd3eb20 [4]) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xdfbd3e600, Length=0x330, ReturnLength=0xdfbd3e5b8) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xdfbd3e600, Length=0x330, ReturnLength=0xdfbd3e5b8) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb80 [0x00007ffa6c4b0000], Size=0xdfbd3eb88 [0x1000], NewProtect=4, OldProtect=0x15fd3f836a8 [2]) => 0

NtOpenSection(SectionHandle=0xdfbd3e618, DesiredAccess=0xd, ObjectAttributes=0x3c:"ucrtbased.dll") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xa8) => 0

NtClose(Handle=0xa4) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\lab1.1\ucrtbased.dll", Attributes=0xdfbd3eb78) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", Attributes=0xdfbd3eb78 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0xdfbd3ec80 [0xa8], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", IoStatusBlock=0xdfbd3ece8 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xdfbd3ec88 [0xac], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xa8) => 0

Loaded DLL at 00007FFA34C30000 C:\Windows\SYSTEM32\ucrtbased.dll

NtMapViewOfSection(SectionHandle=0xac, ProcessHandle=-1, BaseAddress=0x15fd3f866d0 [0x00007ffa34c30000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15fd3f86630 [0x00221000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3eb20 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb30 [0x00007ffa75771000], Size=0xdfbd3eb28 [0x4000], NewProtect=4, OldProtect=0xdfbd3eb20 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb30 [0x00007ffa75771000], Size=0xdfbd3eb28 [0x4000], NewProtect=2, OldProtect=0xdfbd3eb20 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3eb80 [0x00007ffa34ddb000], Size=0xdfbd3eb88 [0x1000], NewProtect=4, OldProtect=0x15fd3f86618 [2]) => 0

NtClose(Handle=0xac) => 0

NtClose(Handle=0xa8) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\lab1.1\ucrtbased.dll", Attributes=0xdfbd3eb78) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", Attributes=0xdfbd3eb78 [ARCHIVE]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3f348 [0x00007ff642e23000], Size=0xdfbd3f350 [0x1000], NewProtect=2, OldProtect=0xdfbd3eea0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3f865f8 [0x00007ffa34ddb000], Size=0x15fd3f86600 [0x1000], NewProtect=2, OldProtect=0xdfbd3eea0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3f83688 [0x00007ffa6c4b0000], Size=0x15fd3f83690 [0x1000], NewProtect=2, OldProtect=0xdfbd3eea0 [4]) => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3f208, VmInformation=0xdfbd3f130, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11 [ThreadHideFromDebugger], ThreadInformation=0xdfbd3f040, Length=1, ReturnLength=null) => 0

Initial breakpoint

NtSetEvent(EventHandle=0x40, PrevState=null) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3eec0, VmInformation=0xdfbd3ef98, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e290 [0x0000015fd3f88000], ZeroBits=0, pSize=0xdfbd3e338 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x50, IoStatusBlock=0xdfbd3ebe0 [0/8], FsInformation=0xdfbd3ec00, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xdfbd3ebe0 [0/8], FsInformation=0xdfbd3ec00, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0xdfbd3ebe0 [0/8], FsInformation=0xdfbd3ec00, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtOpenKey(KeyHandle=0xdfbd3d6c0 [0xac], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions") => 0

NtQueryValueKey(KeyHandle=0xac, ValueName="", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0xdfbd3dba0, Length=0x214, ResultLength=0xdfbd3db58 [0x2a]) => 0

NtQueryValueKey(KeyHandle=0xac, ValueName="000603xx", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0xdfbd3db80, Length=0x214, ResultLength=0xdfbd3d938 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e2f0 [0x0000015fd3f8a000], ZeroBits=0, pSize=0xdfbd3e398 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e2d0 [0x0000015fd3f8c000], ZeroBits=0, pSize=0xdfbd3e378 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3ef00, VmInformation=0xdfbd3efd8, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtSetEvent(EventHandle=0x40, PrevState=null) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=3 [WorkerFactoryBindingCount], Buffer=0xdfbd3f368, BufferLength=4) => 0

NtSetEvent(EventHandle=8, PrevState=null) => 0

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff642e11122, MemoryInformationClass=0 [MemoryBasicInformation], MemoryInformation=0xdfbd3f580, Length=0x30, ReturnLength=0xdfbd3f530 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff642e11122, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xdfbd3f5b0, Length=0x30, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff642e11122, MemoryInformationClass=2 [MemoryMappedFilenameInformation], MemoryInformation=0xdfbd3f628, Length=0x21a, ReturnLength=null) => 0

Incorrect num argsNtDeviceIoControlFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xdfbd3d990 [0/0x12], IoControlCode=0x00500016, InputBuffer=0xdfbd3d9a0, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0xdfbd3f1a0, Length=4) => 0

NtOpenSection(SectionHandle=0xdfbd3f178, DesiredAccess=0xd, ObjectAttributes=0x3c:"kernel.appcore.dll") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээvщ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\kernel.appcore.dll", Attributes=0xdfbd3ef38 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0xdfbd3ef30 [0xb0], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0xdfbd3ef98 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xdfbd3ef38 [0xb4], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xb0) => 0

Loaded DLL at 00007FFA70AD0000 C:\Windows\SYSTEM32\kernel.appcore.dll

NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x15fd3f8a630 [0x00007ffa70ad0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15fd3f8acb0 [0x00012000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3edd0 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3ede8 [0x00007ffa70adf000], Size=0xdfbd3ede0 [0x1000], NewProtect=2, OldProtect=0xdfbd3ee50 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3ede0 [0x00007ffa75771000], Size=0xdfbd3edd8 [0x4000], NewProtect=4, OldProtect=0xdfbd3edd0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3ede0 [0x00007ffa75771000], Size=0xdfbd3edd8 [0x4000], NewProtect=2, OldProtect=0xdfbd3edd0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3ee30 [0x00007ffa70ad5000], Size=0xdfbd3ee38 [0x1000], NewProtect=4, OldProtect=0x15fd3f8ac98 [2]) => 0

NtOpenSection(SectionHandle=0xdfbd3e8c8 [0xa8], DesiredAccess=0xd, ObjectAttributes=0x3c:"msvcrt.dll") => 0

Loaded DLL at 00007FFA75400000 C:\Windows\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x15fd3f8ca00 [0x00007ffa75400000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15fd3f8c960 [0x0009e000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3e740 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e750 [0x00007ffa75771000], Size=0xdfbd3e748 [0x4000], NewProtect=4, OldProtect=0xdfbd3e740 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e750 [0x00007ffa75771000], Size=0xdfbd3e748 [0x4000], NewProtect=2, OldProtect=0xdfbd3e740 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e7a0 [0x00007ffa75476000], Size=0xdfbd3e7a8 [0x2000], NewProtect=4, OldProtect=0x15fd3f8c948 [2]) => 0

NtClose(Handle=0xa8) => 0

NtOpenSection(SectionHandle=0xdfbd3e8c8 [0xa8], DesiredAccess=0xd, ObjectAttributes=0x3c:"RPCRT4.dll") => 0

Loaded DLL at 00007FFA75140000 C:\Windows\System32\RPCRT4.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x15fd3f8cdc0 [0x00007ffa75140000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x15fd3f8cd20 [0x00123000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xdfbd3e740 [1.79995e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e758 [0x00007ffa7525b000], Size=0xdfbd3e750 [0x1000], NewProtect=2, OldProtect=0xdfbd3e7c0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e750 [0x00007ffa75771000], Size=0xdfbd3e748 [0x4000], NewProtect=4, OldProtect=0xdfbd3e740 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e750 [0x00007ffa75771000], Size=0xdfbd3e748 [0x4000], NewProtect=2, OldProtect=0xdfbd3e740 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xdfbd3e7a0 [0x00007ffa7522c000], Size=0xdfbd3e7a8 [0x2000], NewProtect=4, OldProtect=0x15fd3f8cd08 [2]) => 0

NtClose(Handle=0xa8) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3f8ac78 [0x00007ffa70ad5000], Size=0x15fd3f8ac80 [0x1000], NewProtect=2, OldProtect=0xdfbd3ed20 [4]) => 0

NtClose(Handle=0xb4) => 0

NtClose(Handle=0xb0) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3f8c928 [0x00007ffa75476000], Size=0x15fd3f8c930 [0x2000], NewProtect=2, OldProtect=0xdfbd3f040 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0xdfbd3efa0, Length=0x28) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x15fd3f8cce8 [0x00007ffa7522c000], Size=0x15fd3f8ccf0 [0x2000], NewProtect=2, OldProtect=0xdfbd3f040 [4]) => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3f060, VmInformation=0xdfbd3f138, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e890 [0x0000015fd40a0000], ZeroBits=0, pSize=0xdfbd3e898 [0x001b0000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e890 [0x0000015fd40a0000], pSize=0xdfbd3e888 [0x001a0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e878 [0x0000015fd4240000], ZeroBits=0, pSize=0xdfbd3e870 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x50, IoStatusBlock=0xdfbd3ee60 [0/8], FsInformation=0xdfbd3ee80, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xdfbd3ee60 [0/8], FsInformation=0xdfbd3ee80, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0xdfbd3ee60 [0/8], FsInformation=0xdfbd3ee80, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e700 [0x0000015fd3f8e000], ZeroBits=0, pSize=0xdfbd3e7a8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e6d0 [0x0000015fd4242000], ZeroBits=0, pSize=0xdfbd3e778 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xdfbd3e6b0 [0x0000015fd4243000], ZeroBits=0, pSize=0xdfbd3e758 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3f060, VmInformation=0xdfbd3f138, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xdfbd3f0a0, VmInformation=0xdfbd3f178, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtSetEvent(EventHandle=0x40, PrevState=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xdfbd3f2d0, Length=0x330, ReturnLength=0xdfbd3f288) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xdfbd3f2d0, Length=0x330, ReturnLength=0xdfbd3f288) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtTerminateProcess(ProcessHandle=0, ExitStatus=1) => 0

NtClose(Handle=0x60) => 0

NtClose(Handle=0x6c) => 0

NtClose(Handle=0x4c) => 0

NtClose(Handle=0x70) => 0

NtQueryWnfStateData(StateName=0xdfbd3f380 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xdfbd3e2c4 [0x54aa], Buffer=0xdfbd3e320, BufferSize=0xdfbd3e2c0 [0xb6e]) => 0

NtQueryWnfStateData(StateName=0xdfbd3f208 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xdfbd3f298 [0], Buffer=0xdfbd3f2f0, BufferSize=0xdfbd3f1f0 [0]) => 0

Process 7496 exit code: 1

Вывод

В ходе выполнения лабораторной работы я познакомился с такими системными вызовами, как CreateNamedPipe, ConnectNamedPipe, WriteFile, ReadFile, CloseHandle, CreateFile, GetStdHandle, и написал программу для деления чисел, записанных построчно в файл. Проблем при выполнении работы не возникло.