

Московский Авиационный Институт
(Национальный Исследовательский Университет)
Институт №8 “Компьютерные науки и прикладная математика”
Кафедра №806 “Вычислительная математика и программирование”

Лабораторная работа №3 по курсу
«Операционные системы»

Группа: М8О-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 команды, 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. Родительский процесс передает команды пользователя через `file mapping`, который связан со стандартным входным потоком дочернего процесса. Результаты своей работы дочерний процесс пишет в стандартный поток вывода.

Общий метод и алгоритм решения

Использованные системные вызовы:

- `CreateFileMapping` – создает `file mapping`
- `MapViewOfFile` – позволяет посмотреть данные в `file mapping`
- `ReadFile` – читает данные из канала
- `CloseHandle` – закрывает хэндлеры
- `WriteFile` – записывает данные в канал
- `WriteConsoleA` – записывает данные в консоль
- `CreateSemaphore` – создает семафор
- `ReleaseSemaphore` - закрывает один из потоков
- `WaitForSingleObject` - ожидание, пока поток закончит свою работу
- `UnmapViewOfFile` - отменяет сопоставление сопоставленного представления файла из адресного пространства вызывающего процесса

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. Передача данных между процессами осуществляется через `file mapping`.

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++;

                }

            }

        }

        fmt_ptr++;

    }

    *buf_ptr++ = *fmt_ptr++;

}

```

```

    }

    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,
```

```
    ERROR_ARGS_COUNT,
```

```
    ERROR_CREATE_PIPE,
```

```
    ERROR_CREATE_CHILD_PROCESS,
```

```
    ERROR_READ,
```

```
    ERROR_DEV_ZERO,
```

```
    ERROR_FULL,
```

```
    ERROR_OPEN_FILE,
```

```
    ERROR_CLOSE_FILE,
```

```
    ERROR_FILE_WRITE,
```

```
    ERROR_HANDLER_INHERITED,
```

```
    ERROR_PIPE_WRITE,
```

```
    ERROR_HEAP,
```

```
    ERR_FMAP,
```

```
    ERR_SEM,
```

```
    ERR_MAPVIEW
```

```
};
```

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

```
    //my_printf("1\n");
```



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

```
HANDLE hMapFile = CreateFileMapping(INVALID_HANDLE_VALUE, NULL,  
PAGE_READWRITE, 0, BUFFER_SIZE, ConvertToWideString("SharedMemory"));
```

```
if (hMapFile == NULL) {  
    my_printf("Failed to create file mapping\n");  
    return ERR_FMAP;  
}
```

```
HANDLE hSemParent = CreateSemaphore(NULL, 1, 1,  
ConvertToWideString("SemaphoreParent"));
```

```
HANDLE hSemChild = CreateSemaphore(NULL, 0, 1,  
ConvertToWideString("SemaphoreChild"));
```

```
if (hSemParent == NULL || hSemChild == NULL) {  
    CloseHandle(hMapFile);  
    my_printf("Failed to create semaphore\n");  
    return ERR_SEM;  
}
```

```
char* pBuf = (char*)MapViewOfFile(hMapFile, FILE_MAP_ALL_ACCESS, 0, 0,  
BUFFER_SIZE);
```

```
if (pBuf == NULL) {  
    CloseHandle(hMapFile);  
    CloseHandle(hSemParent);  
    CloseHandle(hSemChild);  
    my_printf("Failed to map view of file\n");  
    return ERR_MAPVIEW;
```

```

}

char fileName[BUFFER_SIZE];

char buffer[BUFFER_SIZE];

DWORD bytesRead, bytesWritten;


//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)) {

    UnmapViewOfFile(pBuf);

    CloseHandle(hMapFile);

    CloseHandle(hSemParent);

    CloseHandle(hSemChild);

    my_printf("Failed to create process");

    return ERROR_CREATE_CHILD_PROCESS;

}

```

```
WaitForSingleObject(hSemParent, INFINITE);  
  
strcpy(pBuf, buffer);  
  
ReleaseSemaphore(hSemChild, 1, NULL);
```

```
WaitForSingleObject(hSemParent, INFINITE);  
  
if (strcmp(pBuf, "DIVIDE_BY_ZERO") == 0) {  
    my_printf("Zero division error");  
    return ERROR_DEV_ZERO;  
}
```

```
UnmapViewOfFile(pBuf);  
  
CloseHandle(hMapFile);  
  
CloseHandle(hSemParent);  
  
CloseHandle(hSemChild);  
  
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,  
  
    ERROR_ARGS_COUNT,  
  
    ERROR_CREATE_PIPE,  
  
    ERROR_CREATE_CHILD_PROCESS,  
  
    ERROR_READ,  
  
    ERROR_DEV_ZERO,  
  
    ERROR_FULL,  
  
    ERROR_OPEN_FILE,  
  
    ERROR_CLOSE_FILE,  
  
    ERROR_FILE_WRITE,  
  
    ERROR_HANDLER_INHERITED,  
  
    ERROR_PIPE_WRITE,  
  
    ERROR_HEAP,  
  
    ERR_FMAP,  
  
    ERR_SEM,  
  
    ERR_MAPVIEW  
};
```

```
int main() {  
  
    char buffer[BUFFER_SIZE];  
  
    DWORD bytesRead, bytesWritten;  
  
    HANDLE hMapFile = OpenFileMapping(FILE_MAP_ALL_ACCESS, FALSE,  
    ConvertToWideString("SharedMemory"));  
  
    HANDLE hSemParent = OpenSemaphore(SEMAPHORE_ALL_ACCESS, FALSE,  
    ConvertToWideString("SemaphoreParent"));  
  
    HANDLE hSemChild = OpenSemaphore(SEMAPHORE_ALL_ACCESS, FALSE,  
    ConvertToWideString("SemaphoreChild"));  
  
    if (hMapFile == NULL || hSemParent == NULL || hSemChild == NULL) {
```

```
my_printf("Failed to open file mapping or semaphore\n");  
  
return ERR_FMAP;  
  
}
```

```
char* pBuf = (char*)MapViewOfFile(hMapFile, FILE_MAP_ALL_ACCESS, 0, 0,  
BUFFER_SIZE);
```

```
if (pBuf == NULL) {  
    CloseHandle(hMapFile);  
    CloseHandle(hSemParent);  
    CloseHandle(hSemChild);  
    my_printf("Failed to map view of file\n");  
    return ERR_MAPVIEW;  
}
```

```
WaitForSingleObject(hSemChild, INFINITE);  
  
strcpy(buffer, pBuf);
```

```
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) {

            strcpy(pBuf, "DIVIDE_BY_ZERO");

            ReleaseSemaphore(hSemParent, 1, NULL);

            UnmapViewOfFile(pBuf);

            CloseHandle(hMapFile);

            CloseHandle(hSemParent);

            CloseHandle(hSemChild);

            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);

}

```

```
ReleaseSemaphore(hSemParent, 1, NULL);
```

```
UnmapViewOfFile(pBuf);
```

```
CloseHandle(hMapFile);
```

```
CloseHandle(hSemParent);
```

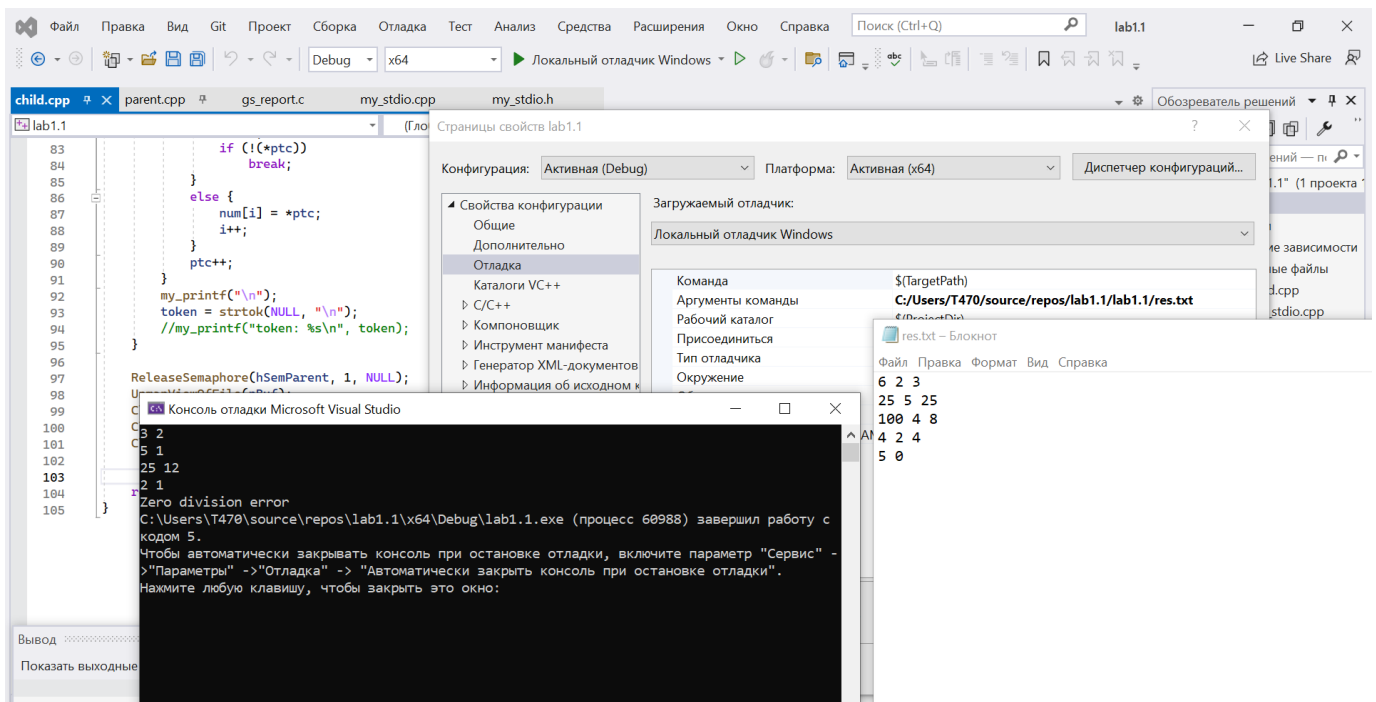
```
CloseHandle(hSemChild);
```

```
return SUCCESS;
```

```
}
```

Протокол работы программы

Тестирование:



NtTrace:

Process 44704 starting at 00007FF6C36C12FD with command line: "parent.exe"

C:\Users\T470\source\repos\lab1.1\x64\Debug\parent.exe

Loaded DLL at 00007FFB552F0000 C:\Windows\SYSTEM32\ntdll.dll

NtQueryPerformanceCounter(Counter=0xbc284ff640 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff688 [0x00007ffb55474000], Size=0xbc284ff680 [0x1000], NewProtect=4, OldProtect=0xbc284ff6c0 [8]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff688 [0x00007ffb55474000], Size=0xbc284ff680 [0x1000], NewProtect=8, OldProtect=0xbc284ff6c0 [4]) => 0

NtCreateEvent(EventHandle=0x7ffb5545c478 [8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xbc284ff5f0, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xbc284ff318, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation], SystemInformation=0xbc284ff1f0, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffb552f0000, MemoryInformationClass=6 [MemoryImageInformation], MemoryInformation=0xbc284ff100, Length=0x18, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4 [MemoryWorkingSetExInformation], MemoryInformation=0xbc284ff1c0, Length=0x50, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff210 [0x00007ffb55471000], Size=0xbc284ff208 [0x4000], NewProtect=2, OldProtect=0xbc284ff200 [4]) => 0

NtOpenKey(KeyHandle=0xbc284fde50 [0xc], DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xc, ValueName="RaiseExceptionOnPossibleDeadlock", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xbc284fde60, Length=0x50, ResultLength=0xbc284fde58) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Ърщы.']

NtClose(Handle=0xc) => 0

NtOpenKey(KeyHandle=0xbc284fdde8 [0x10], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options") => 0

NtOpenKey(KeyHandle=0xbc284fde0, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ їрщы.']

NtOpenKey(KeyHandle=0xbc284fde30, 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=0x7ffb5545d230, Length=4, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xbc284ff1a8, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xbc284febe0, Length=0x330, ReturnLength=0xbc284feb98) => 0xc0000225 [1168 'ЫХЬХЭЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xbc284febe0, Length=0x330, ReturnLength=0xbc284feb98) => 0xc0000225 [1168 'ЫХЬХЭЄ эх эрщфхэ.']

NtOpenKey(KeyHandle=0xbc284ff120 [0xc], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xc, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xbc284ff160, Length=0x18, ResultLength=0xbc284ff128) => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ їрщы.']

NtClose(Handle=0xc) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xbc284ff200, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xbc284ff1a0, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation], SystemInformation=0xbc284ff1d0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffb5545dc38 [0x00007ff5f7e80000], ZeroBits=0x000000bc284ff150, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0xbc284ff0b8, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffb5545dc30 [0x00007ff5f9e80000], ZeroBits=0x000000bc284ff158, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null, DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffb5545dca0 [0x00007ff4f7e60000], ZeroBits=0x000000bc284ff100, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0xbc284ff068, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xbc284ff040, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fec00 [0x0000025effbe0000], ZeroBits=0, pSize=0xbc284fec08 [0x00110000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fec00 [0x0000025effbe0000], pSize=0xbc284feb8 [0x00010000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284febe8 [0x0000025effbf0000], ZeroBits=0, pSize=0xbc284febe0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5 [SystemHypervisorSharedPageInformation], SystemInformation=0xbc284ff3a8, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap], SystemInformation=0xbc284fee10, Length=0x408, ReturnLength=0xbc284ff230 [0x18]) => 0

NtCreateEvent(EventHandle=0xbc284ff048 [0x14], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x25effbf0b20 [0xc], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xbc284feda0 [1], Alignment=4, SystemInformation=0x25effbf0ed0, Length=0x50, ReturnLength=0xbc284fed98 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x25effbf0c00 [0x18], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, NumberOfConcurrentThreads=5) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x25effbf0bf8 [0x1c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null, CompletionPortHandle=0x18, WorkerProcessHandle=-1, StartRoutine=0x7ffb5533d110, StartParameter=0x25effbf0bc0, MaxThreadCount=0x200, StackReserve=0x00100000, StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x25effbf0c50 [0x20], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x7ffb00000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x25effbf0c58 [0x24], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x24, IoCompletionHandle=0x18, TargetObjectHandle=0x20, KeyContext=0x25effbf0c60, ApcContext=0x25effbf0c30, IoStatus=0, IoStatusInformation=1, AlreadySignaled=0xbc284fed60 [0]) => 0

NtCreateTimer2(TimerHandle=0x25effbf0cc8 [0x28], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x25e000000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x25effbf0cd0 [0x2c], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x2c, IoCompletionHandle=0x18, TargetObjectHandle=0x28, KeyContext=0x25effbf0cd8, ApcContext=0x25effbf0c30, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0xbc284fed60 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0xbc284fee68, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=0xe [WorkerFactoryThreadSoftMaximum], Buffer=0xbc284fee68, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=3 [WorkerFactoryBindingCount], Buffer=0xbc284fef88, BufferLength=4) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xc, IoCompletionHandle=0x18, TargetObjectHandle=0x14, KeyContext=0x25effbf0b38, ApcContext=0x25effbf09b0, IoStatus=0x0000025e00000000, IoStatusInformation=0, AlreadySignaled=0xbc284fedd0 [0xffbf0b00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0xbc284ff088, InputBufferLength=4, OutputBuffer=null, OutputBufferLength=0, ReturnLength=0xbc284ff040 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xbc284ff0e8, InputBufferLength=0xa0, OutputBuffer=0xbc284ff0e8, OutputBufferLength=0xa0, ReturnLength=0xbc284ff0e0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xbc284ff0e8, InputBufferLength=0xa0, OutputBuffer=0xbc284ff0e8, OutputBufferLength=0xa0, ReturnLength=0xbc284ff0e0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xbc284ff0e8, InputBufferLength=0xa0, OutputBuffer=0xbc284ff0e8, OutputBufferLength=0xa0, ReturnLength=0xbc284ff0e0 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, IpAddress=0xbc284fea50 [0x0000025effbf2000], ZeroBits=0, pSize=0xbc284feaf8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, IpAddress=0xbc284ff230 [0x0000025effb70000], pSize=0xbc284ff238 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff210 [0x00007ffb55471000], Size=0xbc284ff208 [0x4000], NewProtect=4, OldProtect=0xbc284ff200 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ffb55471298 [0x3c], DesiredAccess=0x3, ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff210 [0x00007ffb55471000], Size=0xbc284ff208 [0x4000], NewProtect=2, OldProtect=0xbc284ff200 [4]) => 0

NtOpenSymbolicLinkObject(LinkHandle=0xbc284ff368 [0x40], DesiredAccess=0x1, ObjectAttributes=0x3c:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x40, LinkTarget="C:\Windows\System32", ReturnedLength=0xbc284ff31c [0x28]) => 0

NtClose(Handle=0x40) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff1e0 [0x00007ffb55471000], Size=0xbc284ff1d8 [0x4000], NewProtect=4, OldProtect=0xbc284ff1d0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff210 [0x00007ffb55471000], Size=0xbc284ff208 [0x4000], NewProtect=2, OldProtect=0xbc284ff200 [4]) => 0

NtCreateEvent(EventHandle=0x7ffb5545c380 [0x44], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ffb5545c3b0 [0x48], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtQueryPerformanceCounter(Counter=0xbc284ff160 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff170 [0x00007ffb55471000], Size=0xbc284ff168 [0x4000], NewProtect=4, OldProtect=0xbc284ff160 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff170 [0x00007ffb55471000], Size=0xbc284ff168 [0x4000], NewProtect=2, OldProtect=0xbc284ff160 [4]) => 0

NtOpenFile(FileHandle=0xbc284ff218 [0x40], DesiredAccess=SYNCHRONIZE|0x20, ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\x64\Debug\", IoStatusBlock=0xbc284ff188 [0/1], ShareAccess=3, OpenOptions=0x21) => 0

NtQueryVolumeInformationFile(FileHandle=0x40, IoStatusBlock=0xbc284ff188 [0/8], FsInformation=0xbc284ff170, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtSetEvent(EventHandle=0x44, PrevState=null) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0xbc284feed0, Length=4) => 0

NtOpenSection(SectionHandle=0xbc284feea8 [0x4c], DesiredAccess=0xd, ObjectAttributes=0x3c:"KERNEL32.DLL") => 0

Loaded DLL at 00007FFB551E0000 C:\Windows\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x4c, ProcessHandle=-1, BaseAddress=0x25effbf32a0 [0x00007ffb551e0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x25effbf3200 [0x000c2000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xbc284fed20 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed38 [0x00007ffb5529f000], Size=0xbc284fed30 [0x1000], NewProtect=2, OldProtect=0xbc284feda0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed30 [0x00007ffb55471000], Size=0xbc284fed28 [0x4000], NewProtect=4, OldProtect=0xbc284fed20 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed30 [0x00007ffb55471000], Size=0xbc284fed28 [0x4000], NewProtect=2, OldProtect=0xbc284fed20 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed80 [0x00007ffb55263000], Size=0xbc284fed88 [0x4000], NewProtect=4, OldProtect=0x25effbf31e8 [2]) => 0

NtOpenSection(SectionHandle=0xbc284fe818 [0x5c], DesiredAccess=0xd, ObjectAttributes=0x3c:"KERNELBASE.dll") => 0

Loaded DLL at 00007FFB52990000 C:\Windows\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x25effbf3980 [0x00007ffb52990000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x25effbf38e0 [0x002fe000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xbc284fe690 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe6a8 [0x00007ffb52c63000], Size=0xbc284fe6a0 [0x1000], NewProtect=2, OldProtect=0xbc284fe710 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe6a0 [0x00007ffb55471000], Size=0xbc284fe698 [0x4000], NewProtect=4, OldProtect=0xbc284fe690 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe6a0 [0x00007ffb55471000], Size=0xbc284fe698 [0x4000], NewProtect=2, OldProtect=0xbc284fe690 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe6f0 [0x00007ffb52b7a000], Size=0xbc284fe6f8 [0x3000], NewProtect=4, OldProtect=0x25effbf38c8 [2]) => 0

NtClose(Handle=0x5c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effbf31c8 [0x00007ffb55263000], Size=0x25effbf31d0 [0x4000], NewProtect=2, OldProtect=0xbc284fec70 [4]) => 0

NtClose(Handle=0x4c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effbf38a8 [0x00007ffb52b7a000], Size=0x25effbf38b0 [0x3000], NewProtect=2, OldProtect=0xbc284fed70 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0xbc284fecd0, Length=0x28) => 0

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

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xbc284fed90, VmInformation=0xbc284fee68, VmInformationLength=4) => 0xc00000bb [50 'пррющ чряЁюё эх яюфхЁцштрхЄё .']

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation], SystemInformation=0xbc284fe9f0, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x7ffb52c4ee60, Length=0x40, ReturnLength=null) => 0

NtOpenSection(SectionHandle=0xbc284fe7b0 [0x5c], DesiredAccess=0x4, ObjectAttributes="\Sessions\16\Windows\SharedSection") => 0

NtCreateSection(SectionHandle=0xbc284fe7d0 [0x4c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER[0x1f],
ObjectAttributes=null, SectionSize=0xbc284fe7c0 [65536], Protect=4, Attributes=0x08000000,
FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ffb5545cc48 [0x60], PortName="\Sessions\16\Windows\ApiPort",
SecurityQos=0xbc284fe8f0, ClientView=0xbc284fe7e8, ServerView=0xbc284fe818,
MaxMsgLength=0xbc284fe7e0 [0x3b8], ConnectionInfo=0xbc284fe860,
ConnectionInfoLength=0xbc284fe7b8 [0x30]) => 0

NtClose(Handle=0x4c) => 0

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0xbc284fe7c8
[0x00007ff4f7d60000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xbc284fe7d8
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x5c) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effb70000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0xbc284fe4a0, Length=0x30, ReturnLength=null) =>
0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe1b0 [0x0000025effbf4000],
ZeroBits=0, pSize=0xbc284fe258 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtInitializeNlsFiles(BaseAddress=0xbc284fe990 [0x0000025effcf0000],
DefaultLocaleId=0x7ffb52c508e0 [0x419], DefaultCasingTableSize=null) => 0

NtCreateFile(FileHandle=0xbc284fe9f8 [0x64],
DesiredAccess=READ_CONTROL|SYNCHRONIZE[0x19f], ObjectAttributes=4:"\Connect",
IoStatusBlock=0xbc284fe3b0 [0/0x18], AllocationSize=null, FileAttributes=0, ShareAccess=7,
CreateDisposition=2, CreateOptions=0x20, EaBuffer=0x25effbf4800, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x64, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xbc284fe940 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0xbc284fe960, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0xbc284fe968, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x64, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xbc284fe730, IoControlCode=0x00500016, InputBuffer=0xbc284fe740,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '==x
эрщфхэю єрчрээюх шь ёшёСхьэюю ёхьрїюЁр.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xbc284fe858, InputBufferLength=0xa0,
OutputBuffer=0xbc284fe858, OutputBufferLength=0xa0, ReturnLength=0xbc284fe850 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xbc284fe898, InputBufferLength=0x18,
OutputBuffer=0xbc284fe8b0, OutputBufferLength=0x78, ReturnLength=0xbc284fe890 [0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xbc284fe890 [0x4c]) =>
0

NtQueryInformationToken(TokenHandle=0x4c, TokenInformationClass=0xc [TokenSessionId], TokenInformation=0xbc284fe1b0, Length=4, ReturnLength=0xbc284fe190 [4]) => 0

NtQueryInformationToken(TokenHandle=0x4c, TokenInformationClass=0x1d [TokenIsAppContainer], TokenInformation=0xbc284fe1f8, Length=4, ReturnLength=0xbc284fe190 [4]) => 0

NtQueryInformationToken(TokenHandle=0x4c, TokenInformationClass=0x2a [TokenPrivateNameSpace], TokenInformation=0xbc284fe194, Length=4, ReturnLength=0xbc284fe190 [4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0xbc284fe1b8 [0x68], DesiredAccess=0xf, ObjectAttributes="\Sessions\16\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x4c, TokenInformationClass=0x2c [TokenBnoIsolation], TokenInformation=0xbc284fe4b0, Length=0x120, ReturnLength=0xbc284fe190 [0x10]) => 0

NtClose(Handle=0x4c) => 0

NtCreateMutant(MutantHandle=0xbc284fe8e8 [0x4c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1, ObjectAttributes=0x68:"Local\SM0:44704:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x4c, Alertable=false, Timeout=null) => 0

NtOpenSemaphore(SemaphoreHandle=0xbc284fe6d8, DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x68:"Local\SM0:44704:304:WilStaging_02_p0") => 0xc0000034 [2 '==x
ефрхСё эрщСш єърчрээ√щ Ърщы.']

NtCreateSemaphore(SemaphoreHandle=0xbc284fe5c8 [0x6c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x68:"Local\SM0:44704:304:WilStaging_02_p0", InitialCount=0x3fe24c, MaxCount=0x3fe24c) => 0

NtCreateSemaphore(SemaphoreHandle=0xbc284fe5c8 [0x70], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x68:"Local\SM0:44704:304:WilStaging_02_p0h", InitialCount=0x12f, MaxCount=0x12f) => 0

NtReleaseMutant(MutantHandle=0x4c, PreviousCount=null) => 0

NtQueryWnfStateData(StateName=0xbc284fe940 [0xa3bc0875], TypeId=0xbc284fe9e8, ExplicitScope=null, ChangeStamp=0xbc284fe934 [8], Buffer=0xbc284fd930, BufferSize=0xbc284fe930 [8]) => 0

NtCreateEvent(EventHandle=0xbc284fe8a0 [0x74], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe060 [0x0000025effbf5000], ZeroBits=0, pSize=0xbc284fe108 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x25effbf4fd0 [0x78], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x74) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x78, IoCompletionHandle=0x18, TargetObjectHandle=0x74, KeyContext=0x25effbf4fe8, ApcContext=0x25effbf4e60, IoStatus=0x0000025e00000000, IoStatusInformation=0, AlreadySignaled=0xbc284fe820 [0xffbf0b00]) => 0

NtSubscribeWnfStateChange(StateName=0x25effbf5160 [0xa3bc0875], ChangeStamp=8, EventMask=0x11, SubscriptionId=0xbc284fe910 [0x000343dc]) => 0

NtQueryWnfStateData(StateName=0xbc284fea80 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xbc284fea78 [0], Buffer=null, BufferSize=0xbc284fea7c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x25effbf5490 [0xa3bc7c75], ChangeStamp=0, EventMask=0x11, SubscriptionId=0xbc284fe8f0 [0x000343dd]) => 0

NtQueryWnfStateData(StateName=0xbc284fea80 [0xa3bc88f5], TypeId=null, ExplicitScope=null, ChangeStamp=0xbc284fea78 [0], Buffer=null, BufferSize=0xbc284fea7c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x25effbf5640 [0xa3bc88f5], ChangeStamp=0, EventMask=0x11, SubscriptionId=0xbc284fe8f0 [0x000343de]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3 [SystemFeatureConfigurationSectionInformation], QueryType=0xbc284fe830 [0], Alignment=0x18, SystemInformation=0xbc284fe850, Length=0x50, ReturnLength=null) => 0

NtMapViewOfSection(SectionHandle=0x7c, ProcessHandle=-1, BaseAddress=0xbc284fe800 [0x0000025effb80000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xbc284fe808 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x80, ProcessHandle=-1, BaseAddress=0xbc284fe800 [0x0000025effbe0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xbc284fe808 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x84, ProcessHandle=-1, BaseAddress=0xbc284fe800 [0x0000025effdc0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xbc284fe808 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0x7c) => 0

NtClose(Handle=0x80) => 0

NtClose(Handle=0x84) => 0

NtQueryWnfStateData(StateName=0xbc284fe838 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xbc284fe8c8 [0], Buffer=0xbc284fe920, BufferSize=0xbc284fe820 [0]) => 0

NtSetTimer2(TimerHandle=0x28, DueTime=0xbc284fe8b0 [-3e+09], Period=null, Parameters=0xbc284fe8b8) => 0

NtOpenKey(KeyHandle=0xbc284fea80, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys") => 0xc0000034 [2 'x еррхЄё эрщЄш єърчрээ√щ їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xbc284fea98, InputBufferLength=0xa0, OutputBuffer=0xbc284fea98, OutputBufferLength=0xa0, ReturnLength=0xbc284fea90 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xbc284fead8, InputBufferLength=0x18, OutputBuffer=0xbc284feaf0, OutputBufferLength=0x78, ReturnLength=0xbc284fead0 [0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe3b0 [0x0000025effbf6000], ZeroBits=0, pSize=0xbc284fe458 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xbc284feac8, InputBufferLength=0xa0, OutputBuffer=0xbc284feac8, OutputBufferLength=0xa0, ReturnLength=0xbc284feac0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xbc284feb08, InputBufferLength=0x18, OutputBuffer=0xbc284feb20, OutputBufferLength=0x78, ReturnLength=0xbc284feb00 [0]) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xbc284fedd0, VmInformation=0xbc284feea8, VmInformationLength=4) => 0xc00000bb [50 'пррющ чряЁюё эх яюфхЁцштрхЁ .']

NtOpenKey(KeyHandle=0xbc284fe9b0, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") => 0xc0000034 [2 'х ефрхЁ эршЁш ёърчрээ\ш їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xbc284fe8b8, InputBufferLength=0xa0, OutputBuffer=0xbc284fe8b8, OutputBufferLength=0xa0, ReturnLength=0xbc284fe8b0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xbc284fe8f8, InputBufferLength=0x18, OutputBuffer=0xbc284fe910, OutputBufferLength=0x78, ReturnLength=0xbc284fe8f0 [0]) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x7ffb55297aa0, Length=0x40, ReturnLength=null) => 0

NtSetEvent(EventHandle=0x44, PrevState=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=4, OldProtect=0xbc284feaf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284feae8 [0x00007ffb52c63000], Size=0xbc284feae0 [0x1000], NewProtect=2, OldProtect=0xbc284feaf8 [4]) => 0

NtOpenKey(KeyHandle=0xbc284ff0d0, DesiredAccess=0x3, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") => 0xc0000034 [2 'x ефрхЄē эрщЄш єърчрээ\щ їрщы.']

NtOpenKey(KeyHandle=0xbc284ff0b0, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0xc0000034 [2 'x ефрхЄē эрщЄш єърчрээ\щ їрщы.']

NtOpenKey(KeyHandle=0xbc284ff0a8 [0x7c], DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0

NtQueryValueKey(KeyHandle=0x7c, ValueName="TransparentEnabled",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xbc284ff160,
Length=0x50, ResultLength=0xbc284ff0a0) => 0xc0000034 [2 '==x ефрхЄё эрщЄш єърчрээ\щ
Їрщы.']

NtClose(Handle=0x7c) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xbc284feff0, Length=0x58, ReturnLength=0xbc284fefe8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xbc284ff0a8, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-
1-5-21-279210374-529612743-1025975986-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '==x
ефрхЄё эрщЄш єърчрээ\щ Їрщы.']

NtOpenKey(KeyHandle=0xbc284ff190 [0x7c], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x7c, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xbc284ff1d0, Length=0x14,
ResultLength=0xbc284ff198 [0x10]) => 0

NtClose(Handle=0x7c) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour],
ProcessInformation=0xbc284ff170, Length=4) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xbc284ff0f0 [1], Alignment=4,
SystemInformation=0x25effbf3160, Length=0x50, ReturnLength=0xbc284ff0e8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x25effbf6230 [0x7c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=5) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x25effbf6228 [0x8c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff,
ObjectAttributes=null, CompletionPortHandle=0x7c, WorkerProcessHandle=-1,
StartRoutine=0x7ffb5533d110, StartParameter=0x25effbf61f0, MaxThreadCount=0x200,
StackReserve=0x00100000, StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0xbc284ff1b8, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x25effbf6280 [0x90], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x25effbf6288 [0x94],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x94, IoCompletionHandle=0x7c,
TargetObjectHandle=0x90, KeyContext=0x25effbf6290, ApcContext=0x25effbf6260, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0xbc284ff0b0 [0]) => 0

NtCreateTimer2(TimerHandle=0x25effbf62f8 [0x98], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x25e00000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x25effbf6300 [0x9c], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x9c, IoCompletionHandle=0x7c, TargetObjectHandle=0x98, KeyContext=0x25effbf6308, ApcContext=0x25effbf6260, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0xbc284ff0b0 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=2 [WorkerFactoryIdleTimeout], Buffer=0xbc284ff1b8, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0xbc284ff1b8, BufferLength=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff1c0 [0x00007ff6c36d3000], Size=0xbc284ff1c8 [0x1000], NewProtect=4, OldProtect=0xbc284ff558 [2]) => 0

NtOpenSection(SectionHandle=0xbc284fec58, DesiredAccess=0xd, ObjectAttributes=0x3c:"VCRUNTIME140D.dll") => 0xc0000034 [2 'x ефрхЄё эрщЄш єърчрээ√щ Ърщы.']

NtOpenSection(SectionHandle=0xbc284fec58, DesiredAccess=0xd, ObjectAttributes=0x3c:"ucrtbased.dll") => 0xc0000034 [2 'x ефрхЄё эрщЄш єърчрээ√щ Ърщы.']

NtQueryWnfStateData(StateName=0xbc284fea50 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xbc284feae8 [0], Buffer=0xbc284feb40, BufferSize=0xbc284fea40 [0]) => 0

NtQueryWnfStateData(StateName=0xbc284fe8f0 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xbc284fe988 [0], Buffer=0xbc284fe9e0, BufferSize=0xbc284fe8e0 [0]) => 0

NtOpenKey(KeyHandle=0xbc284fecc0 [0xa0], DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xa0, ValueName="SafeDllSearchMode", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xbc284fecd0, Length=0x10, ResultLength=0xbc284fecc8) => 0xc0000034 [2 'x ефрхЄё эрщЄш єърчрээ√щ Ърщы.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe4a0 [0x0000025effbf7000], ZeroBits=0, pSize=0xbc284fe548 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\64\Debug\VCRUNTIME140D.dll", Attributes=0xbc284fed68) => 0xc0000034 [2 'x ефрхЄё эрщЄш єърчрээ√щ Ърщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\VCRUNTIME140D.dll", Attributes=0xbc284fed68 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0xbc284fee70 [0xa4], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\VCRUNTIME140D.dll", IoStatusBlock=0xbc284feed8 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xbc284fee78 [0xa8], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xa4) => 0

Loaded DLL at 00007FFB41E70000 C:\Windows\SYSTEM32\VCRUNTIME140D.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x25effbf6430 [0x00007ffb41e70000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x25effbf3700 [0x0002b000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xbc284fed10 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed20 [0x00007ffb55471000], Size=0xbc284fed18 [0x4000], NewProtect=4, OldProtect=0xbc284fed10 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed20 [0x00007ffb55471000], Size=0xbc284fed18 [0x4000], NewProtect=2, OldProtect=0xbc284fed10 [4]) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xbc284fe7f0, Length=0x330, ReturnLength=0xbc284fe7a8) => 0xc0000225 [1168 ' БХБХЭЭ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xbc284fe7f0, Length=0x330, ReturnLength=0xbc284fe7a8) => 0xc0000225 [1168 ' БХБХЭЭ эх эрщфхэ.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed70 [0x00007ffb41e90000], Size=0xbc284fed78 [0x1000], NewProtect=4, OldProtect=0x25effbf36e8 [2]) => 0

NtOpenSection(SectionHandle=0xbc284fe808, DesiredAccess=0xd, ObjectAttributes=0x3c:"ucrtbased.dll") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Ёрщы.']

NtClose(Handle=0xa8) => 0

NtClose(Handle=0xa4) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\64\Debug\ucrtbased.dll", Attributes=0xbc284fed68) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Ёрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", Attributes=0xbc284fed68 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0xbc284fee70 [0xa4], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", IoStatusBlock=0xbc284feed8 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xbc284fee78 [0xa8], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xa4) => 0

Loaded DLL at 00007FFAB47B0000 C:\Windows\SYSTEM32\ucrtbased.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x25effbf6690 [0x00007ffab47b0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x25effbf65f0 [0x00221000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xbc284fed10 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed20 [0x00007ffb55471000], Size=0xbc284fed18 [0x4000], NewProtect=4, OldProtect=0xbc284fed10 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed20 [0x00007ffb55471000], Size=0xbc284fed18 [0x4000], NewProtect=2, OldProtect=0xbc284fed10 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed70 [0x00007ffab495b000], Size=0xbc284fed78 [0x1000], NewProtect=4, OldProtect=0x25effbf65d8 [2]) => 0

NtClose(Handle=0xa8) => 0

NtClose(Handle=0xa4) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab1.1\64\Debug\ucrtbased.dll", Attributes=0xbc284fed68) => 0xc0000034 [2 'x ефрхЄё эрщЄш єърчрээ√щ їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", Attributes=0xbc284fed68 [ARCHIVE]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff538 [0x00007ff6c36d3000], Size=0xbc284ff540 [0x1000], NewProtect=2, OldProtect=0xbc284ff090 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effbf65b8 [0x00007ffab495b000], Size=0x25effbf65c0 [0x1000], NewProtect=2, OldProtect=0xbc284ff090 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effbf36c8 [0x00007ffb41e90000], Size=0x25effbf36d0 [0x1000], NewProtect=2, OldProtect=0xbc284ff090 [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=0xbc284ff3f8, VmInformation=0xbc284ff320, VmInformationLength=4) => 0xc00000bb [50 'ппрьющ чряЁюё эх ююфхЁцштрхЄё .']

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11 [ThreadHideFromDebugger], ThreadInformation=0xbc284ff230, Length=1, ReturnLength=null) => 0

Initial breakpoint

NtSetEvent(EventHandle=0x44, PrevState=null) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xbc284ff0b0, VmInformation=0xbc284ff188, VmInformationLength=4) => 0xc00000bb [50 'ппрьющ чряЁюё эх ююфхЁцштрхЄё .']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe480 [0x0000025effbf8000], ZeroBits=0, pSize=0xbc284fe528 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x50, IoStatusBlock=0xbc284fedd0 [0/8], FsInformation=0xbc284fedf0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xbc284fedd0 [0/8],
FsInformation=0xbc284fedf0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0xbc284fedd0 [0/8],
FsInformation=0xbc284fedf0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtOpenKey(KeyHandle=0xbc284fd8b0 [0xac], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions") => 0

NtQueryValueKey(KeyHandle=0xac, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xbc284fdda0, Length=0x214,
ResultLength=0xbc284fdd48 [0x2a]) => 0

NtQueryValueKey(KeyHandle=0xac, ValueName="000603xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xbc284fdd80, Length=0x214,
ResultLength=0xbc284fdb28 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe4e0 [0x0000025effbfa000],
ZeroBits=0, pSize=0xbc284fe588 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe4c0 [0x0000025effbfc000],
ZeroBits=0, pSize=0xbc284fe568 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xbc284ff0f0, VmInformation=0xbc284ff1c8, VmInformationLength=4) =>
0xc00000bb [50 'пррющ чряЁюё эх яюфхЁцштрхЄё .']

NtSetEvent(EventHandle=0x44, PrevState=null) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x8c, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0xbc284ff558, BufferLength=4) => 0

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

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6c36c1122,
MemoryInformationClass=0 [MemoryBasicInformation], MemoryInformation=0xbc284ff770,
Length=0x30, ReturnLength=0xbc284ff720 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6c36c1122,
MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xbc284ff7a0,
Length=0x30, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6c36c1122,
MemoryInformationClass=2 [MemoryMappedFilenameInformation],
MemoryInformation=0xbc284ff818, Length=0x21a, ReturnLength=null) => 0

Incorrect num argsNtDeviceIoControlFile(FileHandle=0x54, Event=0, ApcRoutine=null,
ApcContext=null, IoStatusBlock=0xbc284fe150 [0/0x12], IoControlCode=0x00500016,
InputBuffer=0xbc284fe160, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour],
ProcessInformation=0xbc284ff390, Length=4) => 0

NtOpenSection(SectionHandle=0xbc284ff368, DesiredAccess=0xd,
ObjectAttributes=0x3c:"kernel.appcore.dll") => 0xc0000034 [2 '≡x εφρxЄё эрщЄш єърчрээ√щ
Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\kernel.appcore.dll",
Attributes=0xbc284ff128 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0xbc284ff120 [0xa4], DesiredAccess=SYNCHRONIZE|0x21,
ObjectAttributes="\??\C:\Windows\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0xbc284ff188 [0/1],
ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xbc284ff128 [0xa8], DesiredAccess=0xd, ObjectAttributes=null,
SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xa4) => 0

Loaded DLL at 00007FFB506F0000 C:\Windows\SYSTEM32\kernel.appcore.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x25effbfab10
[0x00007ffb506f0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x25effbf6c40
[0x00012000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xbc284fec0 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed8 [0x00007ffb506ff000],
Size=0xbc284fed0 [0x1000], NewProtect=2, OldProtect=0xbc284ff040 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed0 [0x00007ffb55471000],
Size=0xbc284fec8 [0x4000], NewProtect=4, OldProtect=0xbc284fec0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fed0 [0x00007ffb55471000],
Size=0xbc284fec8 [0x4000], NewProtect=2, OldProtect=0xbc284fec0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284ff020 [0x00007ffb506f5000],
Size=0xbc284ff028 [0x1000], NewProtect=4, OldProtect=0x25effbf6c28 [2]) => 0

NtOpenSection(SectionHandle=0xbc284feab8 [0xb0], DesiredAccess=0xd,
ObjectAttributes=0x3c:"msvcrt.dll") => 0

Loaded DLL at 00007FFB53CC0000 C:\Windows\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x25effbfc9a0
[0x00007ffb53cc0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x25effbfc900
[0x0009e000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xbc284fe930 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe940 [0x00007ffb55471000],
Size=0xbc284fe938 [0x4000], NewProtect=4, OldProtect=0xbc284fe930 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe940 [0x00007ffb55471000],
Size=0xbc284fe938 [0x4000], NewProtect=2, OldProtect=0xbc284fe930 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe990 [0x00007ffb53d36000],
Size=0xbc284fe998 [0x2000], NewProtect=4, OldProtect=0x25effbfc8e8 [2]) => 0

NtClose(Handle=0xb0) => 0

NtOpenSection(SectionHandle=0xbc284feab8 [0xb4], DesiredAccess=0xd,
ObjectAttributes=0x3c:"RPCRT4.dll") => 0

Loaded DLL at 00007FFB546E0000 C:\Windows\System32\RPCRT4.dll

NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x25effbfccf0
[0x00007ffb546e0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x25effbfcc50
[0x00123000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xbc284fe930 [1.10575e+13], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe948 [0x00007ffb547fb000],
Size=0xbc284fe940 [0x1000], NewProtect=2, OldProtect=0xbc284fe9b0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe940 [0x00007ffb55471000],
Size=0xbc284fe938 [0x4000], NewProtect=4, OldProtect=0xbc284fe930 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe940 [0x00007ffb55471000],
Size=0xbc284fe938 [0x4000], NewProtect=2, OldProtect=0xbc284fe930 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xbc284fe990 [0x00007ffb547cc000],
Size=0xbc284fe998 [0x2000], NewProtect=4, OldProtect=0x25effbfcc38 [2]) => 0

NtClose(Handle=0xb4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effbf6c08 [0x00007ffb506f5000],
Size=0x25effbf6c10 [0x1000], NewProtect=2, OldProtect=0xbc284fef10 [4]) => 0

NtClose(Handle=0xa8) => 0

NtClose(Handle=0xa4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effbf6c8 [0x00007ffb53d36000],
Size=0x25effbf6cd0 [0x2000], NewProtect=2, OldProtect=0xbc284ff230 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation],
ProcessInformation=0xbc284ff190, Length=0x28) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x25effbfcc18 [0x00007ffb547cc000],
Size=0x25effbfcc20 [0x2000], NewProtect=2, OldProtect=0xbc284ff230 [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=0xbc284ff250, VmInformation=0xbc284ff328, VmInformationLength=4) =>
0xc00000bb [50 'пррющ чряЁюё эх яюфхЁцштрхЄё .']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fea80 [0x0000025effdd0000],
ZeroBits=0, pSize=0xbc284fea88 [0x001b0000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fea80 [0x0000025effdd0000],
pSize=0xbc284fea78 [0x001a0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fea68 [0x0000025efff70000], ZeroBits=0, pSize=0xbc284fea60 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x50, IoStatusBlock=0xbc284ff050 [0/8], FsInformation=0xbc284ff070, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xbc284ff050 [0/8], FsInformation=0xbc284ff070, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0xbc284ff050 [0/8], FsInformation=0xbc284ff070, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe8f0 [0x0000025effbfe000], ZeroBits=0, pSize=0xbc284fe998 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe8c0 [0x0000025efff72000], ZeroBits=0, pSize=0xbc284fe968 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xbc284fe8a0 [0x0000025efff73000], ZeroBits=0, pSize=0xbc284fe948 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xbc284ff250, VmInformation=0xbc284ff328, VmInformationLength=4) => 0xc00000bb [50 'пръющ чряЁюё эх яюфхЁцштрхЄё .']

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xbc284ff290, VmInformation=0xbc284ff368, VmInformationLength=4) => 0xc00000bb [50 'пръющ чряЁюё эх яюфхЁцштрхЄё .']

NtSetEvent(EventHandle=0x44, PrevState=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xbc284ff4c0, Length=0x330, ReturnLength=0xbc284ff478) => 0xc0000225 [1168 'ЫХЪХЭЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xbc284ff4c0, Length=0x330, ReturnLength=0xbc284ff478) => 0xc0000225 [1168 'ЫХЪХЭЄ эх эрщфхэ.']

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

NtClose(Handle=0x88) => 0

NtClose(Handle=0x5c) => 0

NtClose(Handle=0x84) => 0

NtClose(Handle=0x80) => 0

NtQueryWnfStateData(StateName=0xbc284ff570 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xbc284fe4b4 [0x652e], Buffer=0xbc284fe510, BufferSize=0xbc284fe4b0 [0x55a]) => 0

NtQueryWnfStateData(StateName=0xbc284ff3f8 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xbc284ff488 [0], Buffer=0xbc284ff4e0, BufferSize=0xbc284ff3e0 [0]) => 0

Process 44704 exit code: 1

Вывод

В ходе выполнения лабораторной работы я переделал первое задание с использованием file mapping. Проблем при выполнении работы не возникло.