Московский Авиационный Институт

(Национальный Исследовательский Университет)

Институт №8 “Компьютерные науки и прикладная математика”

Кафедра №806 “Вычислительная математика и программирование”

Лабораторная работа №2 по курсу

«Операционные системы»

Группа: М8О-214Б-23

Студент: Кондратенко А.С.

Преподаватель: Бахарев В.Д. (ФИИТ)

Оценка: _____

Дата: 22.12.24

Москва, 2024

Постановка задачи

Вариант 14.

Составить программу на языке Си, обрабатывающую данные в многопоточном режиме. При обработки использовать стандартные средства создания потоков операционной системы (Windows/Unix). Ограничение максимального количества потоков, работающих в один момент времени, должно быть задано ключом запуска вашей программы. Так же необходимо уметь продемонстрировать количество потоков, используемое вашей программой с помощью стандартных средств операционной системы. В отчете привести исследование зависимости ускорения и эффективности алгоритма от входных данных и количества потоков. Получившиеся результаты необходимо объяснить.

Есть набор 128 битных чисел, записанных в шестнадцатеричном представлении, хранящихся в файле. Необходимо посчитать их среднее арифметическое. Округлить результат до целых. Количество используемой оперативной памяти должно задаваться "ключом".

Общий метод и алгоритм решения

Использованные системные вызовы:

- CreateFile – открывает файл
- ReadFile – читает данные из канала
- CloseHandle – закрывает дескриптор канала
- WriteFile – записывает данные в канал
- WriteConsoleA – записывает данные в консоль
- ReleaseSemaphore - закрывает один из потоков
- CreateThread - создать поток
- WaitForSingleObject - ожидание, пока поток закончит свою работу
- WaitForMultipleObjects - – ожидание, пока все потоки не закончат свою работу

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.

Затем началась работа над самим заданием непосредственно. Сначала я написал функцию для перевода числа в строковом представлении из заданной системы счисления в десятичную(to_dec) по схеме Горнера. Далее идут стандартные обработки ошибок на входные данные. На вход подается название файла с входными данными, объем оперативной памяти и количество потоков. Размер массива надо ограничить, тут понятно, просто int нужно обработать.

Но как определить предел количества потоков? Вообще потоков физически не может быть больше количества ядер процессора. Т.е. если процессор 4-х ядерный, он не может выполнять более 4-х потоков одновременно. Есть технология Hyper-threading суть которой - оптимизация "переключений" между процессами, т.е. Hyper-Threading 4-8 не означает что 8 выполняются одновременно, а означает что переключение между потоками организовано таким образом, что создаётся впечатление что ядер больше. Логически (уровень ОС) - пока не закончится память хэндлов (т.е. много). Тогда вопрос сводится к максимальному количеству хэндлов (т.к. каждому

thread нужно присвоить хэндл), ответ - до 10000 (минус штук 300 используется системой). Активные хэндлы ОС "преобразует" в таски, а процессор аппаратным решением выбирает какой таск выполнять сейчас на аппаратном уровне. Хэндлами могут быть - файлы, pipes, event, mailslot и другие обьекты ОС, если программа активно использует хэндлы (например, для каждого thread открывается f то хэндлы закончатся в два раза быстрее, т.к. общее число хэндлов не должно превышать 10000. Активный Thread всегда подкреплен Thread Handle ОС, но неактивные можно создавать - пока не закончится память Heap. При превышении определённого числа активных Thread - получим ошибку, что невозможно создать хэндл. Апаратный уровнь. TSS или Task Gate Descriptor. Для 32 битных процессоров, существует каталог GDT - таблица таблиц на 8192 ячеек. В каждой можно сохранить ссылку на 8192 LDT элементов, один из которых может быть дескриптором процесса Task-и (частью Thread без которой процессор не сможет аппаратно переключать Thread. Т.е. 67 108 864 – это "теоретически" предел аппаратных мест для потоков, но нужно учесть, что дескрипторы памяти так же нужно разместить в этой таблице, т.е. минус дескрипторы памяти... выйдет от миллиона до 60 миллионов. Но в реальности, есть предел, выше которого процессор будет "ничем другим не занят кроме как переключением процессов", поэтому столько не используют. Процессор распределяет эти таски между ядрами аппаратным решением. Что ОС будет делать когда они закончатся - скорее всего у ОС встроен константой предел на количество тасков, так как при слишком большом их количестве процессор начнёт терять производительность.

Теперь суть задания. Нужно посчитать количество кусков массива, которые будут отправляться в потоки (просто разделить количество чисел на количество потоков). Создаем семафор на запрошенное количество потоков. Затем читаем данные из файла в буфер, с помощью функции strtok делим его по символам переноса строки и каждую лексему преобразуем в число типа unsigned long long int. Далее создаем массив потоков заданного размера и заполняем его, пока семафор позволяет. Ждем, пока семафор даст отмашку об освободившемся потоке и дальше запускаем следующий поток (в каждом потоке изменяются глобальные сумма и количество чисел). В конце вычисляется среднее арифметическое чисел из файла (сумма чисел делится на их количество, результат с помощью функции llround округляется до ближайшего целого).

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>
#include <stdlib.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 'l': {
    unsigned long long value = va_arg(args, unsigned long long);
    char num_buffer[40];
    char* num_ptr = num_buffer;
    do {
        *num_ptr++ = (char)((value % 10) + '0');
        value /= 10;
    } while (value > 0);
    while (num_ptr > num_buffer) {
        *buf_ptr++ = *--num_ptr;
    }
    break;
}
```

```
case 'k': {
    double value = va_arg(args, double);
    char num_buffer[20];
    char* num_ptr = num_buffer;
    if (value < 0) {
        *buf_ptr++ = '-';
        value = -value;
    }

    int afterDot = (value - (int)value) * 100000000;
    int beforeDot = (int)value;

    do {
        *num_ptr++ = (char)((afterDot % 10) + '0');
        afterDot /= 10;
    } while (afterDot > 0);

    *num_ptr++ = '.';

    do {
        *num_ptr++ = (char)((beforeDot % 10) + '0');
        beforeDot /= 10;
    } while (beforeDot > 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 'k': {
    double value = va_arg(args, double);
    char num_buffer[20];
    char* num_ptr = num_buffer;
    if (value < 0) {
        *buf_ptr++ = '-';
        value = -value;
    }

    int afterDot = (value - (int)value) * 100000000;
    int beforeDot = (int)value;

    do {
```

```
            *num_ptr++ = (char)((afterDot % 10) + '0');
            afterDot /= 10;
        } while (afterDot > 0);

        *num_ptr++ = '.';

        do {
            *num_ptr++ = (char)((beforeDot % 10) + '0');
            beforeDot /= 10;
        } while (beforeDot > 0);

        while (num_ptr > num_buffer) {
            *buf_ptr++ = *--num_ptr;
        }
        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;
}
```

lab2.cpp

```
#define _CRT_SECURE_NO_WARNINGS
#define BUF_SIZE 1000
#define MAX_THREADS 100000
#include "my_stdio.h"
#include <math.h>
#include <time.h>

enum ret_type {
    SUCCESS,
    FILE_OPENING_ERROR,
    ERROR_MALLOC,
    ERROR_ARGS_COUNT,
    ERR_SEM,
    ERR_THREAD
};

unsigned long long to_dec(const char* num, int base){
    unsigned long long res = 0, i = 0;
    while (num[i]) {
        res = res * base + (num[i] <= '9' ? num[i] - '0' : num[i] - 'A' + 10);
        i++;
```

```
    }
    return res;
}

unsigned long long sum = 0, cnt = 0;
HANDLE semaphore;

typedef struct {
    const unsigned long long* numbers;
    unsigned long long count;
} ThreadData;

DWORD WINAPI sum_array_part(LPVOID lpParam) {
    ThreadData* data = (ThreadData*)lpParam;
    unsigned long long local_sum = 0;

    for (unsigned long long i = 0; i < data->count; ++i) {
        //my_printf("%l\n", data->numbers[i]);
        local_sum += data->numbers[i];
    }

    WaitForSingleObject(semaphore, INFINITE);
    sum += local_sum;
    cnt += data->count;
    ReleaseSemaphore(semaphore, 1, NULL);

    return 0;
}
```

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

    HANDLE hFile = CreateFile(ConvertToWideString(argv[1]), GENERIC_READ, 0, NULL,
OPEN_EXISTING, 0, NULL);
    if (hFile == INVALID_HANDLE_VALUE) {
        my_printf("Failed to open file");
        return FILE_OPENING_ERROR;
    }

    char buffer[BUF_SIZE];
    DWORD bytesRead;
    ReadFile(hFile, buffer, BUF_SIZE, &bytesRead, NULL);
    buffer[bytesRead] = '\0';
    CloseHandle(hFile);

    unsigned long long cnt_nums = to_dec(argv[2], 10) / sizeof(unsigned long long);
    unsigned long long* nums = (unsigned long long*)malloc(sizeof(unsigned long long) *
cnt_nums);
    if (!nums)
        return ERROR_MALLOC;

    int NUM_THREADS = to_dec(argv[3], 10);
    if (!NUM_THREADS) {
        my_printf("No threads error\n");
        return ERR_THREAD;
    }

    if (NUM_THREADS > MAX_THREADS || NUM_THREADS > cnt_nums) {
        my_printf("\nMax threads limit exceeded. Setting to %d\n\n", cnt_nums);
        NUM_THREADS = cnt_nums;
```

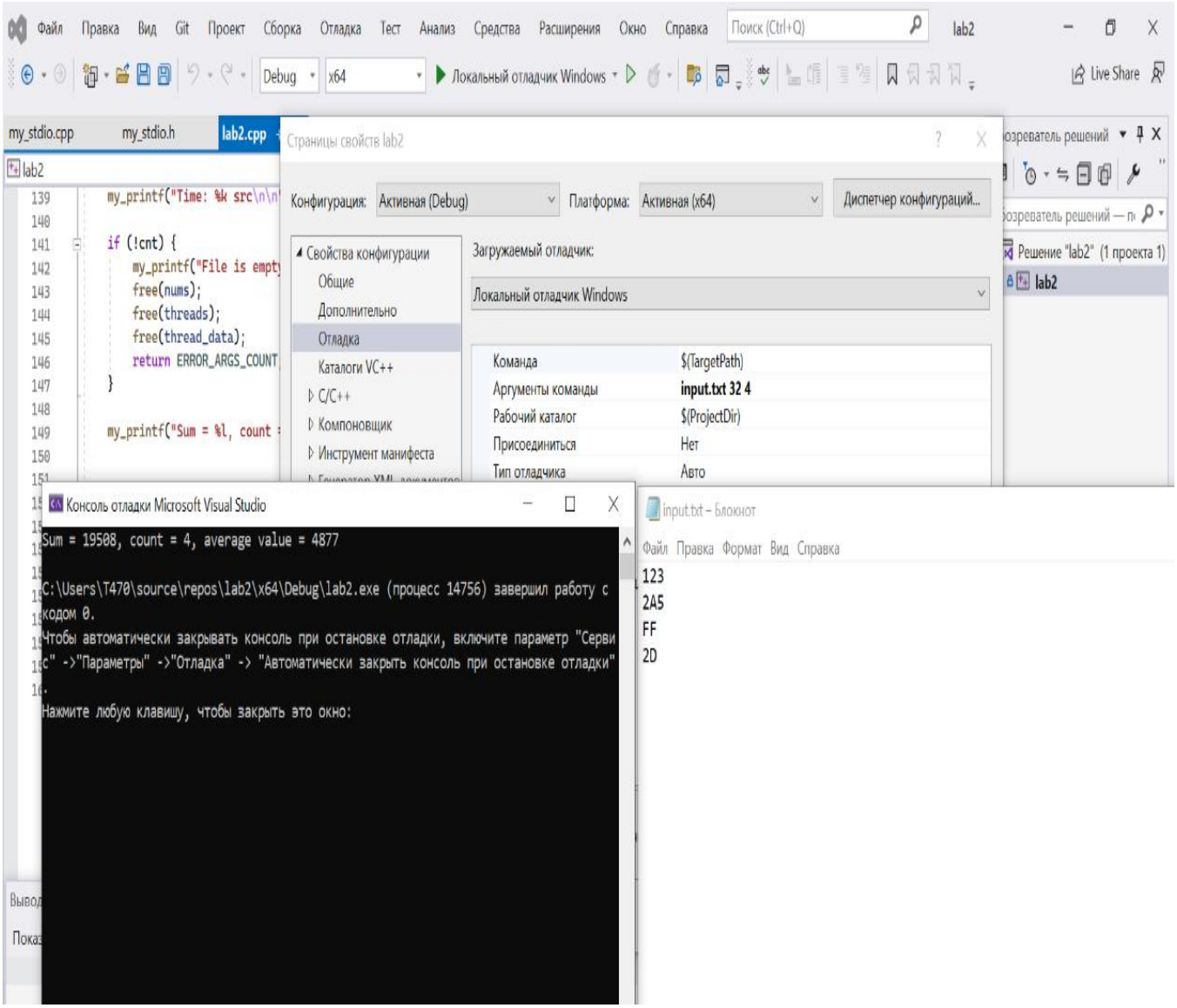
```
}

semaphore = CreateSemaphore(NULL, NUM_THREADS, NUM_THREADS, NULL);
if (!semaphore) {
    free(nums);
    my_printf("Create semaphore error occured\n");
    return ERR_SEM;
}

char* pch = strtok(buffer, "\n");
unsigned long long i = 0;
while (pch) {
    nums[i] = to_dec(pch, 16);
    pch = strtok(NULL, "\n");
    i++;
}

HANDLE* threads = (HANDLE*)malloc(NUM_THREADS * sizeof(HANDLE));
if (!threads) {
    free(nums);
    return ERROR_MALLOC;
}
ThreadData* thread_data = (ThreadData*)malloc(NUM_THREADS * sizeof(ThreadData));
if (!thread_data) {
    free(nums);
    free(threads);
    return ERROR_MALLOC;
}

unsigned long long size_thread = cnt_nums / NUM_THREADS;
```

```
    //my_printf("cnt = %l, nt = %l, st = %l\n", cnt_nums, NUM_THREADS, size_thread);
    clock_t start = clock();

    for (i = 0; i < NUM_THREADS; i++) {
        thread_data[i].numbers = &(nums[i * size_thread]);
        thread_data[i].count = (i * (size_thread + 1) <= cnt_nums && i < NUM_THREADS - 1) ? size_thread : cnt_nums - i * size_thread;
        //my_printf("ind = %l, count = %l\n", i, thread_data[i].count);
        threads[i] = CreateThread(NULL, 0, sum_array_part, (LPVOID)&thread_data[i], 0, NULL);
        if (!threads[i]) {
            free(nums);
            free(threads);
            free(thread_data);
            my_printf("Create thread error occured\n");
            return ERR_THREAD;
        }
    }

    WaitForMultipleObjects(NUM_THREADS, threads, TRUE, INFINITE);

    clock_t end = clock();
    double seconds = (double)(end - start) / CLOCKS_PER_SEC;
    my_printf("Time: %k src\n\n", seconds);

    if (!cnt) {
        my_printf("%l %l\n", sum, cnt);
        my_printf("File is empty\n");
        free(nums);
        free(threads);
        free(thread_data);
```

```
        return ERROR_ARGS_COUNT;
    }

    my_printf("Sum = %l, count = %l, average value = %l\n", sum, cnt, llround(1. * sum / cnt));



    CloseHandle(semaphore);
    for (unsigned long long i = 0; i < NUM_THREADS; ++i)
        CloseHandle(threads[i]);

    free(nums);
    free(threads);
    free(thread_data);
    return 0;
}
```

Протокол работы программы

Тестирование:



NtTrace:

Process 9284 starting at 00007FF6F9BD12FD with command line: "lab2.exe"

C:\Users\T470\source\repos\lab2\x64\Debug\lab2.exe

Loaded DLL at 00007FF8E5470000 C:\Windows\SYSTEM32\ntdll.dll

NtQueryPerformanceCounter(Counter=0x5b9056f700 [8.92378e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f748 [0x00007ff8e55f4000], Size=0x5b9056f740 [0x1000], NewProtect=4, OldProtect=0x5b9056f780 [8]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f748 [0x00007ff8e55f4000], Size=0x5b9056f740 [0x1000], NewProtect=8, OldProtect=0x5b9056f780 [4]) => 0

NtCreateEvent(EventHandle=0x7ff8e55dc478 [8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x5b9056f6b0, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0x5b9056f3d8, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation], SystemInformation=0x5b9056f2b0, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff8e5470000, MemoryInformationClass=6 [MemoryImageInformation], MemoryInformation=0x5b9056f1c0, Length=0x18, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4 [MemoryWorkingSetExInformation], MemoryInformation=0x5b9056f280, Length=0x50, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f2d0 [0x00007ff8e55f1000], Size=0x5b9056f2c8 [0x4000], NewProtect=2, OldProtect=0x5b9056f2c0 [4]) => 0

NtOpenKey(KeyHandle=0x5b9056df10 [0xc], DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xc, ValueName="RaiseExceptionOnPossibleDeadlock", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9056df20, Length=0x50, ResultLength=0x5b9056df18) => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xc) => 0

NtOpenKey(KeyHandle=0x5b9056dea8 [0x10], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options") => 0

NtOpenKey(KeyHandle=0x5b9056df90, DesiredAccess=0x9, ObjectAttributes=0x10:"lab2.exe") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x5b9056def0, 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=0x7ff8e55dd230, Length=4, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0x5b9056f268, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0x5b9056eca0, Length=0x330, ReturnLength=0x5b9056ec58) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0x5b9056eca0, Length=0x330, ReturnLength=0x5b9056ec58) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtOpenKey(KeyHandle=0x5b9056f1e0 [0x14], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x14, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9056f220, Length=0x18, ResultLength=0x5b9056f1e8) => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x14) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0x5b9056f2c0, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x5b9056f260, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation], SystemInformation=0x5b9056f290, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff8e55ddc38 [0x00007ff52b9a0000], ZeroBits=0x0000005b9056f210, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0x5b9056f178, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff8e55ddc30 [0x00007ff52d9a0000], ZeroBits=0x0000005b9056f218, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null, DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff8e55ddca0 [0x00007ff42b980000], ZeroBits=0x0000005b9056f1c0, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0x5b9056f128, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x5b9056f100, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056ecc0 [0x00000166c14e0000], ZeroBits=0, pSize=0x5b9056ecc8 [0x001c0000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056ecc0 [0x00000166c14e0000], pSize=0x5b9056ecb8 [0x000c0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056eca8 [0x00000166c15a0000], ZeroBits=0, pSize=0x5b9056eca0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5 [SystemHypervisorSharedPageInformation], SystemInformation=0x5b9056f468, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap], SystemInformation=0x5b9056eed0, Length=0x408, ReturnLength=0x5b9056f2f0 [0x18]) => 0

NtCreateEvent(EventHandle=0x5b9056f108 [0x14], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x166c15a0b20 [0x18], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9056ee60 [1], Alignment=4, SystemInformation=0x166c15a0ed0, Length=0x50, ReturnLength=0x5b9056ee58 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x166c15a0c00 [0x1c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, NumberOfConcurrentThreads=5) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x166c15a0bf8 [0xc], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null, CompletionPortHandle=0x1c, WorkerProcessHandle=-1, StartRoutine=0x7ff8e54bd110, StartParameter=0x166c15a0bc0, MaxThreadCount=0x200, StackReserve=0x00100000, StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x166c15a0c50 [0x20], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x7ff800000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x166c15a0c58 [0x24], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x24, IoCompletionHandle=0x1c, TargetObjectHandle=0x20, KeyContext=0x166c15a0c60, ApcContext=0x166c15a0c30, IoStatus=0, IoStatusInformation=1, AlreadySignaled=0x5b9056ee20 [0]) => 0

NtCreateTimer2(TimerHandle=0x166c15a0cc8 [0x28], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x16600000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x166c15a0cd0 [0x2c], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x2c, IoCompletionHandle=0x1c, TargetObjectHandle=0x28, KeyContext=0x166c15a0cd8, ApcContext=0x166c15a0c30, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0x5b9056ee20 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xc, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0x5b9056ef28, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xc, InformationClass=0xe [WorkerFactoryThreadSoftMaximum], Buffer=0x5b9056ef28, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xc, InformationClass=3 [WorkerFactoryBindingCount], Buffer=0x5b9056f048, BufferLength=4) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x18, IoCompletionHandle=0x1c, TargetObjectHandle=0x14, KeyContext=0x166c15a0b38, ApcContext=0x166c15a09b0, IoStatus=0x0000016600000000, IoStatusInformation=0, AlreadySignaled=0x5b9056f090 [0xc15a0b00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0x5b9056f148, InputBufferLength=4, OutputBuffer=null, OutputBufferLength=0, ReturnLength=0x5b9056f100 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9056f1a8, InputBufferLength=0xa0, OutputBuffer=0x5b9056f1a8, OutputBufferLength=0xa0, ReturnLength=0x5b9056f1a0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9056f1a8, InputBufferLength=0xa0, OutputBuffer=0x5b9056f1a8, OutputBufferLength=0xa0, ReturnLength=0x5b9056f1a0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9056f1a8, InputBufferLength=0xa0, OutputBuffer=0x5b9056f1a8, OutputBufferLength=0xa0, ReturnLength=0x5b9056f1a0 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056eb10 [0x00000166c15a2000], ZeroBits=0, pSize=0x5b9056ebb8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056f2f0 [0x00000166c1470000], pSize=0x5b9056f2f8 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f2d0 [0x00007ff8e55f1000], Size=0x5b9056f2c8 [0x4000], NewProtect=4, OldProtect=0x5b9056f2c0 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ff8e55f1298 [0x3c], DesiredAccess=0x3, ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f2d0 [0x00007ff8e55f1000], Size=0x5b9056f2c8 [0x4000], NewProtect=2, OldProtect=0x5b9056f2c0 [4]) => 0

NtOpenSymbolicLinkObject(LinkHandle=0x5b9056f428 [0x40], DesiredAccess=0x1, ObjectAttributes=0x3c:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x40, LinkTarget="C:\Windows\System32", ReturnedLength=0x5b9056f3dc [0x28]) => 0

NtClose(Handle=0x40) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f2a0 [0x00007ff8e55f1000], Size=0x5b9056f298 [0x4000], NewProtect=4, OldProtect=0x5b9056f290 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f2d0 [0x00007ff8e55f1000], Size=0x5b9056f2c8 [0x4000], NewProtect=2, OldProtect=0x5b9056f2c0 [4]) => 0

NtCreateEvent(EventHandle=0x7ff8e55dc380 [0x40], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ff8e55dc3b0 [0x44], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtQueryPerformanceCounter(Counter=0x5b9056f220 [8.92381e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f230 [0x00007ff8e55f1000], Size=0x5b9056f228 [0x4000], NewProtect=4, OldProtect=0x5b9056f220 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f230 [0x00007ff8e55f1000], Size=0x5b9056f228 [0x4000], NewProtect=2, OldProtect=0x5b9056f220 [4]) => 0

NtOpenFile(FileHandle=0x5b9056f2d8 [0x48], DesiredAccess=SYNCHRONIZE|0x20, ObjectAttributes="\??\C:\Users\T470\source\repos\lab2\x64\Debug\", IoStatusBlock=0x5b9056f248 [0/1], ShareAccess=3, OpenOptions=0x21) => 0

NtQueryVolumeInformationFile(FileHandle=0x48, IoStatusBlock=0x5b9056f248 [0/8], FsInformation=0x5b9056f230, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

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

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0x5b9056ef90, Length=4) => 0

NtOpenSection(SectionHandle=0x5b9056ef68 [0x4c], DesiredAccess=0xd, ObjectAttributes=0x3c:"KERNEL32.DLL") => 0

Loaded DLL at 00007FF8E36A0000 C:\Windows\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x4c, ProcessHandle=-1, BaseAddress=0x166c15a3260 [0x00007ff8e36a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x166c15a31c0 [0x000c2000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x5b9056ede0 [8.92382e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056edf8 [0x00007ff8e375f000], Size=0x5b9056edf0 [0x1000], NewProtect=2, OldProtect=0x5b9056ee60 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056edf0 [0x00007ff8e55f1000], Size=0x5b9056ede8 [0x4000], NewProtect=4, OldProtect=0x5b9056ede0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056edf0 [0x00007ff8e55f1000], Size=0x5b9056ede8 [0x4000], NewProtect=2, OldProtect=0x5b9056ede0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ee40 [0x00007ff8e3723000], Size=0x5b9056ee48 [0x4000], NewProtect=4, OldProtect=0x166c15a31a8 [2]) => 0

NtOpenSection(SectionHandle=0x5b9056e8d8 [0x5c], DesiredAccess=0xd, ObjectAttributes=0x3c:"KERNELBASE.dll") => 0

Loaded DLL at 00007FF8E2F90000 C:\Windows\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x166c15a3940 [0x00007ff8e2f90000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x166c15a38a0 [0x002fe000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x5b9056e750 [8.92382e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056e768 [0x00007ff8e3263000], Size=0x5b9056e760 [0x1000], NewProtect=2, OldProtect=0x5b9056e7d0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056e760 [0x00007ff8e55f1000], Size=0x5b9056e758 [0x4000], NewProtect=4, OldProtect=0x5b9056e750 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056e760 [0x00007ff8e55f1000], Size=0x5b9056e758 [0x4000], NewProtect=2, OldProtect=0x5b9056e750 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056e7b0 [0x00007ff8e317a000], Size=0x5b9056e7b8 [0x3000], NewProtect=4, OldProtect=0x166c15a3888 [2]) => 0

NtClose(Handle=0x5c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c15a3188 [0x00007ff8e3723000], Size=0x166c15a3190 [0x4000], NewProtect=2, OldProtect=0x5b9056ed30 [4]) => 0

NtClose(Handle=0x4c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c15a3868 [0x00007ff8e317a000], Size=0x166c15a3870 [0x3000], NewProtect=2, OldProtect=0x5b9056ee30 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0x5b9056ed90, Length=0x28) => 0

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

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0x5b9056ee50, VmInformation=0x5b9056ef28, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation], SystemInformation=0x5b9056eab0, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x7ff8e324ee60, Length=0x40, ReturnLength=null) => 0

NtOpenSection(SectionHandle=0x5b9056e870 [0x5c], DesiredAccess=0x4, ObjectAttributes="\Sessions\2\Windows\SharedSection") => 0

NtCreateSection(SectionHandle=0x5b9056e890 [0x4c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null, SectionSize=0x5b9056e880 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ff8e55dcc48 [0x60], PortName="\Sessions\2\Windows\ApiPort", SecurityQos=0x5b9056e9b0, ClientView=0x5b9056e8a8, ServerView=0x5b9056e8d8, MaxMsgLength=0x5b9056e8a0 [0x3b8], ConnectionInfo=0x5b9056e920, ConnectionInfoLength=0x5b9056e878 [0x30]) => 0

NtClose(Handle=0x4c) => 0

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x5b9056e888 [0x00007ff42b880000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9056e898 [0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x5c) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c1470000, MemoryInformationClass=0 [MemoryBasicInformation], MemoryInformation=0x5b9056e560, Length=0x30, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e270 [0x00000166c15a4000], ZeroBits=0, pSize=0x5b9056e318 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtInitializeNlsFiles(BaseAddress=0x5b9056ea50 [0x00000166c16a0000], DefaultLocaleId=0x7ff8e3250900 [0x419], DefaultCasingTableSize=null) => 0

NtCreateFile(FileHandle=0x5b9056eab8 [0x5c], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f, ObjectAttributes=4:"\Connect", IoStatusBlock=0x5b9056e470 [0/0x18], AllocationSize=null, FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20, EaBuffer=0x166c15a47c0, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x5c, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x5b9056ea00 [0/0], IoControlCode=0x00500023, InputBuffer=null, InputBufferLength=0, OutputBuffer=0x5b9056ea20, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31 [ProcessOwnerInformation], ProcessInformation=0x5b9056ea28, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x5c, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x5b9056e7f0, IoControlCode=0x00500016, InputBuffer=0x5b9056e800, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '═х эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9056e918, InputBufferLength=0xa0, OutputBuffer=0x5b9056e918, OutputBufferLength=0xa0, ReturnLength=0x5b9056e910 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9056e958, InputBufferLength=0x18, OutputBuffer=0x5b9056e970, OutputBufferLength=0x78, ReturnLength=0x5b9056e950 [0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x5b9056e950 [0x64]) => 0

NtQueryInformationToken(TokenHandle=0x64, TokenInformationClass=0xc [TokenSessionId], TokenInformation=0x5b9056e270, Length=4, ReturnLength=0x5b9056e250 [4]) => 0

NtQueryInformationToken(TokenHandle=0x64, TokenInformationClass=0x1d [TokenIsAppContainer], TokenInformation=0x5b9056e2b8, Length=4, ReturnLength=0x5b9056e250 [4]) => 0

NtQueryInformationToken(TokenHandle=0x64, TokenInformationClass=0x2a [TokenPrivateNameSpace], TokenInformation=0x5b9056e254, Length=4, ReturnLength=0x5b9056e250 [4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x5b9056e278 [0x68], DesiredAccess=0xf, ObjectAttributes="\Sessions\2\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x64, TokenInformationClass=0x2c [TokenBnoIsolation], TokenInformation=0x5b9056e570, Length=0x120, ReturnLength=0x5b9056e250 [0x10]) => 0

NtClose(Handle=0x64) => 0

NtCreateMutant(MutantHandle=0x5b9056e9a8 [0x64], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1, ObjectAttributes=0x68:"Local\SM0:9284:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x64, Alertable=false, Timeout=null) => 0

NtOpenSemaphore(SemaphoreHandle=0x5b9056e798, DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x68:"Local\SM0:9284:304:WilStaging_02_p0") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtCreateSemaphore(SemaphoreHandle=0x5b9056e688 [0x6c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x68:"Local\SM0:9284:304:WilStaging_02_p0", InitialCount=0x3056923c, MaxCount=0x3056923c) => 0

NtCreateSemaphore(SemaphoreHandle=0x5b9056e688 [0x70], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=0x68:"Local\SM0:9284:304:WilStaging_02_p0h", InitialCount=0xb3, MaxCount=0xb3) => 0

NtReleaseMutant(MutantHandle=0x64, PreviousCount=null) => 0

NtQueryWnfStateData(StateName=0x5b9056ea00 [0xa3bc0875], TypeId=0x5b9056eaa8, ExplicitScope=null, ChangeStamp=0x5b9056e9f4 [3], Buffer=0x5b9056d9f0, BufferSize=0x5b9056e9f0 [8]) => 0

NtCreateEvent(EventHandle=0x5b9056e960 [0x74], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e120 [0x00000166c15a5000], ZeroBits=0, pSize=0x5b9056e1c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x166c15a4f90 [0x78], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x74) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x78, IoCompletionHandle=0x1c, TargetObjectHandle=0x74, KeyContext=0x166c15a4fa8, ApcContext=0x166c15a4e20, IoStatus=0x0000016600000000, IoStatusInformation=0, AlreadySignaled=0x5b9056e8e0 [0xc15a0b00]) => 0

NtSubscribeWnfStateChange(StateName=0x166c15a5120 [0xa3bc0875], ChangeStamp=3, EventMask=0x11, SubscriptionId=0x5b9056e9d0 [0x8774]) => 0

NtQueryWnfStateData(StateName=0x5b9056eb40 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x5b9056eb38 [0], Buffer=null, BufferSize=0x5b9056eb3c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x166c15a5450 [0xa3bc7c75], ChangeStamp=0, EventMask=0x11, SubscriptionId=0x5b9056e9b0 [0x8775]) => 0

NtQueryWnfStateData(StateName=0x5b9056eb40 [0xa3bc88f5], TypeId=null, ExplicitScope=null, ChangeStamp=0x5b9056eb38 [0], Buffer=null, BufferSize=0x5b9056eb3c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x166c15a5600 [0xa3bc88f5], ChangeStamp=0, EventMask=0x11, SubscriptionId=0x5b9056e9b0 [0x8776]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3 [SystemFeatureConfigurationSectionInformation], QueryType=0x5b9056e8f0 [0], Alignment=0x18, SystemInformation=0x5b9056e910, Length=0x50, ReturnLength=null) => 0

NtMapViewOfSection(SectionHandle=0x7c, ProcessHandle=-1, BaseAddress=0x5b9056e8c0 [0x00000166c1480000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9056e8c8 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x80, ProcessHandle=-1, BaseAddress=0x5b9056e8c0 [0x00000166c14e0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9056e8c8 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x84, ProcessHandle=-1, BaseAddress=0x5b9056e8c0 [0x00000166c14f0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9056e8c8 [0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0x7c) => 0

NtClose(Handle=0x80) => 0

NtClose(Handle=0x84) => 0

NtQueryWnfStateData(StateName=0x5b9056e8f8 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x5b9056e988 [0], Buffer=0x5b9056e9e0, BufferSize=0x5b9056e8e0 [0]) => 0

NtSetTimer2(TimerHandle=0x28, DueTime=0x5b9056e970 [-3e+09], Period=null, Parameters=0x5b9056e978) => 0

NtOpenKey(KeyHandle=0x5b9056eb40, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9056eb58, InputBufferLength=0xa0, OutputBuffer=0x5b9056eb58, OutputBufferLength=0xa0, ReturnLength=0x5b9056eb50 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9056eb98, InputBufferLength=0x18, OutputBuffer=0x5b9056ebb0, OutputBufferLength=0x78, ReturnLength=0x5b9056eb90 [0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e470 [0x00000166c15a6000], ZeroBits=0, pSize=0x5b9056e518 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9056eb88, InputBufferLength=0xa0, OutputBuffer=0x5b9056eb88, OutputBufferLength=0xa0, ReturnLength=0x5b9056eb80 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9056ebc8, InputBufferLength=0x18, OutputBuffer=0x5b9056ebe0, OutputBufferLength=0x78, ReturnLength=0x5b9056ebc0 [0]) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0x5b9056ee90, VmInformation=0x5b9056ef68, VmInformationLength=4) => 0xc00000bb [50 '╥оъюощ чряЁюё эх яюффхЁцштрхЄё .']

NtOpenKey(KeyHandle=0x5b9056ea70, DesiredAccess=0x9, ObjectAttributes=0x10:"lab2.exe") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9056e978, InputBufferLength=0xa0, OutputBuffer=0x5b9056e978, OutputBufferLength=0xa0, ReturnLength=0x5b9056e970 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9056e9b8, InputBufferLength=0x18, OutputBuffer=0x5b9056e9d0, OutputBufferLength=0x78, ReturnLength=0x5b9056e9b0 [0]) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x7ff8e3757aa0, Length=0x40, ReturnLength=null) => 0

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

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=4, OldProtect=0x5b9056ebb8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056eba8 [0x00007ff8e3263000], Size=0x5b9056eba0 [0x1000], NewProtect=2, OldProtect=0x5b9056ebb8 [4]) => 0

NtOpenKey(KeyHandle=0x5b9056f190, DesiredAccess=0x3, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x5b9056f170, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x5b9056f168 [0x90], DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0

NtQueryValueKey(KeyHandle=0x90, ValueName="TransparentEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9056f220, Length=0x50, ResultLength=0x5b9056f160) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x90) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0x5b9056f0b0, Length=0x58, ReturnLength=0x5b9056f0a8 [0x2c]) => 0

NtOpenKey(KeyHandle=0x5b9056f168, 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=0x5b9056f250 [0x94], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x94, ValueName="LongPathsEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9056f290, Length=0x14, ResultLength=0x5b9056f258 [0x10]) => 0

NtClose(Handle=0x94) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0x5b9056f230, Length=4) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9056f1b0 [1], Alignment=4, SystemInformation=0x166c15a3840, Length=0x50, ReturnLength=0x5b9056f1a8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x166c15a6270 [0x98], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, NumberOfConcurrentThreads=5) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x166c15a6268 [0x9c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null, CompletionPortHandle=0x98, WorkerProcessHandle=-1, StartRoutine=0x7ff8e54bd110, StartParameter=0x166c15a6230, MaxThreadCount=0x200, StackReserve=0x00100000, StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=0xd [WorkerFactoryFlags], Buffer=0x5b9056f278, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x166c15a62c0 [0xa0], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x166c15a62c8 [0xa4], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xa4, IoCompletionHandle=0x98, TargetObjectHandle=0xa0, KeyContext=0x166c15a62d0, ApcContext=0x166c15a62a0, IoStatus=0, IoStatusInformation=1, AlreadySignaled=0x5b9056f170 [0]) => 0

NtCreateTimer2(TimerHandle=0x166c15a6338 [0xa8], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x16600000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x166c15a6340 [0xac], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xac, IoCompletionHandle=0x98, TargetObjectHandle=0xa8, KeyContext=0x166c15a6348, ApcContext=0x166c15a62a0, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0x5b9056f170 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=2 [WorkerFactoryIdleTimeout], Buffer=0x5b9056f278, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0x5b9056f278, BufferLength=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f280 [0x00007ff6f9be4000], Size=0x5b9056f288 [0x1000], NewProtect=4, OldProtect=0x5b9056f618 [2]) => 0

NtOpenSection(SectionHandle=0x5b9056ed18, DesiredAccess=0xd, ObjectAttributes=0x3c:"VCRUNTIME140D.dll") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtOpenSection(SectionHandle=0x5b9056ed18, DesiredAccess=0xd, ObjectAttributes=0x3c:"ucrtbased.dll") => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtQueryWnfStateData(StateName=0x5b9056eb10 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x5b9056eba8 [0], Buffer=0x5b9056ec00, BufferSize=0x5b9056eb00 [0]) => 0

NtQueryWnfStateData(StateName=0x5b9056e9b0 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x5b9056ea48 [0], Buffer=0x5b9056eaa0, BufferSize=0x5b9056e9a0 [0]) => 0

NtOpenKey(KeyHandle=0x5b9056ed80 [0x94], DesiredAccess=0x1, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x94, ValueName="SafeDllSearchMode", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9056ed90, Length=0x10, ResultLength=0x5b9056ed88) => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e560 [0x00000166c15a7000], ZeroBits=0, pSize=0x5b9056e608 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab2\x64\Debug\VCRUNTIME140D.dll", Attributes=0x5b9056ee28) => 0xc0000034 [2 '═x єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\VCRUNTIME140D.dll", Attributes=0x5b9056ee28 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0x5b9056ef30 [0xb0], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\VCRUNTIME140D.dll", IoStatusBlock=0x5b9056ef98 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0x5b9056ef38 [0xb4], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xb0) => 0

Loaded DLL at 00007FF8C53F0000 C:\Windows\SYSTEM32\VCRUNTIME140D.dll

NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x166c15a6470 [0x00007ff8c53f0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x166c15a36c0 [0x0002b000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x5b9056edd0 [8.92392e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ede0 [0x00007ff8e55f1000], Size=0x5b9056edd8 [0x4000], NewProtect=4, OldProtect=0x5b9056edd0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ede0 [0x00007ff8e55f1000], Size=0x5b9056edd8 [0x4000], NewProtect=2, OldProtect=0x5b9056edd0 [4]) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0x5b9056e8b0, Length=0x330, ReturnLength=0x5b9056e868) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0x5b9056e8b0, Length=0x330, ReturnLength=0x5b9056e868) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ee30 [0x00007ff8c5410000], Size=0x5b9056ee38 [0x1000], NewProtect=4, OldProtect=0x166c15a36a8 [2]) => 0

NtOpenSection(SectionHandle=0x5b9056e8c8, DesiredAccess=0xd, ObjectAttributes=0x3c:"ucrtbased.dll") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xb4) => 0

NtClose(Handle=0xb0) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab2\x64\Debug\ucrtbased.dll", Attributes=0x5b9056ee28) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", Attributes=0x5b9056ee28 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0x5b9056ef30 [0xb8], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", IoStatusBlock=0x5b9056ef98 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0x5b9056ef38 [0xbc], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xb8) => 0

Loaded DLL at 00007FF8B05B0000 C:\Windows\SYSTEM32\ucrtbased.dll

NtMapViewOfSection(SectionHandle=0xbc, ProcessHandle=-1, BaseAddress=0x166c15a66d0 [0x00007ff8b05b0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x166c15a6630 [0x00221000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x5b9056edd0 [8.92393e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ede0 [0x00007ff8e55f1000], Size=0x5b9056edd8 [0x4000], NewProtect=4, OldProtect=0x5b9056edd0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ede0 [0x00007ff8e55f1000], Size=0x5b9056edd8 [0x4000], NewProtect=2, OldProtect=0x5b9056edd0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ee30 [0x00007ff8b075b000], Size=0x5b9056ee38 [0x1000], NewProtect=4, OldProtect=0x166c15a6618 [2]) => 0

NtClose(Handle=0xbc) => 0

NtClose(Handle=0xb8) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Users\T470\source\repos\lab2\x64\Debug\ucrtbased.dll", Attributes=0x5b9056ee28) => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\ucrtbased.dll", Attributes=0x5b9056ee28 [ARCHIVE]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f5f8 [0x00007ff6f9be4000], Size=0x5b9056f600 [0x1000], NewProtect=2, OldProtect=0x5b9056f150 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c15a65f8 [0x00007ff8b075b000], Size=0x166c15a6600 [0x1000], NewProtect=2, OldProtect=0x5b9056f150 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c15a3688 [0x00007ff8c5410000], Size=0x166c15a3690 [0x1000], NewProtect=2, OldProtect=0x5b9056f150 [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=0x5b9056f4b8, VmInformation=0x5b9056f3e0, VmInformationLength=4) => 0xc00000bb [50 '╥рьющ чряЁюё эх яюффхЁцштрхЄё .']

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11 [ThreadHideFromDebugger], ThreadInformation=0x5b9056f2f0, Length=1, ReturnLength=null) => 0

Initial breakpoint

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0x5b9056f170, VmInformation=0x5b9056f248, VmInformationLength=4) => 0xc00000bb [50 '╥рьющ чряЁюё эх яюффхЁцштрхЄё .']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e540 [0x00000166c15a8000], ZeroBits=0, pSize=0x5b9056e5e8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x50, IoStatusBlock=0x5b9056ee90 [0/8], FsInformation=0x5b9056eeb0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0x5b9056ee90 [0/8], FsInformation=0x5b9056eeb0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0x5b9056ee90 [0/8], FsInformation=0x5b9056eeb0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtOpenKey(KeyHandle=0x5b9056d970 [0xb0], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions") => 0

NtQueryValueKey(KeyHandle=0xb0, ValueName="", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x5b9056de60, Length=0x214, ResultLength=0x5b9056de08 [0x2a]) => 0

NtQueryValueKey(KeyHandle=0xb0, ValueName="000603xx", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0x5b9056de40, Length=0x214, ResultLength=0x5b9056dbe8 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e5a0 [0x00000166c15aa000], ZeroBits=0, pSize=0x5b9056e648 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e580 [0x00000166c15ac000], ZeroBits=0, pSize=0x5b9056e628 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0x5b9056f1b0, VmInformation=0x5b9056f288, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

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

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=3 [WorkerFactoryBindingCount], Buffer=0x5b9056f618, BufferLength=4) => 0

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

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6f9bd1127, MemoryInformationClass=0 [MemoryBasicInformation], MemoryInformation=0x5b9056f830, Length=0x30, ReturnLength=0x5b9056f7e0 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6f9bd1127, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0x5b9056f860, Length=0x30, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6f9bd1127, MemoryInformationClass=2 [MemoryMappedFilenameInformation], MemoryInformation=0x5b9056f8d8, Length=0x21a, ReturnLength=null) => 0

Failed to open fileNtDeviceIoControlFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0x5b9056e6a0 [0/0x13], IoControlCode=0x00500016, InputBuffer=0x5b9056e6b0, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0x5b9056f450, Length=4) => 0

NtOpenSection(SectionHandle=0x5b9056f428, DesiredAccess=0xd, ObjectAttributes=0x3c:"kernel.appcore.dll") => 0xc0000034 [2 '═х єфрхЄё эрщЄш єърчрээ√щ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\SYSTEM32\kernel.appcore.dll", Attributes=0x5b9056f1e8 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0x5b9056f1e0 [0xb8], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\Windows\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0x5b9056f248 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0x5b9056f1e8 [0xbc], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xb8) => 0

Loaded DLL at 00007FF8E0950000 C:\Windows\SYSTEM32\kernel.appcore.dll

NtMapViewOfSection(SectionHandle=0xbc, ProcessHandle=-1, BaseAddress=0x166c15aa630 [0x00007ff8e0950000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x166c15aacb0 [0x00012000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x5b9056f080 [8.92395e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f098 [0x00007ff8e095f000], Size=0x5b9056f090 [0x1000], NewProtect=2, OldProtect=0x5b9056f100 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f090 [0x00007ff8e55f1000], Size=0x5b9056f088 [0x4000], NewProtect=4, OldProtect=0x5b9056f080 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f090 [0x00007ff8e55f1000], Size=0x5b9056f088 [0x4000], NewProtect=2, OldProtect=0x5b9056f080 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056f0e0 [0x00007ff8e0955000], Size=0x5b9056f0e8 [0x1000], NewProtect=4, OldProtect=0x166c15aac98 [2]) => 0

NtOpenSection(SectionHandle=0x5b9056eb78 [0xb4], DesiredAccess=0xd, ObjectAttributes=0x3c:"msvcrt.dll") => 0

Loaded DLL at 00007FF8E42A0000 C:\Windows\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x166c15aca00 [0x00007ff8e42a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x166c15ac960 [0x0009e000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x5b9056e9f0 [8.92396e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ea00 [0x00007ff8e55f1000], Size=0x5b9056e9f8 [0x4000], NewProtect=4, OldProtect=0x5b9056e9f0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ea00 [0x00007ff8e55f1000], Size=0x5b9056e9f8 [0x4000], NewProtect=2, OldProtect=0x5b9056e9f0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ea50 [0x00007ff8e4316000], Size=0x5b9056ea58 [0x2000], NewProtect=4, OldProtect=0x166c15ac948 [2]) => 0

NtClose(Handle=0xb4) => 0

NtOpenSection(SectionHandle=0x5b9056eb78 [0xc0], DesiredAccess=0xd, ObjectAttributes=0x3c:"RPCRT4.dll") => 0

Loaded DLL at 00007FF8E3820000 C:\Windows\System32\RPCRT4.dll

NtMapViewOfSection(SectionHandle=0xc0, ProcessHandle=-1, BaseAddress=0x166c15acdc0 [0x00007ff8e3820000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x166c15acd20 [0x00123000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x5b9056e9f0 [8.92396e+11], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ea08 [0x00007ff8e393b000], Size=0x5b9056ea00 [0x1000], NewProtect=2, OldProtect=0x5b9056ea70 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ea00 [0x00007ff8e55f1000], Size=0x5b9056e9f8 [0x4000], NewProtect=4, OldProtect=0x5b9056e9f0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ea00 [0x00007ff8e55f1000], Size=0x5b9056e9f8 [0x4000], NewProtect=2, OldProtect=0x5b9056e9f0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9056ea50 [0x00007ff8e390c000], Size=0x5b9056ea58 [0x2000], NewProtect=4, OldProtect=0x166c15acd08 [2]) => 0

NtClose(Handle=0xc0) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c15aac78 [0x00007ff8e0955000], Size=0x166c15aac80 [0x1000], NewProtect=2, OldProtect=0x5b9056efd0 [4]) => 0

NtClose(Handle=0xbc) => 0

NtClose(Handle=0xb8) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c15ac928 [0x00007ff8e4316000], Size=0x166c15ac930 [0x2000], NewProtect=2, OldProtect=0x5b9056f2f0 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0x5b9056f250, Length=0x28) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x166c15acce8 [0x00007ff8e390c000], Size=0x166c15accf0 [0x2000], NewProtect=2, OldProtect=0x5b9056f2f0 [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=0x5b9056f310, VmInformation=0x5b9056f3e8, VmInformationLength=4) => 0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056eb40 [0x00000166c1770000], ZeroBits=0, pSize=0x5b9056eb48 [0x001c0000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056eb40 [0x00000166c1770000], pSize=0x5b9056eb38 [0x001b0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056eb28 [0x00000166c1920000], ZeroBits=0, pSize=0x5b9056eb20 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x50, IoStatusBlock=0x5b9056f110 [0/8], FsInformation=0x5b9056f130, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0x5b9056f110 [0/8], FsInformation=0x5b9056f130, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0x5b9056f110 [0/8], FsInformation=0x5b9056f130, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e9b0 [0x00000166c15ae000], ZeroBits=0, pSize=0x5b9056ea58 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e980 [0x00000166c1922000], ZeroBits=0, pSize=0x5b9056ea28 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9056e960 [0x00000166c1923000], ZeroBits=0, pSize=0x5b9056ea08 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0x5b9056f310, VmInformation=0x5b9056f3e8, VmInformationLength=4) => 0xc00000bb [50 '╥рьющ чряЁюё эх яюффхЁцштрхЄё .']

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0x5b9056f350, VmInformation=0x5b9056f428, VmInformationLength=4) => 0xc00000bb [50 '╥рьющ чряЁюё эх яюффхЁцштрхЄё .']

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

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0x5b9056f580, Length=0x330, ReturnLength=0x5b9056f538) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0x5b9056f580, Length=0x330, ReturnLength=0x5b9056f538) => 0xc0000225 [1168 '▌ ыхьхэЄ эх эрщфхэ.']

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

NtClose(Handle=0x8c) => 0

NtClose(Handle=0x4c) => 0

NtClose(Handle=0x7c) => 0

NtClose(Handle=0x88) => 0

NtQueryWnfStateData(StateName=0x5b9056f630 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x5b9056e574 [0x68d9], Buffer=0x5b9056e5d0, BufferSize=0x5b9056e570 [0x684]) => 0

NtQueryWnfStateData(StateName=0x5b9056f4b8 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x5b9056f548 [0], Buffer=0x5b9056f5a0, BufferSize=0x5b9056f4a0 [0]) => 0

Process 9284 exit code: 1

Исследование зависимости ускорения и эффективности алгоритма от входных данных и количества потоков

Число потоков	Время исполнения(мс)	Ускорение	Эффективность
1	**0.200000**	**1**	**1**
3	**0.200000**	**1**	**0.333333333**
4	**0.1200000**	**1.666666667**	**0.416666675**

Вывод

В ходе выполнения лабораторной работы я познакомился с примитивом синхронизации семафор и написал многопоточную программу для вычисления среднего арифметического чисел в файле. Проблем при выполнении работы не возникло.