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: Демидов М.С.

Преподаватель: Бахарев В.Д. (ФИИТ)

Оценка: _____

Дата: 05.11.24

Москва, 2024

Постановка задачи

Вариант 3.

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.

Отсортировать массив целых чисел при помощи параллельной сортировки слиянием.

Общий метод и алгоритм решения

Использованные системные вызовы:

- WriteFile; – записывает данные в канал.
- CloseHandle; – закрывает хендлеры, в том числе и каналы.
- GetStdHandle; – Возвращает хендлер по DWORD.
- ReleaseSemaphore; – закрывает один из потоков.
- CreateSemaphore; – создает семафор.
- CreateThread; – создать поток.
- WaitForSingleObject; – ожидание, пока поток закончит свою работу.
- WaitForMultipleObjects; – ожидание, пока все потоки не закончат свою работу.

Я создал свой собственный printf, fprintf с помощью функций WriteConsoleA & WriteFile соответственно. То есть просто обрабатывается форматная строка, подставляются все аргументы, конвертируются в единую строку, а затем записываются куда надо.

Затем началась работа над самим заданием непосредственно. Сначала я реализовал алгоритм сортировки слиянием стандартный. То есть написал функцию mergeSort, которая разделяет массив на две части и вызывает рекурсивно для них сортировку. А потом уже вызывается merge, который, соответственно, сливает разделенные части массива в нужном порядке. Далее идут стандартные обработки ошибок на входные данные. На вход подается размер массива и количество потоков. Размер массива надо ограничить, тут понятно, просто int нужно обработать. А что делать с количеством потоков? Как понять, какой предел? Вообще по-хорошему потоки привязаны к ядру, но сейчас вставлю интересную вырезку из статьи:

Физически - не более колличества 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 хандлов (т.е. много). Ваш вопрос сводится к макс колличество хандлов (т.к. каждому thread нужно присвоить хандл) тогда ответ - до 10000 (минус штук 300 используется системой). Активные хандлы ОС "преобразует" в таски, а процессор аппаратным решением выбирает какой таск выполнять сейчас на аппаратном уровне. Хандлами могут быть - файлы, pipes, event, mailslot и другие обьекты ОС, если

программа активно использует хандлы (например для каждого thread открывается file) то хандлы закончатся в два раза быстрее, т.к. общее число ханлов не должно превышать 10000.Уровень DOT NET. У c# Thread - это обьект за которым может быть а может не быть реального Thread Handle. Кроме того, хандлы обьеденяются в пул (для повторного использования). Активный Thread всегда подкреплен Thread Handle ОС, но неактивые можно создавать - пока не закончится память Heap. При превышении определённого числа активных Thread - получим ошибку, что не возможно создать хандл.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 елементов, 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 распределает эти таски между ядрами апаратным решением. Что ОС будет делать когда они закончатся - скорее всего у ОС встроен константой предел на колличество тасков, так как при слишком большом их количестве процессор начнёт терять производительность.

Так, с ограничениями разобрались. Теперь сама суть задания))). Нужно просто посчитать количество чанков, то есть кусков массивов, которые будут отправляться в потоки. То есть просто разделить длину массива на количество запрошенных массивов. Создаем массив, заполняем случайными целыми числами. Создаем семафор на запрошенное количество потоков. Затем создаем массив потоков заданного размера. И заполняем его, пока семафор позволяет. Потом ждем, пока семафор даст отмашку об освободившемся потоке, и дальше запускаем чанки. В конце все это сливается в один массив и выписывается. Вот, собственно, вся суть лабораторноц.

Код программы

demidovStdio.h

```c
#define INITIAL_BUFFER_SIZE 128


  #include <windows.h>

  #include <stdarg.h>

  #include <string.h>


  enum ret_type_t{

      SUCCESS,     //Successful end

      ERROR_ARGS_COUNT,     //Wrong args number

      ERROR_CREATE_PIPE,  //Failed to create a new pipeline

      ERROR_CREATE_CHILD_PROCESS, //Failed to create a child process

      ERROR_READ, //Failed to read from pipe

      ERROR_DEV_ZERO, //Devision by zero detected

      ERROR_FULL, //Overflow

      ERROR_OPEN_FILE,     //Error with file opening

      ERROR_CLOSE_FILE,    //Error with closing file

      ERROR_FILE_WRITE,    //Error with file writing

      ERROR_HANDLER_INHERITED, //Error handler reading

      ERROR_PIPE_WRITE,    //Failed to write smth in the pipe

      ERROR_HEAP,          //Failed to malloc

  };


  //THE MOST POWERFUL PRINTF IN HISTORY

  void demidov_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) {
```

```c
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 '%': {
```

```c
                *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);
}


//Printf for files
int demidov_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 == '%') {
```

```c
fmt_ptr++;

switch (*fmt_ptr) {

    case 'd': {

        int value = va_arg(args, int);

        char num_buffer[20];

        char* num_ptr = num_buffer;

        if (value < 0) {

            *buf_ptr++ = '-';

            value = -value;

        }

        do {

            *num_ptr++ = (char)((value % 10) + '0');

            value /= 10;

        } while (value > 0);

        while (num_ptr > num_buffer) {

            *buf_ptr++ = *--num_ptr;

        }

        break;

    }

    case 's': {

        const char* str = va_arg(args, const char*);

        while (*str) {

            *buf_ptr++ = *str++;

        }

        break;

    }

    case 'c': {

        char ch = (char)va_arg(args, int);

        *buf_ptr++ = ch;

        break;

    }

    case '%': {

        *buf_ptr++ = '%';
```

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


// Open the file for writing
DWORD bytesWritten;
WriteFile(fileHandle, buffer, (DWORD)(buf_ptr - buffer), &bytesWritten, NULL);


va_end(args);
}
```

Lab2.c

```c
#include "demidovStdio.h"


typedef struct {
    int* array;
    int start;
    int end;
} ThreadData;


HANDLE semaphore;


void merge(int* array, int start, int mid, int end) {
    int i, j, k;
```

```c
int n1 = mid - start + 1;

int n2 = end - mid;


int* L = (int*)malloc(n1 * sizeof(int));

int* R = (int*)malloc(n2 * sizeof(int));


for (i = 0; i < n1; i++)

    L[i] = array[start + i];

for (j = 0; j < n2; j++)

    R[j] = array[mid + 1 + j];


i = 0;

j = 0;

k = start;

while (i < n1 && j < n2) {

    if (L[i] <= R[j]) {

        array[k] = L[i];

        i++;

    } else {

        array[k] = R[j];

        j++;

    }

    k++;

}


while (i < n1) {

    array[k] = L[i];

    i++;

    k++;

}
```

```c
        while (j < n2) {

            array[k] = R[j];

            j++;

            k++;

        }


        free(L);

        free(R);

}


void mergeSort(int* array, int start, int end) {

    if (start < end) {

        int mid = start + (end - start) / 2;

        mergeSort(array, start, mid);

        mergeSort(array, mid + 1, end);

        merge(array, start, mid, end);

    }

}


DWORD WINAPI mergeSortThread(LPVOID lpParam) {

    ThreadData* data = (ThreadData*)lpParam;

    mergeSort(data->array, data->start, data->end);


    ReleaseSemaphore(semaphore, 1, NULL);

    return SUCCESS;

}


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

    if (argc != 3) {
```

```c
        demidov_printf("Usage: %s <array_size> <max_threads>\n", argv[0]);

        return ERROR_ARGS_COUNT;

    }


    int arraySize = atoi(argv[1]);

    int maxThreads = atoi(argv[2]);


    if (arraySize == 0) {

        demidov_printf("The array is empty. Cannot sort a void\n");

        return ERROR_ZERO_LENGTH_ARRAY;

    }


    if (maxThreads == 0) {

        demidov_printf("There are no threads. Cannot do anything\n");

        return ERROR_ZERO_THREADS;

    }


    if (maxThreads > MAX_THREADS || maxThreads > arraySize) {

        demidov_printf("\nMax threads limit exceeded. Setting to %d\n\n", arraySize);

        maxThreads = arraySize;

    }


    int* array = (int*)malloc(arraySize * sizeof(int));

    if (!array) {

        demidov_printf("Memory allocation error occured\n");

        return ERROR_MALLOC;

    }


    srand(time(NULL));

    for (int i = 0; i < arraySize; i++) {
```

```c
        array[i] = rand() % 1000;
    }

    for (int i = 0; i < arraySize; i++) {
        demidov_printf("%d ", array[i]);
    }
    demidov_printf("\n\n");

    semaphore = CreateSemaphore(NULL, maxThreads, maxThreads, NULL);
    if (semaphore == NULL) {
        demidov_printf("CreateSemaphore error occured\n");
        return ERROR_CREATE_SEMAPHORE;
    }

    HANDLE* threads = (HANDLE*)malloc(maxThreads * sizeof(HANDLE));
    if (!threads) {
        demidov_printf("Failed to malloc for threads\n");
        return ERROR_MALLOC;
    }

    ThreadData* threadData = (ThreadData*)malloc(maxThreads * sizeof(ThreadData));
    if (!threadData) {
        demidov_printf("Failed to malloc for threadData\n");
        return ERROR_MALLOC;
    }

    int chunkSize = arraySize / maxThreads;
    for (int i = 0; i < maxThreads; i++) {
        threadData[i].array = array;
        threadData[i].start = i * chunkSize;
```

```c
        threadData[i].end = (((i + 1) * chunkSize - 1) >= arraySize - chunkSize - 1) ? arraySize - 1 : (i
+ 1) * chunkSize - 1;


        WaitForSingleObject(semaphore, INFINITE);


        threads[i] = CreateThread(NULL, 0, mergeSortThread, &threadData[i], 0, NULL);

        if (threads[i] == NULL) {

            demidov_printf("CreateThread error occured\n");

            return ERROR_CREATE_THREAD;

        }

    }


    WaitForMultipleObjects(maxThreads, threads, TRUE, INFINITE);


    for (int i = 1; i < maxThreads; i++) {

        merge(array, 0, i * chunkSize - 1, (i + 1) * chunkSize - 1);

    }


    for (int i = 0; i < arraySize - 1; i++) {

        if (array[i] > array[i + 1]) {

            demidov_printf("Sorting failed at index %d\n", i);

            break;

        }

    }


    for (int i = 0; i < arraySize; i++) {

        demidov_printf("%d ", array[i]);

    }
    demidov_printf("\n");
```

```c
    CloseHandle(semaphore);

    for (int i = 0; i < maxThreads; i++) {

        CloseHandle(threads[i]);

    }

    free(threads);

    free(threadData);

    free(array);


    demidov_printf("Sorting completed successfully\n");

    return 0;

}
```

Протокол работы программы

PS D:\Users\lenovo\Desktop\osi\Lab2> NtTrace .\lab2.exe 10 10

Process 288048 starting at 00007FF6DBBC13E0 with command line: ".\lab2.exe 10 10"

D:\Users\lenovo\Desktop\osi\Lab2\lab2.exe

Loaded DLL at 00007FFD04B90000 ntdll.dll

NtQueryPerformanceCounter(Counter=0xe54c7ff640 [7.42868e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff688 [0x00007ffd04d2e000], Size=0xe54c7ff680 [0x1000], NewProtect=4, OldProtect=0xe54c7ff6c0 [8]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff688 [0x00007ffd04d2e000], Size=0xe54c7ff680 [0x1000], NewProtect=8, OldProtect=0xe54c7ff6c0 [4]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd04c34240, MemoryInformationClass=6 [MemoryImageInformation], MemoryInformation=0xe54c7ff610, Length=0x18, ReturnLength=null) => 0

NtCreateEvent(EventHandle=0x7ffd04d16398 [8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtManageHotPatch(Unknown=9, Unknown=0xe54c7ff4a8 [1], Unknown=8, Unknown=0xe54c7ff4a0) => 0xc00000bb [50 '╥рьющ чряЁюё эх яюффхЁцштрхЄё .']

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

NtCreateEvent(EventHandle=0x7ffd04d163e8 [0xc], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xe54c7ff3c0, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xe54c7ff0b8, Length=4, ReturnLength=null) => 0

NtOpenKey(KeyHandle=0xe54c7fef68 [0x10], DesiredAccess=GENERIC_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\CodePage") => 0

NtQueryValueKey(KeyHandle=0x10, ValueName="ACP", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe54c7fefd0, Length=0x24, ResultLength=0xe54c7fef60 [0x16]) => 0

NtQueryValueKey(KeyHandle=0x10, ValueName="OEMCP", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe54c7fefd0, Length=0x24, ResultLength=0xe54c7fef60 [0x14]) => 0

NtClose(Handle=0x10) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null, SectionPointer=0x7ffd04d137e0 [0x0000020081530000], SectionSize=null) => 0

```
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x7ffd04d137e8 [0x000020081550000], SectionSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0xe54c7ff058 [0x000020081570000], SectionSize=null) => 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0xe54c7ff010, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd04b90000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0xe54c7fefa0, Length=0x18, ReturnLength=null) =>
0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0xe54c7fefe0, Length=0x50,
ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff030 [0x00007ffd04d2b000],
Size=0xe54c7ff028 [0x4000], NewProtect=2, OldProtect=0xe54c7ff020 [4]) => 0

NtOpenKey(KeyHandle=0xe54c7fece0 [0x14], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x14, ValueName="RaiseExceptionOnPossibleDeadlock",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe54c7fecf0,
Length=0x50, ResultLength=0xe54c7fece8) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x14) => 0

NtOpenKey(KeyHandle=0xe54c7fec78 [0x18], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options") => 0

NtOpenKey(KeyHandle=0xe54c7fed60, DesiredAccess=0x9, ObjectAttributes=0x18:"lab2.exe") =>
0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xe54c7fecc0, 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=0x7ffd04d17268, Length=4, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0xe54c7fefc8, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0xe54c7fe960, Length=0x330, ReturnLength=0xe54c7fe918) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0xe54c7fe960, Length=0x330, ReturnLength=0xe54c7fe918) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtOpenKey(KeyHandle=0xe54c7fef10 [0x1c], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x1c, ValueName="ResourcePolicies", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe54c7fef50, Length=0x18,
ResultLength=0xe54c7fef18) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
```

```
NtClose(Handle=0x1c) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0xe54c7ff020, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xe54c7fefc0, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation],
SystemInformation=0xe54c7feff0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffd04d17a88 [0x00007ff533d30000],
ZeroBits=0x000000e54c7fef70, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0xe54c7feeb8, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffd04d17a80 [0x00007ff535d30000],
ZeroBits=0x000000e54c7fef78, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null,
DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffd04d17af0 [0x00007ff433d10000],
ZeroBits=0x000000e54c7fef20, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0xe54c7fee68, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xe54c7fee60, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fea40 [0x0000020081580000],
ZeroBits=0, pSize=0xe54c7fea48 [0x00270000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fea40 [0x0000020081580000],
pSize=0xe54c7fea38 [0x00170000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fea28 [0x00000200816f0000],
ZeroBits=0, pSize=0xe54c7fea20 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5
[SystemHypervisorSharedPageInformation], SystemInformation=0xe54c7ff1c0, Length=8,
ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap],
SystemInformation=0xe54c7fec30, Length=0x408, ReturnLength=0xe54c7ff050 [0x18]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xe54c7fec18 [4], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0xe54c7fec10) => 0xc0000004 [24 '¬ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xe54c7fec18 [4], Alignment=4,
SystemInformation=0x200816f0880, Length=0x50, ReturnLength=0xe54c7fec10 [0x50]) => 0

NtCreateEvent(EventHandle=0xe54c7fee08 [0x20],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x200816f0c40 [0x24],
DesiredAccess=0x1, ObjectAttributes=null) => 0
```

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xe54c7feb80 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0xe54c7feb78) => 0xc0000004 [24 '¬ышэр
т√фрээющ яЁюуЁрьыющ ъьюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xe54c7feb80 [6], Alignment=4,
SystemInformation=0x200816f0ff0, Length=0x30, ReturnLength=0xe54c7feb78 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x200816f0d20 [0x14],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x200816f0d18 [0x28],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x14, WorkerProcessHandle=-1, StartRoutine=0x7ffd04bc5580,
StartParameter=0x200816f0ce0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x200816f0d70 [0x2c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x200816f0d78 [0x30],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x30, IoCompletionHandle=0x14,
TargetObjectHandle=0x2c, KeyContext=0x200816f0d80, ApcContext=0x200816f0d50, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0xe54c7feb40 [0]) => 0

NtCreateTimer2(TimerHandle=0x200816f0de8 [0x1c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x20000000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x200816f0df0 [0x10],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x10, IoCompletionHandle=0x14,
TargetObjectHandle=0x1c, KeyContext=0x200816f0df8, ApcContext=0x200816f0d50, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xe54c7feb40 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x28, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0xe54c7fec28, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x28, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0xe54c7fec28, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x28, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0xe54c7fed48, BufferLength=4) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x24, IoCompletionHandle=0x14,
TargetObjectHandle=0x20, KeyContext=0x200816f0c58, ApcContext=0x200816f0ad0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xe54c7fed90 [0x816f0c00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0xe54c7fee48, InputBufferLength=4,
OutputBuffer=null, OutputBufferLength=0, ReturnLength=0xe54c7fee00 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7feea8, InputBufferLength=0xa0,
OutputBuffer=0xe54c7feea8, OutputBufferLength=0xa0, ReturnLength=0xe54c7feea0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe54c7feef8, InputBufferLength=0x18,
OutputBuffer=0xe54c7fef10, OutputBufferLength=0x78, ReturnLength=0xe54c7feef0 [0]) => 0

```
NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7feef8, InputBufferLength=0xa0,
OutputBuffer=0xe54c7feef8, OutputBufferLength=0xa0, ReturnLength=0xe54c7feef0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7feef8, InputBufferLength=0xa0,
OutputBuffer=0xe54c7feef8, OutputBufferLength=0xa0, ReturnLength=0xe54c7feef0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7feea8, InputBufferLength=0xa0,
OutputBuffer=0xe54c7feea8, OutputBufferLength=0xa0, ReturnLength=0xe54c7feea0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe54c7feef8, InputBufferLength=0x18,
OutputBuffer=0xe54c7fef10, OutputBufferLength=0x78, ReturnLength=0xe54c7feef0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7feef8, InputBufferLength=0xa0,
OutputBuffer=0xe54c7feef8, OutputBufferLength=0xa0, ReturnLength=0xe54c7feef0 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe830 [0x00000200816f2000],
ZeroBits=0, pSize=0xe54c7fe8d8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe450 [0x00000200816f4000],
ZeroBits=0, pSize=0xe54c7fe4f8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7ff050 [0x00000200814c0000],
pSize=0xe54c7ff058 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff030 [0x00007ffd04d2b000],
Size=0xe54c7ff028 [0x4000], NewProtect=4, OldProtect=0xe54c7ff020 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ffd04d2b2b0 [0x48], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff030 [0x00007ffd04d2b000],
Size=0xe54c7ff028 [0x4000], NewProtect=2, OldProtect=0xe54c7ff020 [4]) => 0

NtOpenSymbolicLinkObject(LinkHandle=0xe54c7ff1a8 [0x4c], DesiredAccess=0x1,
ObjectAttributes=0x48:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x4c, LinkTarget="C:\WINDOWS\System32",
ReturnedLength=0xe54c7ff140 [0x28]) => 0

NtClose(Handle=0x4c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff000 [0x00007ffd04d2b000],
Size=0xe54c7feff8 [0x4000], NewProtect=4, OldProtect=0xe54c7feff0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff030 [0x00007ffd04d2b000],
Size=0xe54c7ff028 [0x4000], NewProtect=2, OldProtect=0xe54c7ff020 [4]) => 0

NtCreateEvent(EventHandle=0x7ffd04d162d8 [0x4c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ffd04d16310 [0x50],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe830 [0x00000200816f5000],
ZeroBits=0, pSize=0xe54c7fe8d8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fef90 [0x00007ffd04d2b000],
Size=0xe54c7fef88 [0x4000], NewProtect=4, OldProtect=0xe54c7fef80 [2]) => 0
```

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fef90 [0x00007ffd04d2b000], Size=0xe54c7fef88 [0x4000], NewProtect=2, OldProtect=0xe54c7fef80 [4]) => 0

NtOpenFile(FileHandle=0xe54c7ff038 [0x54], DesiredAccess=SYNCHRONIZE|0x20, ObjectAttributes="\??\D:\Users\lenovo\Desktop\osi\Lab2\", IoStatusBlock=0xe54c7fefa8 [0/1], ShareAccess=3, OpenOptions=0x21) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xe54c7fefa8 [0/8], FsInformation=0xe54c7fef90, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0xe54c7fed00) => 0xc000007c [1008 '┴юя√€ьр ёё√ыъш эр эхёе·хё€те■·шщ €юъхэ.']

NtOpenSection(SectionHandle=0xe54c7fec98 [0x58], DesiredAccess=0xd, ObjectAttributes=0x48:"KERNEL32.DLL") => 0

Loaded DLL at 00007FFD02EF0000 C:\WINDOWS\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x58, ProcessHandle=-1, BaseAddress=0x200816f5510 [0x00007ffd02ef0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x200816f5468 [0x000c4000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xe54c7feaf0 [7.42868e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fea80 [0x00007ffd02fb1000], Size=0xe54c7fea78 [0x1000], NewProtect=2, OldProtect=0xe54c7fea70 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7feb00 [0x00007ffd04d2b000], Size=0xe54c7feaf8 [0x4000], NewProtect=4, OldProtect=0xe54c7feaf0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7feb00 [0x00007ffd04d2b000], Size=0xe54c7feaf8 [0x4000], NewProtect=2, OldProtect=0xe54c7feaf0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7feb40 [0x00007ffd02f73000], Size=0xe54c7feb48 [0x4000], NewProtect=4, OldProtect=0x200816f5450 [2]) => 0

NtOpenSection(SectionHandle=0xe54c7fe538 [0x5c], DesiredAccess=0xd, ObjectAttributes=0x48:"KERNELBASE.dll") => 0

Loaded DLL at 00007FFD02360000 C:\WINDOWS\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x200816f5c50 [0x00007ffd02360000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x200816f5ba8 [0x003b9000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xe54c7fe390 [7.42868e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe320 [0x00007ffd026e7000], Size=0xe54c7fe318 [0x1000], NewProtect=2, OldProtect=0xe54c7fe310 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe3a0 [0x00007ffd04d2b000], Size=0xe54c7fe398 [0x4000], NewProtect=4, OldProtect=0xe54c7fe390 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe3a0 [0x00007ffd04d2b000], Size=0xe54c7fe398 [0x4000], NewProtect=2, OldProtect=0xe54c7fe390 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe3e0 [0x00007ffd025cf000], Size=0xe54c7fe3e8 [0x2000], NewProtect=4, OldProtect=0x200816f5b90 [2]) => 0

```
NtClose(Handle=0x5c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x200816f5430 [0x00007ffd02f73000],
Size=0x200816f5438 [0x4000], NewProtect=2, OldProtect=0xe54c7fe940 [4]) => 0

NtClose(Handle=0x58) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x200816f5b70 [0x00007ffd025cf000],
Size=0x200816f5b78 [0x2000], NewProtect=2, OldProtect=0xe54c7fea80 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0xe54c7fe9e0, Length=0x28) => 0

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

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

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0xe54c7fe7c0, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffd026c8ec0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fdd40 [0x00000200816f6000],
ZeroBits=0, pSize=0xe54c7fdde8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenSection(SectionHandle=0xe54c7fe580 [0x60], DesiredAccess=0x4,
ObjectAttributes="\Sessions\15\Windows\SharedSection") => 0

NtCreateSection(SectionHandle=0xe54c7fe5a0 [0x70],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0xe54c7fe590 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ffd04d16c08 [0x74], PortName="\Sessions\15\Windows\ApiPort",
SecurityQos=0xe54c7fe6c0, ClientView=0xe54c7fe5b8, ServerView=0xe54c7fe5e8,
MaxMsgLength=0xe54c7fe5b0 [0x3b8], ConnectionInfo=0xe54c7fe630,
ConnectionInfoLength=0xe54c7fe588 [0x30]) => 0

NtClose(Handle=0x70) => 0

NtMapViewOfSection(SectionHandle=0x60, ProcessHandle=-1, BaseAddress=0xe54c7fe598
[0x00007ff433c10000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe54c7fe5a8
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x60) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x200814c0000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0xe54c7fe280, Length=0x30, ReturnLength=null) =>
0

NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0xe54c7fe768 [0x00000200814d0000], SectionSize=null) => 0

NtInitializeNlsFiles(BaseAddress=0xe54c7fe760 [0x0000020081580000],
DefaultLocaleId=0x7ffd026cabb8 [0x419], DefaultCasingTableSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0xe54c7fe740 [0x0000020081650000], SectionSize=0xe54c7fe708 [0x00011000]) =>
0
```

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0xe54c7fe740 [0x0000020081670000], SectionSize=0xe54c7fe708 [0x00011000]) =>
0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fdeb0 [0x00000200816f7000],
ZeroBits=0, pSize=0xe54c7fdf58 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateFile(FileHandle=0xe54c7fe7c8 [0x78], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f,
ObjectAttributes=4:"\Connect", IoStatusBlock=0xe54c7fe180 [0/0x18], AllocationSize=null,
FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20,
EaBuffer=0x200816f70f0, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54c7fe710 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0xe54c7fe730, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0xe54c7fe738, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54c7fe500, IoControlCode=0x00500016, InputBuffer=0xe54c7fe510,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7fe618, InputBufferLength=0xa0,
OutputBuffer=0xe54c7fe618, OutputBufferLength=0xa0, ReturnLength=0xe54c7fe610 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe54c7fe668, InputBufferLength=0x18,
OutputBuffer=0xe54c7fe680, OutputBufferLength=0x78, ReturnLength=0xe54c7fe660 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7fe878, InputBufferLength=0xa0,
OutputBuffer=0xe54c7fe878, OutputBufferLength=0xa0, ReturnLength=0xe54c7fe870 [0xa0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xe54c7fe620 [0x70]) =>
0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0xc [TokenSessionId],
TokenInformation=0xe54c7fdf40, Length=4, ReturnLength=0xe54c7fdf20 [4]) => 0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0xe54c7fdf88, Length=4, ReturnLength=0xe54c7fdf20 [4]) => 0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0x2a
[TokenPrivateNameSpace], TokenInformation=0xe54c7fdf24, Length=4, ReturnLength=0xe54c7fdf20
[4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0xe54c7fdf48 [0x80], DesiredAccess=0xf,
ObjectAttributes="\Sessions\15\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x70, TokenInformationClass=0x2c [TokenBnoIsolation],
TokenInformation=0xe54c7fe240, Length=0x120, ReturnLength=0xe54c7fdf20 [0x10]) => 0

NtClose(Handle=0x70) => 0

NtCreateMutant(MutantHandle=0xe54c7fe678 [0x84],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x80:"Local\SM0:288048:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x84, Alertable=false, Timeout=null) => 0

```
NtOpenSemaphore(SemaphoreHandle=0xe54c7fe438,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x80:"Local\SM0:288048:304:WilStaging_02_p0") => 0xc0000034 [2 '=x єфрхЄё
эрщєш єьрчрээ√щ Їрщы.']

NtCreateSemaphore(SemaphoreHandle=0xe54c7fe398 [0x88],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x80:"Local\SM0:288048:304:WilStaging_02_p0", InitialCount=0x205bdcd4,
MaxCount=0x205bdcd4) => 0

NtCreateSemaphore(SemaphoreHandle=0xe54c7fe398 [0x5c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x80:"Local\SM0:288048:304:WilStaging_02_p0h", InitialCount=0x100,
MaxCount=0x100) => 0

NtReleaseMutant(MutantHandle=0x84, PreviousCount=null) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7fe858, InputBufferLength=0xa0,
OutputBuffer=0xe54c7fe858, OutputBufferLength=0xa0, ReturnLength=0xe54c7fe850 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe54c7fe8a8, InputBufferLength=0x18,
OutputBuffer=0xe54c7fe8c0, OutputBufferLength=0x78, ReturnLength=0xe54c7fe8a0 [0]) => 0

NtQueryWnfStateData(StateName=0xe54c7fe740 [0xa3bc0875], TypeId=0xe54c7fe7e8,
ExplicitScope=null, ChangeStamp=0xe54c7fe734 [1], Buffer=0xe54c7fd730,
BufferSize=0xe54c7fe730 [8]) => 0

NtCreateEvent(EventHandle=0xe54c7fe6b0 [0x90],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x200816f7b20 [0x94],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x90) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x94, IoCompletionHandle=0x14,
TargetObjectHandle=0x90, KeyContext=0x200816f7b38, ApcContext=0x200816f79b0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xe54c7fe630 [0x816f0c00]) => 0

NtSubscribeWnfStateChange(StateName=0x200816f7cb0 [0xa3bc0875], ChangeStamp=1,
EventMask=0x11, SubscriptionId=0xe54c7fe720 [0x0002c32d]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0xe54c7fe5a0 [0], Alignment=0x18,
SystemInformation=0xe54c7fe5c0, Length=0x50, ReturnLength=null) => 0

NtMapViewOfSection(SectionHandle=0x98, ProcessHandle=-1, BaseAddress=0xe54c7fe530
[0x0000020081690000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe54c7fe540
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x9c, ProcessHandle=-1, BaseAddress=0xe54c7fe530
[0x00000200816a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe54c7fe540
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0xa0, ProcessHandle=-1, BaseAddress=0xe54c7fe530
[0x00000200816b0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe54c7fe540
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0x98) => 0
```

```
NtClose(Handle=0x9c) => 0

NtClose(Handle=0xa0) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fd1f0 [0x00000200816f8000],
ZeroBits=0, pSize=0xe54c7fd298 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtSetTimer2(TimerHandle=0x1c, DueTime=0xe54c7fe6b0 [-3e+09], Period=null,
Parameters=0xe54c7fe6b8) => 0

NtOpenKey(KeyHandle=0xe54c7fe850, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\Redirec
tionMap\Keys") => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7fe858, InputBufferLength=0xa0,
OutputBuffer=0xe54c7fe858, OutputBufferLength=0xa0, ReturnLength=0xe54c7fe850 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe54c7fe8a8, InputBufferLength=0x18,
OutputBuffer=0xe54c7fe8c0, OutputBufferLength=0x78, ReturnLength=0xe54c7fe8a0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe54c7fe888, InputBufferLength=0xa0,
OutputBuffer=0xe54c7fe888, OutputBufferLength=0xa0, ReturnLength=0xe54c7fe880 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe54c7fe8d8, InputBufferLength=0x18,
OutputBuffer=0xe54c7fe8f0, OutputBufferLength=0x78, ReturnLength=0xe54c7fe8d0 [0]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe7a0 [0x00007ffd04d2b000],
Size=0xe54c7fe798 [0x4000], NewProtect=4, OldProtect=0xe54c7fe790 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe7a0 [0x00007ffd04d2b000],
Size=0xe54c7fe798 [0x4000], NewProtect=2, OldProtect=0xe54c7fe790 [4]) => 0

NtOpenKey(KeyHandle=0xe54c7fe770, DesiredAccess=0x9, ObjectAttributes=0x18:"lab2.exe") =>
0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xe54c7fe828 [0xa0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0

NtQueryValueKey(KeyHandle=0xa0, ValueName="TSAppCompat", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x200816f8860, Length=0x224,
ResultLength=0xe54c7fe818) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xa0, ValueName="TSUserEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x200816f8860, Length=0x224,
ResultLength=0xe54c7fe818 [0x10]) => 0

NtClose(Handle=0xa0) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffd02fa9a80, Length=0x40, ReturnLength=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=4, OldProtect=0xe54c7fe938 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe928 [0x00007ffd026e7000],
Size=0xe54c7fe920 [0x1000], NewProtect=2, OldProtect=0xe54c7fe938 [4]) => 0

NtOpenKey(KeyHandle=0xe54c7feef0, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '=x єфрх€ё  эрщ€ш єърчрээ√щ Їрщы.']
```

```
NtOpenKey(KeyHandle=0xe54c7feed0 [0xac], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0

NtQueryKey(KeyHandle=0xac, KeyInformationClass=2 [KeyFullInformation],
KeyInformation=0xe54c7fef48, Length=0x30, ResultLength=0xe54c7feec0 [0x2c]) => 0

NtClose(Handle=0xac) => 0

NtOpenKey(KeyHandle=0xe54c7feec8 [0xac], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0

NtQueryValueKey(KeyHandle=0xac, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe54c7fef80, Length=0x50,
ResultLength=0xe54c7feec0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш еърчрээ√щ Їрщы.']

NtClose(Handle=0xac) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xe54c7fedf0, Length=0x58, ReturnLength=0xe54c7fede8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xe54c7feec8, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-
21-3512441621-816733789-498939024-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '=x єфрхЄё
эрщЄш еърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xe54c7fefa0 [0x9c], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x9c, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe54c7fefe0, Length=0x14,
ResultLength=0xe54c7fefa8 [0x10]) => 0

NtClose(Handle=0x9c) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xe54c7fef30 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0xe54c7fef28) => 0xc0000004 [24 '¬ышэр
т√фрээющ яЁюуЁрьыющ ъьюрэф√ ёыш°ъьь тхышэр.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xe54c7fef30 [6], Alignment=4,
SystemInformation=0x200816f5bc0, Length=0x30, ReturnLength=0xe54c7fef28 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x200816f5790 [0xac],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x200816f5788 [0xa0],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0xac, WorkerProcessHandle=-1, StartRoutine=0x7ffd04bc5580,
StartParameter=0x200816f5750, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0xe54c7fefd8, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x200816f57e0 [0x58], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0
```

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x200816f57e8 [0xb0],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xb0, IoCompletionHandle=0xac,
TargetObjectHandle=0x58, KeyContext=0x200816f57f0, ApcContext=0x200816f57c0, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0xe54c7feef0 [0]) => 0

NtCreateTimer2(TimerHandle=0x200816f5858 [0x9c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x20000000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x200816f5860 [0xb4],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xb4, IoCompletionHandle=0xac,
TargetObjectHandle=0x9c, KeyContext=0x200816f5868, ApcContext=0x200816f57c0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xe54c7feef0 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=2
[WorkerFactoryIdleTimeout], Buffer=0xe54c7fefd8, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0xe54c7fefd8, BufferLength=4) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0xe54c7ff050) => 0xc000007c [1008 '⌐юя√Єьр ёё√ыьш эр эхёє·хёЄтє■·шщ Єюъхэ.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fefd0 [0x00007ff6dbbc9000],
Size=0xe54c7fefd8 [0x1000], NewProtect=4, OldProtect=0xe54c7ff320 [8]) => 0

NtOpenSection(SectionHandle=0xe54c7fe9c8 [0xb8], DesiredAccess=0xd,
ObjectAttributes=0x48:"msvcrt.dll") => 0

Loaded DLL at 00007FFD03280000 C:\WINDOWS\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xb8, ProcessHandle=-1, BaseAddress=0x200816f8890
[0x00007ffd03280000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x200816f5a08
[0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0xe54c7fe820 [7.42868e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe830 [0x00007ffd04d2b000],
Size=0xe54c7fe828 [0x4000], NewProtect=4, OldProtect=0xe54c7fe820 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe830 [0x00007ffd04d2b000],
Size=0xe54c7fe828 [0x4000], NewProtect=2, OldProtect=0xe54c7fe820 [4]) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0xe54c7fe2e0, Length=0x330, ReturnLength=0xe54c7fe298) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0xe54c7fe2e0, Length=0x330, ReturnLength=0xe54c7fe298) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd03280000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0xe54c7fe558, Length=0x30, ReturnLength=null)
=> 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7fe870 [0x00007ffd032fe000],
Size=0xe54c7fe878 [0x1000], NewProtect=4, OldProtect=0x200816f59f0 [2]) => 0

NtClose(Handle=0xb8) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe54c7ff300 [0x00007ff6dbbc9000],
Size=0xe54c7ff308 [0x1000], NewProtect=8, OldProtect=0xe54c7fedd0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x200816f59d0 [0x00007ffd032fe000],
Size=0x200816f59d8 [0x1000], NewProtect=2, OldProtect=0xe54c7fedd0 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0xe54c7fed30, Length=0x28) => 0

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

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

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11
[ThreadHideFromDebugger], ThreadInformation=0xe54c7ff050, Length=1, ReturnLength=null) => 0

Initial breakpoint

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xe54c7fefc0 [0x98]) =>
0

NtQueryInformationToken(TokenHandle=0x98, TokenInformationClass=0xa [TokenStatistics],
TokenInformation=0xe54c7fefd0, Length=0x38, ReturnLength=0xe54c7fefc8 [0x38]) => 0

NtClose(Handle=0x98) => 0

NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode",
Type=0xe54c7febcc [4], Buffer=0xe54c7febc0, Length=4, ReturnedLength=0xe54c7febc4 [4]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe760 [0x00000200817f0000],
ZeroBits=0, pSize=0xe54c7fe768 [0x00140000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe760 [0x00000200817f0000],
pSize=0xe54c7fe758 [0x00130000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe748 [0x0000020081920000],
ZeroBits=0, pSize=0xe54c7fe740 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0xe54c7fed10 [0/8],
FsInformation=0xe54c7fed30, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x68, IoStatusBlock=0xe54c7fed10 [0/8],
FsInformation=0xe54c7fed30, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x6c, IoStatusBlock=0xe54c7fed10 [0/8],
FsInformation=0xe54c7fed30, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe570 [0x00000200816f9000],
ZeroBits=0, pSize=0xe54c7fe618 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe520 [0x0000020081922000],
ZeroBits=0, pSize=0xe54c7fe5c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenKey(KeyHandle=0xe54c7fda50 [0x98], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions")
=> 0

```
NtQueryValueKey(KeyHandle=0x98, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xe54c7fdf20, Length=0x214,
ResultLength=0xe54c7fded8 [0x2a]) => 0

NtQueryValueKey(KeyHandle=0x98, ValueName="000604xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xe54c7fdf00, Length=0x214,
ResultLength=0xe54c7fdcb8 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe54c7fe520 [0x0000020081923000],
ZeroBits=0, pSize=0xe54c7fe5c8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd0330ed28, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0xe54c7feb40, Length=0x18, ReturnLength=null) =>
0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtOpenKey(KeyHandle=0xe54c7ff050 [0xbc], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xbc, ValueName="SmtDelaySleepLoopWindowSize",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe54c7fefb0,
Length=0x50, ResultLength=0xe54c7fefa0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xbc, ValueName="SmtDelaySpinCountThreshold",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe54c7fefb0,
Length=0x50, ResultLength=0xe54c7fefa0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xbc, ValueName="SmtDelayBaseYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe54c7fefb0, Length=0x50,
ResultLength=0xe54c7fefa0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xbc, ValueName="SmtFactorYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe54c7fefb0, Length=0x50,
ResultLength=0xe54c7fefa0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xbc, ValueName="SmtDelayMaxYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe54c7fefb0, Length=0x50,
ResultLength=0xe54c7fefa0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xbc) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0xe54c7ff328, BufferLength=4) => 0

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

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6dbbc2b30, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0xe54c7ff870, Length=0x30,
ReturnLength=0xe54c7ff820 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6dbbc2b30, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0xe54c7ff8a0, Length=0x30, ReturnLength=null)
=> 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6dbbc2b30, MemoryInformationClass=2
[MemoryMappedFilenameInformation], MemoryInformation=0xe54c7ff918, Length=0x21a,
ReturnLength=null) => 0
```

395 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

213 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

239 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

440 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

938 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

161 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

729 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

942 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

830 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

199 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/2], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtCreateSemaphore(SemaphoreHandle=0xe54c7ff9c8 [0xc0], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, InitialCount=0xa, MaxCount=0xa) => 0

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xc4], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a, Argument=0x20081921850, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe54c7ff630) => 0

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

Created thread: 288056 at 00007FF6DBBC1D1A

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c9fefe0, IoControlCode=0x00500016, InputBuffer=0xe54c9feff0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xc8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a, Argument=0x20081921860, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe54c7ff630) => 0

Created thread: 288060 at 00007FF6DBBC1D1A

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

Created thread: 288064 at 00007FF6DBBC1D1A

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xbc], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a, Argument=0x20081921870, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe54c7ff630) => 0

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtTestAlert() => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54cbfed10, IoControlCode=0x00500016, InputBuffer=0xe54cbfed20, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

Created thread: 288068 at 00007FF6DBBC1D1A

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xcc], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a, Argument=0x20081921880, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe54c7ff630) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe54c9ffd68, Length=4, ReturnLength=null) => 0

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

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

NtAlertThreadByThreadId(ThreadId=0x00046540) => 0

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xb8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a, Argument=0x20081921890, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe54c7ff630) => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739 'ERROR_ALERTED']

Created thread: 288072 at 00007FF6DBBC1D1A

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtAlertThreadByThreadId(ThreadId=0x00046540) => 0

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

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739 'ERROR_ALERTED']

<mark>NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xd0], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a, Argument=0x200819218a0, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe54c7ff630) => 0</mark>

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtTestAlert() => 0

Created thread: 288076 at 00007FF6DBBC1D1A

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtAlertThreadByThreadId(ThreadId=0x00046540) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54cffedf0, IoControlCode=0x00500016, InputBuffer=0xe54cffee00, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739 'ERROR_ALERTED']

NtAlertThreadByThreadId(ThreadId=0x00046538) => 0

<mark>NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xd4], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a, Argument=0x200819218b0, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe54c7ff630) => 0</mark>

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739 'ERROR_ALERTED']

Created thread: 288080 at 00007FF6DBBC1D1A

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe54cbffa98, Length=4, ReturnLength=null) => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739 'ERROR_ALERTED']

NtAlertThreadByThreadId(ThreadId=0x00046544) => 0

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xd8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff,
ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a,
Argument=0x200819218c0, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0,
AttributeList=0xe54c7ff630) => 0

Created thread: 288084 at 00007FF6DBBC1D1A

Thread 288056 exit code: 0

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtAlertThreadByThreadId(ThreadId=0x00046544) => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtAlertThreadByThreadId(ThreadId=0x0004654c) => 0

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

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtAlertThreadByThreadId(ThreadId=0x00046548) => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0x70],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff,
ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a,
Argument=0x200819218d0, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0,
AttributeList=0xe54c7ff630) => 0

Created thread: 288088 at 00007FF6DBBC1D1A

NtAlertThreadByThreadId(ThreadId=0x00046544) => 0

NtWaitForSingleObject(Handle=0xc0, Alertable=false, Timeout=null) => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtAlertThreadByThreadId(ThreadId=0x00046540) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtCreateThreadEx(ThreadHandle=0xe54c7ff518 [0xdc],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff,
ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6dbbc1d1a,
Argument=0x200819218e0, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0,
AttributeList=0xe54c7ff630) => 0

Created thread: 288092 at 00007FF6DBBC1D1A

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

NtTestAlert() => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtAlertThreadByThreadId(ThreadId=0x00046548) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54cdfebd0, IoControlCode=0x00500016, InputBuffer=0xe54cdfebe0,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю сърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtAlertThreadByThreadId(ThreadId=0x00046554) => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread],
ThreadInformation=0xe54cfffb78, Length=4, ReturnLength=null) => 0

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739
'ERROR_ALERTED']

NtAlertThreadByThreadId(ThreadId=0x0004655c) => 0

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

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54d1fecd0, IoControlCode=0x00500016, InputBuffer=0xe54d1fece0,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю сърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtTestAlert() => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread],
ThreadInformation=0xe54cdff958, Length=4, ReturnLength=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

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

NtTestAlert() => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread],
ThreadInformation=0xe54d1ffa58, Length=4, ReturnLength=null) => 0

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

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

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

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

Thread 288060 exit code: 0

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

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

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

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54d3fef20, IoControlCode=0x00500016, InputBuffer=0xe54d3fef30,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

Thread 288064 exit code: 0

Thread 288072 exit code: 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

Thread 288068 exit code: 0

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

NtTestAlert() => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread],
ThreadInformation=0xe54d3ffca8, Length=4, ReturnLength=null) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54d5fed30, IoControlCode=0x00500016, InputBuffer=0xe54d5fed40,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtTestAlert() => 0

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

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

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

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread],
ThreadInformation=0xe54d5ffab8, Length=4, ReturnLength=null) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54d7fee50, IoControlCode=0x00500016, InputBuffer=0xe54d7fee60,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

Thread 288076 exit code: 0

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

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtTestAlert() => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe54d7ffbd8, Length=4, ReturnLength=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

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

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

NtAlertThreadByThreadId(ThreadId=0x00046554) => 0

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c9fed80, IoControlCode=0x00500016, InputBuffer=0xe54c9fed90, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

NtWaitForAlertByThreadId(Handle=0x00000200816f02c8, Timeout=null) => 0x101 [739 'ERROR_ALERTED']

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

Thread 288080 exit code: 0

NtTestAlert() => 0

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

NtDeviceIoControlFile(FileHandle=0x78, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54d9fed40, IoControlCode=0x00500016, InputBuffer=0xe54d9fed50, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x эрщфхэю єърчрээюх шь ёшёЄхьэюую ёхьрЇюЁр.']

Thread 288084 exit code: 0

NtAlertThreadByThreadId(ThreadId=0x00046558) => 0

NtWaitForAlertByThreadId(Handle=0x00000200819202c8, Timeout=null) => 0x101 [739 'ERROR_ALERTED']

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtTestAlert() => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe54d9ffac8, Length=4, ReturnLength=null) => 0

NtReleaseSemaphore(SemaphoreHandle=0xc0, Count=1, PreviousCount=null) => 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe54c9ffb08, Length=4, ReturnLength=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

NtSetEvent(EventHandle=0x4c, PrevState=null) => 0

Thread 288088 exit code: 0

Thread 288092 exit code: 0

NtWaitForMultipleObjects(Count=0xa, Handles=0x200819217d0 [0xc4], WaitType=0 [WaitAll], Alertable=false, Timeout=null) => 0

161 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

199 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

213 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

239 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

395 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

440 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

729 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

830 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

938 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

942 NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/4], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe54c7ff420 [0/1], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtClose(Handle=0xc0) => 0

NtClose(Handle=0xc4) => 0

NtClose(Handle=0xc8) => 0

NtClose(Handle=0xbc) => 0

NtClose(Handle=0xcc) => 0

NtClose(Handle=0xb8) => 0

```
NtClose(Handle=0xd0) => 0

NtClose(Handle=0xd4) => 0

NtClose(Handle=0xd8) => 0

NtClose(Handle=0x70) => 0

NtClose(Handle=0xdc) => 0

Sorting completed successfully

NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xe54c7ff420 [0/0x1f], IoControlCode=0x00500016, InputBuffer=0xe54c7ff430,
InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

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

NtClose(Handle=0x60) => 0

NtClose(Handle=0xa4) => 0

NtClose(Handle=0xa8) => 0

NtQueryWnfStateData(StateName=0xe54c7ff600 [0xa3bc1c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0xe54c7fe54c [0x0001bcb7], Buffer=0xe54c7fe5a0, BufferSize=0xe54c7fe548 [0x914])
=> 0

NtClose(Handle=0x8c) => 0

NtClose(Handle=0x7c) => 0

Process 288048 exit code: 0
```

Вывод

Задание интересное, в этот раз проблем не возникло, почти все легко и быстро нашел. Единственной проблемой была передача чанков нестандратного размера.

Число потоков	Время исполнения (мс)	Ускорение	Эффективность
1	1000	1	1
2	550	1,818181818	0,909090909
4	300	3,333333333	0,833333333
8	200	5	0,625
16	150	6,666666667	0,416666667