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-213Б-23

Студент: Черников В. В.

Преподаватель: Бахарев В.Д.

Оценка: ____________________

Дата: 11.11.24

Москва, 2024

Постановка задачи

Вариант 15.

Есть колода из 52 карт, рассчитать экспериментально (метод Монте-Карло) вероятность того, что сверху лежат две одинаковых карты. Количество раундов задаётся ключом программы.

Общий метод и алгоритм решения

Использованные системные вызовы:

- CreateThread() – создает новый поток выполнения в программе;
- WaitForMultipleObjects() – ожидает завершения одного или нескольких потоков;
- EnterCriticalSection() - вход в критическую секцию, обеспечивающую синхронизацию между потоками;
- LeaveCriticalSection() - выход из критической секции;
- InitializeCriticalSection() - инициализирует критическую секцию;
- DeleteCriticalSection() - удаляет объект критической секции после завершения его использования;
- CloseHandle() - закрывает дескриптор объекта (потока);
- GetStdHandle() - возвращает дескриптор стандартного вывода (консоли);
- WriteConsole() - отправляет данные в консоль.

Была создана многопоточная программа на языке C для вычисления вероятности совпадения двух верхних карт в случайно перемешанной колоде из 52 карт с использованием метода Монте-Карло. Программа работает в операционной системе Windows, применяя системные вызовы Windows API для создания потоков и их синхронизации.

Программа принимает на вход количество потоков и раундов симуляции, где каждый поток выполняет свою часть раундов. Для перемешивания колоды используется алгоритм Фишера-Йейтса, который гарантирует случайное распределение карт. В каждом раунде поток проверяет, совпадают ли две верхние карты после перемешивания. Если да, увеличивается локальный счетчик совпадений.

Для корректного обновления общего счетчика совпадений используется критическая секция: потоки поочередно получают доступ к глобальному счетчику, предотвращая конфликт данных. Завершив работу, программа собирает результаты всех потоков и вычисляет вероятность совпадений как отношение успешных раундов ко всем проведенным симуляциям. Результат выводится на экран через системный вызов WriteConsole.

Количество потоков	Количество раундов	Время выполнения (секунды)
1	1000	0.5
2	1000	0.3
4	1000	0.2

Код программы

main.c

```
#include <windows.h>
```

```
#include <stdlib.h>
#include <time.h>
#include <strsafe.h>

#define DECK_SIZE 52
#define MAX_THREADS 50

typedef struct {
    int trials;
    int matches;
} ThreadData;

CRITICAL_SECTION cs;

void shuffle_deck(int *deck) {
    for (int i = DECK_SIZE - 1; i > 0; i--) {
        int j = rand() % (i + 1);
        int temp = deck[i];
        deck[i] = deck[j];
        deck[j] = temp;
    }
}

int check_for_match(int *deck) {
    return deck[0] == deck[1];
}

void init_deck(int *deck) {
    for (int i = 0; i < DECK_SIZE; i++) {
        deck[i] = i % (DECK_SIZE / 4);
    }
}

void write_to_console(const char *str) {
    DWORD written;
    HANDLE hConsole = GetStdHandle(STD_OUTPUT_HANDLE);
    WriteConsole(hConsole, str, lstrlenA(str), &written, NULL);
}

DWORD WINAPI monte_carlo_thread(LPVOID lpParam) {
    ThreadData *data = (ThreadData*)lpParam;
    int deck[DECK_SIZE];
    int local_matches = 0;

    init_deck(deck);

    for (int i = 0; i < data->trials; i++) {
        shuffle_deck(deck);
        if (check_for_match(deck)) {
            local_matches++; // если первые две карты совпали
        }
    }

    EnterCriticalSection(&cs);
    data->matches += local_matches;
    LeaveCriticalSection(&cs);

    return 0;
}

int main(int argc, char *argv[]) {
    if (argc != 3) {
        write_to_console("Usage: program.exe <number_of_threads> <trials_per_thread>\n");
        return 1;
    }

    int num_threads = atoi(argv[1]);
    int trials_per_thread = atoi(argv[2]);

    if (num_threads > MAX_THREADS) {
        write_to_console("Too many threads, limiting to MAX_THREADS\n");
        num_threads = MAX_THREADS;
    }

    if (num_threads <= 0 || trials_per_thread <= 0) {
        write_to_console("Invalid arguments.\n");
        return 1;
    }

    InitializeCriticalSection(&cs);

    HANDLE *threads = (HANDLE*)malloc(num_threads * sizeof(HANDLE));
    ThreadData *thread_data = (ThreadData*)malloc(num_threads * sizeof(ThreadData));
    if (!threads || !thread_data) {
        write_to_console("Memory allocation failed.\n");
        return 1;
    }

    srand((unsigned int)time(NULL));

    int total_matches = 0;

    for (int i = 0; i < num_threads; i++) {
        thread_data[i].trials = trials_per_thread;
        thread_data[i].matches = 0;

        threads[i] = CreateThread(NULL, 0, monte_carlo_thread, &thread_data[i], 0,
NULL);

        if (threads[i] == NULL) {
            write_to_console("Error creating thread.\n");
            return 1;
        }
    }

    WaitForMultipleObjects(num_threads, threads, TRUE, INFINITE);
    for (int i = 0; i < num_threads; i++) {
        total_matches += thread_data[i].matches;
        CloseHandle(threads[i]);
    }

    double probability = (double)total_matches / (num_threads * trials_per_thread);

    char buffer[100];
    StringCchPrintfA(buffer, 100, "Probability of matching cards on top: %f\n", 
probability);
    write_to_console(buffer);

    free(threads);
    free(thread_data);
    DeleteCriticalSection(&cs);

    return 0;
}
```

Протокол работы программы

Тестирование:

```
fasti@fastixr MINGW64 /d/lab3
$ ./test.exe 1 100000
Probability of matching cards on top: 0.059330

fasti@fastixr MINGW64 /d/lab3
$ ./test.exe 4 1000000
Probability of matching cards on top: 0.058847

fasti@fastixr MINGW64 /d/lab3
$ ./test.exe 4 100
Probability of matching cards on top: 0.080000
```

Nttrace:

```
Process 8564 starting at 00007FF6B4FE13F0 with command line: "D:\lab3\test.exe 4 100"

D:\lab3\test.exe

Loaded DLL at 00007FFD7B7F0000 ntdll.dll

NtQueryPerformanceCounter(Counter=0xe651ff480 [9.58921e+12], Freq=null) => 0
```

```
        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651ff4c8 [0x00007ffd7b98e000],
Size=0xe651ff4c0 [0x1000], NewProtect=4, OldProtect=0xe651ff500 [8]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651ff4c8 [0x00007ffd7b98e000],
Size=0xe651ff4c0 [0x1000], NewProtect=8, OldProtect=0xe651ff500 [4]) => 0

        NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd7b894240, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0xe651ff450, Length=0x18, ReturnLength=null) => 0

        NtCreateEvent(EventHandle=0x7ffd7b976398 [8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

        NtManageHotPatch(Unknown=9, Unknown=0xe651ff2e8 [1], Unknown=8, Unknown=0xe651ff2e0) =>
0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

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

        NtCreateEvent(EventHandle=0x7ffd7b9763e8 [0xc],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

        NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xe651ff200, Length=0x40, ReturnLength=null) => 0

        NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0xe651feef8, Length=4, ReturnLength=null) => 0

        NtOpenKey(KeyHandle=0xe651feda8 [0x10], DesiredAccess=GENERIC_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\CodePage") => 0

        NtQueryValueKey(KeyHandle=0x10, ValueName="ACP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe651fee10, Length=0x24, ResultLength=0xe651feda0
[0x16]) => 0

        NtQueryValueKey(KeyHandle=0x10, ValueName="OEMCP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe651fee10, Length=0x24, ResultLength=0xe651feda0
[0x14]) => 0

        NtClose(Handle=0x10) => 0

        NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x7ffd7b9737e0 [0x00000161ff630000], SectionSize=null) => 0

        NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x7ffd7b9737e8 [0x00000161ff650000], SectionSize=null) => 0

        NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null, SectionPointer=0xe651fee98
[0x00000161ff670000], SectionSize=null) => 0

        NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0xe651fee50, Length=0x20, ReturnLength=null) => 0

        NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd7b7f0000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0xe651fede0, Length=0x18, ReturnLength=null) => 0

        NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0xe651fee20, Length=0x50, ReturnLength=null) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fee70 [0x00007ffd7b98b000],
Size=0xe651fee68 [0x4000], NewProtect=2, OldProtect=0xe651fee60 [4]) => 0

        NtOpenKey(KeyHandle=0xe651feb20 [0x14], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0
```

```
NtQueryValueKey(KeyHandle=0x14, ValueName="RaiseExceptionOnPossibleDeadlock", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe651feb30, Length=0x50, ResultLength=0xe651feb28) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x14) => 0

NtOpenKey(KeyHandle=0xe651feab8 [0x18], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options") => 0

NtOpenKey(KeyHandle=0xe651feba0, DesiredAccess=0x9, ObjectAttributes=0x18:"test.exe") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xe651feb00, DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0x7ffd7b977268, Length=4, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xe651fee08, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xe651fe7a0, Length=0x330, ReturnLength=0xe651fe758) => 0xc0000225 [1168 'ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xe651fe7a0, Length=0x330, ReturnLength=0xe651fe758) => 0xc0000225 [1168 'ыхьхэЄ эх эрщфхэ.']

NtOpenKey(KeyHandle=0xe651fed50 [0x1c], DesiredAccess=0x9, ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x1c, ValueName="ResourcePolicies", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe651fed90, Length=0x18, ResultLength=0xe651fed58) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x1c) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie], ProcessInformation=0xe651fee60, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xe651fee00, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation], SystemInformation=0xe651fee30, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffd7b977a88 [0x00007ff5743a0000], ZeroBits=0x0000000e651fedb0, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0xe651fecf8, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffd7b977a80 [0x00007ff5763a0000], ZeroBits=0x0000000e651fedb8, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null, DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffd7b977af0 [0x00007ff474380000], ZeroBits=0x0000000e651fed60, pSize=0x102000 [0], flAllocationType=4, DataBuffer=0xe651feca8, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0xe651feca0, Length=0x40, ReturnLength=null) => 0
```

```
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe880 [0x00000161ff680000], ZeroBits=0, pSize=0xe651fe888 [0x001c0000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe880 [0x00000161ff680000], pSize=0xe651fe878 [0x000c0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe868 [0x00000161ff740000], ZeroBits=0, pSize=0xe651fe860 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5 [SystemHypervisorSharedPageInformation], SystemInformation=0xe651ff000, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap], SystemInformation=0xe651fea70, Length=0x408, ReturnLength=0xe651fee90 [0x18]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xe651fea58 [4], Alignment=4, SystemInformation=null, Length=0, ReturnLength=0xe651fea50) => 0xc0000004 [24 '─ышэр т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xe651fea58 [4], Alignment=4, SystemInformation=0x161ff740880, Length=0x50, ReturnLength=0xe651fea50 [0x50]) => 0

NtCreateEvent(EventHandle=0xe651fec48 [0x1c], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x161ff740c40 [0x20], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xe651fe9c0 [6], Alignment=4, SystemInformation=null, Length=0, ReturnLength=0xe651fe9b8) => 0xc0000004 [24 '─ышэр т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xe651fe9c0 [6], Alignment=4, SystemInformation=0x161ff740ff0, Length=0x30, ReturnLength=0xe651fe9b8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x161ff740d20 [0x24], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x161ff740d18 [0x14], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null, CompletionPortHandle=0x24, WorkerProcessHandle=-1, StartRoutine=0x7ffd7b825580, StartParameter=0x161ff740ce0, MaxThreadCount=0x200, StackReserve=0x00200000, StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x161ff740d70 [0x28], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x161ff740d78 [0x10], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x10, IoCompletionHandle=0x24, TargetObjectHandle=0x28, KeyContext=0x161ff740d80, ApcContext=0x161ff740d50, IoStatus=0, IoStatusInformation=1, AlreadySignaled=0xe651fe980 [0]) => 0

NtCreateTimer2(TimerHandle=0x161ff740de8 [0x2c], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x16100000002) => 0
```

```
        NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x161ff740df0 [0x30],
DesiredAccess=0x1, ObjectAttributes=null) => 0

        NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x30, IoCompletionHandle=0x24,
TargetObjectHandle=0x2c, KeyContext=0x161ff740df8, ApcContext=0x161ff740d50, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xe651fe980 [0]) => 0

        NtSetInformationWorkerFactory(WorkerFactoryHandle=0x14, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0xe651fea68, BufferLength=4) => 0

        NtSetInformationWorkerFactory(WorkerFactoryHandle=0x14, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0xe651fea68, BufferLength=4) => 0

        NtSetInformationWorkerFactory(WorkerFactoryHandle=0x14, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0xe651feb88, BufferLength=4) => 0

        NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x20, IoCompletionHandle=0x24,
TargetObjectHandle=0x1c, KeyContext=0x161ff740c58, ApcContext=0x161ff740ad0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xe651febd0 [0xff740c00]) => 0

        NtTraceControl(CtrlCode=0x1b, InputBuffer=0xe651fec88, InputBufferLength=4, OutputBuffer=null,
OutputBufferLength=0, ReturnLength=0xe651fec40 [0]) => 0

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fece8, InputBufferLength=0xa0,
OutputBuffer=0xe651fece8, OutputBufferLength=0xa0, ReturnLength=0xe651fece0 [0xa0]) => 0

        NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe651fed38, InputBufferLength=0x18,
OutputBuffer=0xe651fed50, OutputBufferLength=0x78, ReturnLength=0xe651fed30 [0]) => 0

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fed38, InputBufferLength=0xa0,
OutputBuffer=0xe651fed38, OutputBufferLength=0xa0, ReturnLength=0xe651fed30 [0xa0]) => 0

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fed38, InputBufferLength=0xa0,
OutputBuffer=0xe651fed38, OutputBufferLength=0xa0, ReturnLength=0xe651fed30 [0xa0]) => 0

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fece8, InputBufferLength=0xa0,
OutputBuffer=0xe651fece8, OutputBufferLength=0xa0, ReturnLength=0xe651fece0 [0xa0]) => 0

        NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe651fed38, InputBufferLength=0x18,
OutputBuffer=0xe651fed50, OutputBufferLength=0x78, ReturnLength=0xe651fed30 [0]) => 0

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fed38, InputBufferLength=0xa0,
OutputBuffer=0xe651fed38, OutputBufferLength=0xa0, ReturnLength=0xe651fed30 [0xa0]) => 0

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe670 [0x00000161ff742000],
ZeroBits=0, pSize=0xe651fe718 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe670 [0x00000161ff744000],
ZeroBits=0, pSize=0xe651fe718 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

        NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fee90 [0x00000161ff5c0000],
pSize=0xe651fee98 [0x00020000], flFreeType=0x8000) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fee70 [0x00007ffd7b98b000],
Size=0xe651fee68 [0x4000], NewProtect=4, OldProtect=0xe651fee60 [2]) => 0

        NtOpenDirectoryObject(DirectoryHandle=0x7ffd7b98b2b0 [0x48], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fee70 [0x00007ffd7b98b000],
Size=0xe651fee68 [0x4000], NewProtect=2, OldProtect=0xe651fee60 [4]) => 0

        NtOpenSymbolicLinkObject(LinkHandle=0xe651fefe8 [0x4c], DesiredAccess=0x1,
ObjectAttributes=0x48:"KnownDllPath") => 0
```

```
        NtQuerySymbolicLinkObject(LinkHandle=0x4c, LinkTarget="C:\WINDOWS\System32",
ReturnedLength=0xe651fef80 [0x28]) => 0

        NtClose(Handle=0x4c) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fee40 [0x00007ffd7b98b000],
Size=0xe651fee38 [0x4000], NewProtect=4, OldProtect=0xe651fee30 [2]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fee70 [0x00007ffd7b98b000],
Size=0xe651fee68 [0x4000], NewProtect=2, OldProtect=0xe651fee60 [4]) => 0

        NtCreateEvent(EventHandle=0x7ffd7b9762d8 [0x4c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

        NtCreateEvent(EventHandle=0x7ffd7b976310 [0x50],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fedd0 [0x00007ffd7b98b000],
Size=0xe651fedc8 [0x4000], NewProtect=4, OldProtect=0xe651fedc0 [2]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fedd0 [0x00007ffd7b98b000],
Size=0xe651fedc8 [0x4000], NewProtect=2, OldProtect=0xe651fedc0 [4]) => 0

        NtOpenFile(FileHandle=0xe651fee78 [0x54], DesiredAccess=SYNCHRONIZE|0x20,
ObjectAttributes="\??\C:\Users\fasti\Downloads\NtTrace-main\NtTrace-main\", IoStatusBlock=0xe651fede8
[0/1], ShareAccess=3, OpenOptions=0x21) => 0

        NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xe651fede8 [0/8],
FsInformation=0xe651fedd0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

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

        NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0xe651feb40) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe2a0 [0x00000161ff745000],
ZeroBits=0, pSize=0xe651fe348 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

        NtOpenSection(SectionHandle=0xe651fead8 [0x58], DesiredAccess=0xd,
ObjectAttributes=0x48:"KERNEL32.DLL") => 0

        Loaded DLL at 00007FFD7AD30000 C:\WINDOWS\System32\KERNEL32.DLL

        NtMapViewOfSection(SectionHandle=0x58, ProcessHandle=-1, BaseAddress=0x161ff7450b0
[0x00007ffd7ad30000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x161ff745008
[0x000c4000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

        NtQueryPerformanceCounter(Counter=0xe651fe930 [9.58921e+12], Freq=null) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe8c0 [0x00007ffd7adf1000],
Size=0xe651fe8b8 [0x1000], NewProtect=2, OldProtect=0xe651fe8b0 [4]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe940 [0x00007ffd7b98b000],
Size=0xe651fe938 [0x4000], NewProtect=4, OldProtect=0xe651fe930 [2]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe940 [0x00007ffd7b98b000],
Size=0xe651fe938 [0x4000], NewProtect=2, OldProtect=0xe651fe930 [4]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe980 [0x00007ffd7adb3000],
Size=0xe651fe988 [0x4000], NewProtect=4, OldProtect=0x161ff744ff0 [2]) => 0

        NtOpenSection(SectionHandle=0xe651fe378 [0x5c], DesiredAccess=0xd,
ObjectAttributes=0x48:"KERNELBASE.dll") => 0
```

```
        Loaded DLL at 00007FFD78AF0000 C:\WINDOWS\System32\KERNELBASE.dll

        NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x161ff7457f0
[0x00007ffd78af0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x161ff745748
[0x003b9000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

        NtQueryPerformanceCounter(Counter=0xe651fe1d0 [9.58921e+12], Freq=null) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe160 [0x00007ffd78e77000],
Size=0xe651fe158 [0x1000], NewProtect=2, OldProtect=0xe651fe150 [4]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe1e0 [0x00007ffd7b98b000],
Size=0xe651fe1d8 [0x4000], NewProtect=4, OldProtect=0xe651fe1d0 [2]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe1e0 [0x00007ffd7b98b000],
Size=0xe651fe1d8 [0x4000], NewProtect=2, OldProtect=0xe651fe1d0 [4]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe220 [0x00007ffd78d5f000],
Size=0xe651fe228 [0x2000], NewProtect=4, OldProtect=0x161ff745730 [2]) => 0

        NtClose(Handle=0x5c) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x161ff744fd0 [0x00007ffd7adb3000],
Size=0x161ff744fd8 [0x4000], NewProtect=2, OldProtect=0xe651fe780 [4]) => 0

        NtClose(Handle=0x58) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x161ff745710 [0x00007ffd78d5f000],
Size=0x161ff745718 [0x2000], NewProtect=2, OldProtect=0xe651fe8c0 [4]) => 0

        NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation],
ProcessInformation=0xe651fe820, Length=0x28) => 0

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

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

        NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0xe651fe600, Length=8, ReturnLength=null) => 0

        NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffd78e58ec0, Length=0x40, ReturnLength=null) => 0

        NtOpenSection(SectionHandle=0xe651fe3c0 [0x58], DesiredAccess=0x4,
ObjectAttributes="\Sessions\2\Windows\SharedSection") => 0

        NtCreateSection(SectionHandle=0xe651fe3e0 [0x60],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0xe651fe3d0 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

        NtConnectPort(PortHandle=0x7ffd7b976c08 [0x5c], PortName="\Sessions\2\Windows\ApiPort",
SecurityQos=0xe651fe500, ClientView=0xe651fe3f8, ServerView=0xe651fe428, MaxMsgLength=0xe651fe3f0
[0x3b8], ConnectionInfo=0xe651fe470, ConnectionInfoLength=0xe651fe3c8 [0x30]) => 0

        NtClose(Handle=0x60) => 0

        NtMapViewOfSection(SectionHandle=0x58, ProcessHandle=-1, BaseAddress=0xe651fe3d8
[0x00007ff474280000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe651fe3e8 [0x00100000],
InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

        NtClose(Handle=0x58) => 0

        NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x161ff5c0000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0xe651fe0c0, Length=0x30, ReturnLength=null) => 0
```

```
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fdd80 [0x00000161ff746000], ZeroBits=0, pSize=0xe651fde28 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null, SectionPointer=0xe651fe5a8 [0x00000161ff5d0000], SectionSize=null) => 0

NtInitializeNlsFiles(BaseAddress=0xe651fe5a0 [0x00000161ff840000], DefaultLocaleId=0x7ffd78e5abb8 [0x419], DefaultCasingTableSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null, SectionPointer=0xe651fe580 [0x00000161ff680000], SectionSize=0xe651fe548 [0x00011000]) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null, SectionPointer=0xe651fe580 [0x00000161ff6a0000], SectionSize=0xe651fe548 [0x00011000]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fd720 [0x00000161ff747000], ZeroBits=0, pSize=0xe651fd7c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateFile(FileHandle=0xe651fe608 [0x58], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f, ObjectAttributes=4:"\Connect", IoStatusBlock=0xe651fdfc0 [0/0x18], AllocationSize=null, FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20, EaBuffer=0x161ff746c80, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe651fe550 [0/0], IoControlCode=0x00500023, InputBuffer=null, InputBufferLength=0, OutputBuffer=0xe651fe570, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31 [ProcessOwnerInformation], ProcessInformation=0xe651fe578, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe651fe340, IoControlCode=0x00500016, InputBuffer=0xe651fe350, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '═х эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fe458, InputBufferLength=0xa0, OutputBuffer=0xe651fe458, OutputBufferLength=0xa0, ReturnLength=0xe651fe450 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe651fe4a8, InputBufferLength=0x18, OutputBuffer=0xe651fe4c0, OutputBufferLength=0x78, ReturnLength=0xe651fe4a0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fe6b8, InputBufferLength=0xa0, OutputBuffer=0xe651fe6b8, OutputBufferLength=0xa0, ReturnLength=0xe651fe6b0 [0xa0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xe651fe460 [0x78]) => 0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0xc [TokenSessionId], TokenInformation=0xe651fdd80, Length=4, ReturnLength=0xe651fdd60 [4]) => 0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x1d [TokenIsAppContainer], TokenInformation=0xe651fddc8, Length=4, ReturnLength=0xe651fdd60 [4]) => 0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x2a [TokenPrivateNameSpace], TokenInformation=0xe651fdd64, Length=4, ReturnLength=0xe651fdd60 [4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0xe651fdd88 [0x7c], DesiredAccess=0xf, ObjectAttributes="\Sessions\2\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x2c [TokenBnoIsolation], TokenInformation=0xe651fe080, Length=0x120, ReturnLength=0xe651fdd60 [0x10]) => 0

NtClose(Handle=0x78) => 0
```

```
        NtCreateMutant(MutantHandle=0xe651fe4b8 [0x78],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x7c:"Local\SM0:8564:304:WilStaging_02", InitialOwner=false) => 0

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

        NtOpenSemaphore(SemaphoreHandle=0xe651fe278,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"Local\SM0:8564:304:WilStaging_02_p0") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш
єърчрээ√щ Їрщы.']

        NtCreateSemaphore(SemaphoreHandle=0xe651fe1d8 [0x80],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"Local\SM0:8564:304:WilStaging_02_p0", InitialCount=0x7fdd1bb8,
MaxCount=0x7fdd1bb8) => 0

        NtCreateSemaphore(SemaphoreHandle=0xe651fe1d8 [0x60],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"Local\SM0:8564:304:WilStaging_02_p0h", InitialCount=0xb0, MaxCount=0xb0) => 0

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

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fe698, InputBufferLength=0xa0,
OutputBuffer=0xe651fe698, OutputBufferLength=0xa0, ReturnLength=0xe651fe690 [0xa0]) => 0

        NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe651fe6e8, InputBufferLength=0x18,
OutputBuffer=0xe651fe700, OutputBufferLength=0x78, ReturnLength=0xe651fe6e0 [0]) => 0

        NtQueryWnfStateData(StateName=0xe651fe580 [0xa3bc0875], TypeId=0xe651fe628, ExplicitScope=null,
ChangeStamp=0xe651fe574 [1], Buffer=0xe651fd570, BufferSize=0xe651fe570 [8]) => 0

        NtCreateEvent(EventHandle=0xe651fe4f0 [0x88],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

        NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x161ff7476b0 [0x8c],
DesiredAccess=0x1, ObjectAttributes=null) => 0

        NtSetWnfProcessNotificationEvent(NotificationEvent=0x88) => 0

        NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x8c, IoCompletionHandle=0x24,
TargetObjectHandle=0x88, KeyContext=0x161ff7476c8, ApcContext=0x161ff747540, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xe651fe470 [0xff740c00]) => 0

        NtSubscribeWnfStateChange(StateName=0x161ff747840 [0xa3bc0875], ChangeStamp=1,
EventMask=0x11, SubscriptionId=0xe651fe560 [0x000191d1]) => 0

        NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0xe651fe3e0 [0], Alignment=0x18,
SystemInformation=0xe651fe400, Length=0x50, ReturnLength=null) => 0

        NtMapViewOfSection(SectionHandle=0x90, ProcessHandle=-1, BaseAddress=0xe651fe370
[0x00000161ff6c0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe651fe380 [0x3000],
InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

        NtMapViewOfSection(SectionHandle=0x94, ProcessHandle=-1, BaseAddress=0xe651fe370
[0x00000161ff6d0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe651fe380 [0x3000],
InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

        NtMapViewOfSection(SectionHandle=0x98, ProcessHandle=-1, BaseAddress=0xe651fe370
[0x00000161ff6e0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xe651fe380 [0x1000],
InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

        NtClose(Handle=0x90) => 0
        NtClose(Handle=0x94) => 0

        NtClose(Handle=0x98) => 0

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fdda0 [0x00000161ff748000],
ZeroBits=0, pSize=0xe651fde48 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

        NtSetTimer2(TimerHandle=0x2c, DueTime=0xe651fe4f0 [-3e+09], Period=null, Parameters=0xe651fe4f8)
=> 0

        NtOpenKey(KeyHandle=0xe651fe690, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys")
=> 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Ïрщы.']

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fe698, InputBufferLength=0xa0,
OutputBuffer=0xe651fe698, OutputBufferLength=0xa0, ReturnLength=0xe651fe690 [0xa0]) => 0

        NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe651fe6e8, InputBufferLength=0x18,
OutputBuffer=0xe651fe700, OutputBufferLength=0x78, ReturnLength=0xe651fe6e0 [0]) => 0

        NtTraceControl(CtrlCode=0xf, InputBuffer=0xe651fe6c8, InputBufferLength=0xa0,
OutputBuffer=0xe651fe6c8, OutputBufferLength=0xa0, ReturnLength=0xe651fe6c0 [0xa0]) => 0

        NtTraceControl(CtrlCode=0x1e, InputBuffer=0xe651fe718, InputBufferLength=0x18,
OutputBuffer=0xe651fe730, OutputBufferLength=0x78, ReturnLength=0xe651fe710 [0]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe5e0 [0x00007ffd7b98b000],
Size=0xe651fe5d8 [0x4000], NewProtect=4, OldProtect=0xe651fe5d0 [2]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe5e0 [0x00007ffd7b98b000],
Size=0xe651fe5d8 [0x4000], NewProtect=2, OldProtect=0xe651fe5d0 [4]) => 0

        NtOpenKey(KeyHandle=0xe651fe5b0, DesiredAccess=0x9, ObjectAttributes=0x18:"test.exe") =>
0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Ïрщы.']

        NtOpenKey(KeyHandle=0xe651fe668 [0x94], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0

        NtQueryValueKey(KeyHandle=0x94, ValueName="TSAppCompat", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x161ff7483f0, Length=0x224,
ResultLength=0xe651fe658) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Ïрщы.']

        NtQueryValueKey(KeyHandle=0x94, ValueName="TSUserEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x161ff7483f0, Length=0x224,
ResultLength=0xe651fe658 [0x10]) => 0

        NtClose(Handle=0x94) => 0

        NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffd7ade9a80, Length=0x40, ReturnLength=null) => 0

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

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000],
Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000],
Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000],
Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

        NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000],
Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=4, OldProtect=0xe651fe778 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe768 [0x00007ffd78e77000], Size=0xe651fe760 [0x1000], NewProtect=2, OldProtect=0xe651fe778 [4]) => 0

NtOpenKey(KeyHandle=0xe651fed30, DesiredAccess=0x3, ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") => 0xc0000034 [2 '═x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xe651fed10, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0xc0000034 [2 '═x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xe651fed08 [0x94], DesiredAccess=0x1, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0
```

```
NtQueryValueKey(KeyHandle=0x94, ValueName="TransparentEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe651fedc0, Length=0x50, ResultLength=0xe651fed00) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x94) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0xe651fec30, Length=0x58, ReturnLength=0xe651fec28 [0x2c]) => 0

NtOpenKey(KeyHandle=0xe651fed08, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2409479645-3338554513-3479048774-1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0xe651fede0 [0x90], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x90, ValueName="LongPathsEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe651fee20, Length=0x14, ResultLength=0xe651fede8 [0x10]) => 0

NtClose(Handle=0x90) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xe651fed70 [6], Alignment=4, SystemInformation=null, Length=0, ReturnLength=0xe651fed68) => 0xc0000004 [24 '─ышэр т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b [SystemLogicalProcessorAndGroupInformation], QueryType=0xe651fed70 [6], Alignment=4, SystemInformation=0x161ff745760, Length=0x30, ReturnLength=0xe651fed68 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x161ff745330 [0x94], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3, ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x161ff745328 [0x90], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null, CompletionPortHandle=0x94, WorkerProcessHandle=-1, StartRoutine=0x7ffd7b825580, StartParameter=0x161ff7452f0, MaxThreadCount=0x200, StackReserve=0x00200000, StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x90, InformationClass=0xd [WorkerFactoryFlags], Buffer=0xe651fee18, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x161ff745380 [0xa0], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x161ff745388 [0xa4], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xa4, IoCompletionHandle=0x94, TargetObjectHandle=0xa0, KeyContext=0x161ff745390, ApcContext=0x161ff745360, IoStatus=0, IoStatusInformation=1, AlreadySignaled=0xe651fed30 [0]) => 0

NtCreateTimer2(TimerHandle=0x161ff7453f8 [0xa8], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x16100000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x161ff745400 [0xac], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xac, IoCompletionHandle=0x94, TargetObjectHandle=0xa8, KeyContext=0x161ff745408, ApcContext=0x161ff745360, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0xe651fed30 [0]) => 0
```

```
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x90, InformationClass=2 [WorkerFactoryIdleTimeout], Buffer=0xe651fee18, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x90, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0xe651fee18, BufferLength=4) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0xe651fee90) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fee10 [0x00007ff6b4fec000], Size=0xe651fee18 [0x1000], NewProtect=4, OldProtect=0xe651ff160 [8]) => 0

NtOpenSection(SectionHandle=0xe651fe808 [0xb0], DesiredAccess=0xd, ObjectAttributes=0x48:"ucrtbase.dll") => 0

Loaded DLL at 00007FFD791F0000 C:\WINDOWS\System32\ucrtbase.dll

NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x161ff748420 [0x00007ffd791f0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x161ff7455a8 [0x00111000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xe651fe660 [9.58921e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe670 [0x00007ffd7b98b000], Size=0xe651fe668 [0x4000], NewProtect=4, OldProtect=0xe651fe660 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe670 [0x00007ffd7b98b000], Size=0xe651fe668 [0x4000], NewProtect=2, OldProtect=0xe651fe660 [4]) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xe651fe120, Length=0x330, ReturnLength=0xe651fe0d8) => 0xc0000225 [1168 'ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xe651fe120, Length=0x330, ReturnLength=0xe651fe0d8) => 0xc0000225 [1168 'ыхьхэЄ эх эрщфхэ.']

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd791f0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xe651fe398, Length=0x30, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe6b0 [0x00007ffd792b8000], Size=0xe651fe6b8 [0x1000], NewProtect=4, OldProtect=0x161ff745590 [2]) => 0

NtClose(Handle=0xb0) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651ff140 [0x00007ff6b4fec000], Size=0xe651ff148 [0x1000], NewProtect=8, OldProtect=0xe651fec10 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x161ff745570 [0x00007ffd792b8000], Size=0x161ff745578 [0x1000], NewProtect=2, OldProtect=0xe651fec10 [4]) => 0

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

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

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11 [ThreadHideFromDebugger], ThreadInformation=0xe651fee90, Length=1, ReturnLength=null) => 0

Initial breakpoint

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

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xe651fee00 [0xb0]) => 0
```

```
        NtQueryInformationToken(TokenHandle=0xb0, TokenInformationClass=0xa [TokenStatistics],
TokenInformation=0xe651fee10, Length=0x38, ReturnLength=0xe651fee08 [0x38]) => 0

        NtClose(Handle=0xb0) => 0

        NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode",
Type=0xe651fea0c [4], Buffer=0xe651fea00, Length=4, ReturnedLength=0xe651fea04 [4]) => 0

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe3a0 [0x00000161ff749000],
ZeroBits=0, pSize=0xe651fe448 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe320 [0x00000161ff74a000],
ZeroBits=0, pSize=0xe651fe3c8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

        NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0xe651feb70 [0/8],
FsInformation=0xe651feb90, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

        NtQueryVolumeInformationFile(FileHandle=0x68, IoStatusBlock=0xe651feb70 [0/8],
FsInformation=0xe651feb90, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

        NtQueryVolumeInformationFile(FileHandle=0x6c, IoStatusBlock=0xe651feb70 [0/8],
FsInformation=0xe651feb90, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

        NtOpenKey(KeyHandle=0xe651fd550 [0xb0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions") => 0

        NtQueryValueKey(KeyHandle=0xb0, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xe651fda20, Length=0x214, ResultLength=0xe651fd9d8
[0x2a]) => 0

        NtQueryValueKey(KeyHandle=0xb0, ValueName="000604xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xe651fda00, Length=0x214, ResultLength=0xe651fd7b8
[0x42]) => 0

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe320 [0x00000161ff74c000],
ZeroBits=0, pSize=0xe651fe3c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

        NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe370 [0x00000161ff74d000],
ZeroBits=0, pSize=0xe651fe418 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

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

        NtOpenKey(KeyHandle=0xe651fee90 [0xb4], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

        NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelaySleepLoopWindowSize",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe651fedf0, Length=0x50,
ResultLength=0xe651fede0) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelaySpinCountThreshold",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xe651fedf0, Length=0x50,
ResultLength=0xe651fede0) => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelayBaseYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe651fedf0, Length=0x50, ResultLength=0xe651fede0)
=> 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtFactorYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe651fedf0, Length=0x50, ResultLength=0xe651fede0)
=> 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

        NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelayMaxYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xe651fedf0, Length=0x50, ResultLength=0xe651fede0)
=> 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
```

```
NtClose(Handle=0xb4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x90, InformationClass=3 [WorkerFactoryBindingCount], Buffer=0xe651ff168, BufferLength=4) => 0

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

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6b4fe2200, MemoryInformationClass=0 [MemoryBasicInformation], MemoryInformation=0xe651ff6b0, Length=0x30, ReturnLength=0xe651ff660 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6b4fe2200, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xe651ff6e0, Length=0x30, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6b4fe2200, MemoryInformationClass=2 [MemoryMappedFilenameInformation], MemoryInformation=0xe651ff758, Length=0x21a, ReturnLength=null) => 0

NtCreateThreadEx(ThreadHandle=0xe651ff308 [0xb4], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6b4fe15f2, Argument=0x161ff7485e0, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe651ff420) => 0

Created thread: 9368 at 00007FF6B4FE15F2

NtCreateThreadEx(ThreadHandle=0xe651ff308 [0xb8], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6b4fe15f2, Argument=0x161ff7485e8, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe651ff420) => 0

Created thread: 32164 at 00007FF6B4FE15F2

NtCreateThreadEx(ThreadHandle=0xe651ff308 [0xbc], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6b4fe15f2, Argument=0x161ff7485f0, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe651ff420) => 0

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

Created thread: 33672 at 00007FF6B4FE15F2

NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe653fe9d0, IoControlCode=0x00500016, InputBuffer=0xe653fe9e0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '═х эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']

NtCreateThreadEx(ThreadHandle=0xe651ff308 [0xc0], DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0xffff, ObjectAttributes=null, ProcessHandle=-1, StartRoutine=0x7ff6b4fe15f2, Argument=0x161ff7485f8, CreateFlags=0, ZeroBits=0, StackSize=0, MaximumStackSize=0, AttributeList=0xe651ff420) => 0

Created thread: 14136 at 00007FF6B4FE15F2

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

NtTestAlert() => 0

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

NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe655fe9c0, IoControlCode=0x00500016, InputBuffer=0xe655fe9d0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '═х эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']
```

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

NtTestAlert() => 0

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

NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe657feab0, IoControlCode=0x00500016, InputBuffer=0xe657feac0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '═х эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe657fe6e0 [0x00000161ff74f000], ZeroBits=0, pSize=0xe657fe788 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

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

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

NtTestAlert() => 0

NtDeviceIoControlFile(FileHandle=0x58, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe659fec90, IoControlCode=0x00500016, InputBuffer=0xe659feca0, InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '═х эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe653ff758, Length=4, ReturnLength=null) => 0

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

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

NtTestAlert() => 0

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

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe655ff748, Length=4, ReturnLength=null) => 0

Thread 9368 exit code: 0

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

Thread 32164 exit code: 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe657ff838, Length=4, ReturnLength=null) => 0

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

Thread 33672 exit code: 0

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0xc [ThreadAmILastThread], ThreadInformation=0xe659ffa18, Length=4, ReturnLength=null) => 0

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

Thread 14136 exit code: 0

NtWaitForMultipleObjects(Count=4, Handles=0x161ff745600 [0xb4], WaitType=0 [WaitAll], Alertable=false, Timeout=null) => 0

NtClose(Handle=0xb4) => 0

NtClose(Handle=0xb8) => 0
NtClose(Handle=0xbc) => 0

NtClose(Handle=0xc0) => 0

Probability of matching cards on top: 0.080000

NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xe651ff670 [0/0x2f], IoControlCode=0x00500016, InputBuffer=0xe651ff680, InputBufferLength=0x40, OutputBuffer=null, OutputBufferLength=0) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false, TokenHandle=0xe651ff4e0) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

NtOpenSection(SectionHandle=0xe651ff478, DesiredAccess=0xd, ObjectAttributes=0x48:"kernel.appcore.dll") => 0xc0000034 [2 '═х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryAttributesFile(ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", Attributes=0xe651ff238 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0xe651ff240 [0xb8], DesiredAccess=SYNCHRONIZE|0x21, ObjectAttributes="\??\C:\WINDOWS\SYSTEM32\kernel.appcore.dll", IoStatusBlock=0xe651ff2a8 [0/1], ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xe651ff248 [0xb4], DesiredAccess=0xd, ObjectAttributes=null, SectionSize=null, Protect=0x10, Attributes=0x01000000, FileHandle=0xb8) => 0

Loaded DLL at 00007FFD77B90000 C:\WINDOWS\SYSTEM32\kernel.appcore.dll

NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x161ff74bc30 [0x00007ffd77b90000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x161ff74bb58 [0x00018000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xe651ff0c0 [9.58921e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651ff050 [0x00007ffd77ba5000], Size=0xe651ff048 [0x1000], NewProtect=2, OldProtect=0xe651ff040 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651ff0d0 [0x00007ffd7b98b000], Size=0xe651ff0c8 [0x4000], NewProtect=4, OldProtect=0xe651ff0c0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651ff0d0 [0x00007ffd7b98b000], Size=0xe651ff0c8 [0x4000], NewProtect=2, OldProtect=0xe651ff0c0 [4]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd77b90000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xe651fedf8, Length=0x30, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651ff110 [0x00007ffd77b9a000], Size=0xe651ff118 [0x2000], NewProtect=4, OldProtect=0x161ff74bb40 [2]) => 0

NtOpenSection(SectionHandle=0xe651feb08 [0xc4], DesiredAccess=0xd, ObjectAttributes=0x48:"msvcrt.dll") => 0

Loaded DLL at 00007FFD7AFA0000 C:\WINDOWS\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xc4, ProcessHandle=-1, BaseAddress=0x161ff74bf90 [0x00007ffd7afa0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x161ff74bef8 [0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xe651fe960 [9.58921e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe970 [0x00007ffd7b98b000], Size=0xe651fe968 [0x4000], NewProtect=4, OldProtect=0xe651fe960 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe970 [0x00007ffd7b98b000], Size=0xe651fe968 [0x4000], NewProtect=2, OldProtect=0xe651fe960 [4]) => 0
```

```
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffd7afa0000, MemoryInformationClass=3 [MemoryRegionInformation], MemoryInformation=0xe651fe698, Length=0x30, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xe651fe9b0 [0x00007ffd7b01e000], Size=0xe651fe9b8 [0x1000], NewProtect=4, OldProtect=0x161ff74bee0 [2]) => 0

NtClose(Handle=0xc4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x161ff74bb20 [0x00007ffd77b9a000], Size=0x161ff74bb28 [0x2000], NewProtect=2, OldProtect=0xe651fef10 [4]) => 0

NtClose(Handle=0xb4) => 0

NtClose(Handle=0xb8) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x161ff74bec0 [0x00007ffd7b01e000], Size=0x161ff74bec8 [0x1000], NewProtect=2, OldProtect=0xe651ff260 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23 [ProcessTlsInformation], ProcessInformation=0xe651ff1c0, Length=0x28) => 0

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

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

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651febb0 [0x00000161ff6f0000], ZeroBits=0, pSize=0xe651febb8 [0x00030000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xe651febb0 [0x00000161ff6f0000], pSize=0xe651feba8 [0x00020000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651feb98 [0x00000161ff710000], ZeroBits=0, pSize=0xe651feb90 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0xe651ff160 [0/8], FsInformation=0xe651ff180, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x68, IoStatusBlock=0xe651ff160 [0/8], FsInformation=0xe651ff180, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x6c, IoStatusBlock=0xe651ff160 [0/8], FsInformation=0xe651ff180, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe970 [0x00000161ff712000], ZeroBits=0, pSize=0xe651fea18 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xe651fe970 [0x00000161ff713000], ZeroBits=0, pSize=0xe651fea18 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

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

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xe651ff480, Length=0x330, ReturnLength=0xe651ff438) => 0xc0000225 [1168 'ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xe651ff480, Length=0x330, ReturnLength=0xe651ff438) => 0xc0000225 [1168 'ыхьхэЄ эх эрщфхэ.']

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

NtClose(Handle=0x70) => 0

NtClose(Handle=0x9c) => 0
NtClose(Handle=0x98) => 0

NtQueryWnfStateData(StateName=0xe651ff450 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xe651fe39c [0x9b94], Buffer=0xe651fe3f0, BufferSize=0xe651fe398 [0x59c]) => 0

NtClose(Handle=0x84) => 0

NtClose(Handle=0x74) => 0

Process 8564 exit code:
```

Вывод

В ходе лабораторной работы была успешно создана многопоточная программа на языке С для вычисления вероятности совпадения двух верхних карт в колоде методом Монте-Карло. Программа корректно использует системные вызовы Windows API для создания и синхронизации потоков, а алгоритм Фишера-Йейтса обеспечивает эффективное перемешивание карт. Итоговый результат — вероятность совпадения карт — выводится в консоль, демонстрируя правильную работу многопоточной обработки данных.