

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

Лабораторная работа № 1 по курсу
«Операционные системы»

Группа: М8О-214Б-23

Студент: Шестаков К. Р.

Преподаватель: Бахарев В.Д.

Оценка: _____

Дата: 25.10.24

Москва, 2024

Постановка задачи

Вариант 2.

Родительский процесс создает дочерний процесс. Первой строчкой пользователь в консоль родительского процесса пишет имя файла, которое будет передано при создании дочернего процесса. Родительский и дочерний процесс должны быть представлены разными программами. Родительский процесс передает команды пользователя через pipe1, который связан с стандартным входным потоком дочернего процесса. Дочерний процесс при необходимости передает данные в родительский процесс через pipe2. Результаты своей работы дочерний процесс пишет в созданный им файл. Допускается просто открыть файл и писать туда, не перенаправляя стандартный поток вывода.

Пользователь вводит команды вида: «число число число<endline>». Далее эти числа передаются от родительского процесса в дочерний. Дочерний процесс считает их сумму и выводит её в файл. Числа имеют тип float. Количество чисел может быть произвольным.

Общий метод и алгоритм решения

Использованные системные вызовы:

- CreateProcess(): Создание дочернего процесса.
- CreatePipe(): Создание безымянного канала (pipe) для взаимодействия между процессами.
- ReadFile(): Чтение данных из канала или консоли.
- WriteFile(): Запись данных в канал или файл.
- CloseHandle(): Закрытие handle'а объекта (канала, файла, процесса).
- WaitForSingleObject(): Ожидание завершения дочернего процесса.
- GetExitCodeProcess(): Получение кода завершения дочернего процесса.
- CreateFile(): Создание или открытие файла.
- GetStdHandle(): Получение handle'а стандартных потоков (stdin, stdout, stderr).

1. Родительский процесс:

- Читает имя файла из консоли.
- Создает pipe для связи с дочерним процессом.
- Создает дочерний процесс, передавая ему имя файла через аргументы командной строки и перенаправляя stdin/stdout на pipe.
- Читает строки чисел из консоли и передает их в pipe.
- Ожидает завершения дочернего процесса.
- Выводит код завершения дочернего процесса.

2. Дочерний процесс:

- Получает имя файла из аргументов командной строки.
- Открывает файл для записи.
- Читает строки чисел из pipe (stdin).
- Рассчитывает сумму чисел в каждой строке.
- Записывает сумму в файл.
- Закрывает файл.

Код программы

parent.c

```
#include <windows.h>

#define BUFFER_SIZE 1024

int main()
{
    HANDLE pipe_read, pipe_write;
    SECURITY_ATTRIBUTES sa = {sizeof(SECURITY_ATTRIBUTES), NULL, TRUE};
    STARTUPINFO si;
    PROCESS_INFORMATION pi;
    char buffer[BUFFER_SIZE];
    char filename[MAX_PATH];
    DWORD bytes_read, bytes_written;

    // Создаем pipe
    if (!CreatePipe(&pipe_read, &pipe_write, &sa, 0))
    {
        WriteFile(GetStdHandle(STD_ERROR_HANDLE), "Failed to create pipe\n", 20,
&bytes_written, NULL);
        return 1;
    }

    // Читаем имя файла
    if (!ReadFile(GetStdHandle(STD_INPUT_HANDLE), filename, sizeof(filename), &bytes_read,
NULL))
    {
        CloseHandle(pipe_read);
        CloseHandle(pipe_write);
        return 1;
    }

    // Обработка CRLF
    if (bytes_read >= 2 && filename[bytes_read - 2] == '\\r' && filename[bytes_read - 1] ==
'\\n')
    {
        filename[bytes_read - 2] = '\\0'; // Убираем \\r и \\n
    }
    else if (bytes_read >= 1 && (filename[bytes_read - 1] == '\\n' || filename[bytes_read -
1] == '\\r'))
    {
        filename[bytes_read - 1] = '\\0'; // Убираем одиночный символ переноса строки
    }
    else
    {
        filename[bytes_read] = '\\0';
    }

    // Получаем полный путь к файлу
    char full_path[MAX_PATH];
    DWORD result = GetFullPathName(filename, MAX_PATH, full_path, NULL);
```

```

if (result == 0 || result > MAX_PATH)
{
    WriteFile(GetStdHandle(STD_ERROR_HANDLE), "Failed to get full path\n", 22,
&bytes_written, NULL);
    CloseHandle(pipe_read);
    CloseHandle(pipe_write);
    return 1;
}

// Подготавливаем структуры для создания процесса
ZeroMemory(&si, sizeof(STARTUPINFO));
si.cb = sizeof(STARTUPINFO);
si.hStdInput = pipe_read;
si.hStdOutput = GetStdHandle(STD_OUTPUT_HANDLE);
si.hStdError = GetStdHandle(STD_ERROR_HANDLE);
si.dwFlags |= STARTF_USESTDHANDLES;

// Формируем командную строку
char cmd_line[MAX_PATH * 2];
wsprintf(cmd_line, "child.exe \"%s\"", full_path);

// Получаем путь к текущей директории
char module_dir[MAX_PATH];
GetModuleFileName(NULL, module_dir, MAX_PATH);
char *last_slash = strrchr(module_dir, '\\');
if (last_slash)
    *last_slash = '\\0';

// Создаем дочерний процесс
if (!CreateProcess(NULL, cmd_line, NULL, NULL, TRUE, 0, NULL, module_dir, &si, &pi))
{
    DWORD error = GetLastError();
    char error_msg[256];
    wsprintf(error_msg, "Failed to create process. Error: %d\n", error);
    WriteFile(GetStdHandle(STD_ERROR_HANDLE), error_msg, lstrlen(error_msg),
&bytes_written, NULL);
    CloseHandle(pipe_read);
    CloseHandle(pipe_write);
    return 1;
}

CloseHandle(pipe_read);
CloseHandle(pi.hThread);

// Читаем ввод пользователя и отправляем в pipe
while (ReadFile(GetStdHandle(STD_INPUT_HANDLE), buffer, BUFFER_SIZE, &bytes_read,
NULL) && bytes_read > 0)
{
    if (!WriteFile(pipe_write, buffer, bytes_read, &bytes_written, NULL))
        break;
}

CloseHandle(pipe_write);
WaitForSingleObject(pi.hProcess, INFINITE);

```

```

    DWORD exit_code;
    GetExitCodeProcess(pi.hProcess, &exit_code);
    CloseHandle(pi.hProcess);

    return exit_code;
}

```

child.c

```

#include <windows.h>

#define BUFFER_SIZE 1024

float string_to_float(const char *str)
{
    float result = 0;
    float fraction = 0;
    float div = 1;
    int negative = 0;

    while (*str == ' ')
        str++;

    if (*str == '-')
    {
        negative = 1;
        str++;
    }

    while (*str >= '0' && *str <= '9')
    {
        result = result * 10 + (*str - '0');
        str++;
    }

    if (*str == '.')
    {
        str++;
        while (*str >= '0' && *str <= '9')
        {
            div *= 10;
            fraction = fraction * 10 + (*str - '0');
            str++;
        }
    }

    result += fraction / div;
    return negative ? -result : result;
}

void float_to_string(float num, char *str)
{
    int integer_part = (int)num;

```

```

float decimal_part = num - integer_part;
int idx = 0;
int temp;

if (num < 0)
{
    str[idx++] = '-';
    integer_part = -integer_part;
    decimal_part = -decimal_part;
}

temp = integer_part;
int start_idx = idx;
do
{
    str[idx++] = '0' + (temp % 10);
    temp /= 10;
} while (temp > 0);

int end_idx = idx - 1;
while (start_idx < end_idx)
{
    char t = str[start_idx];
    str[start_idx] = str[end_idx];
    str[end_idx] = t;
    start_idx++;
    end_idx--;
}

str[idx++] = '.';
decimal_part *= 100;
temp = (int)decimal_part;
str[idx++] = '0' + (temp / 10);
str[idx++] = '0' + (temp % 10);
str[idx++] = '\n';
str[idx] = '\0';
}

// Функция для проверки и исправления пути
BOOL validate_and_fix_path(char *path)
{
    // Удаляем начальные и конечные кавычки
    int len = strlen(path);
    if (len > 0)
    {
        if (path[0] == '"')
        {
            memmove(path, path + 1, len);
            len--;
        }
        if (len > 0 && path[len - 1] == '"')
        {
            path[len - 1] = '\0';
            len--;
        }
    }
}

```

```

    }
}

// Проверяем базовую валидность пути
if (len == 0 || len >= MAX_PATH)
    return FALSE;

// Проверяем на недопустимые символы
for (int i = 0; i < len; i++)
{
    if (path[i] < 32 || strchr("<>|?*\\\"", path[i]))
        return FALSE;
}

return TRUE;
}

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

    if (argc != 2)
    {
        WriteFile(GetStdHandle(STD_ERROR_HANDLE), "Invalid arguments\n", 17,
&bytes_written, NULL);
        return 1;
    }

    char file_path[MAX_PATH];
    lstrcpy(file_path, argv[1]);

    // Проверяем и исправляем путь
    if (!validate_and_fix_path(file_path))
    {
        WriteFile(GetStdHandle(STD_ERROR_HANDLE), "Invalid file path\n", 17,
&bytes_written, NULL);
        return 1;
    }

    // Создаем или перезаписываем файл
    HANDLE output_file = CreateFile(
        file_path,
        GENERIC_WRITE,
        0,
        NULL,
        CREATE_ALWAYS,
        FILE_ATTRIBUTE_NORMAL,
        NULL);

    if (output_file == INVALID_HANDLE_VALUE)
    {
        DWORD error = GetLastError();
        char error_msg[256];
        wsprintf(error_msg, "Failed to create file '%s'. Error: %d\n", file_path, error);
    }
}

```

```

        WriteFile(GetStdHandle(STD_ERROR_HANDLE), error_msg, lstrlen(error_msg),
&bytes_written, NULL);
        return 1;
    }

    char buffer[BUFFER_SIZE];
    char num_str[32];
    float sum;
    int num_start = 0;
    DWORD bytes_read;

    while (ReadFile(GetStdHandle(STD_INPUT_HANDLE), buffer, BUFFER_SIZE, &bytes_read,
NULL) && bytes_read > 0)
    {
        sum = 0;
        num_start = 0;

        for (int i = 0; i < bytes_read; i++)
        {
            if (buffer[i] == ' ' || buffer[i] == '\n')
            {
                if (i > num_start)
                {
                    int len = i - num_start;
                    if (len < sizeof(num_str))
                    {
                        memcpy(num_str, buffer + num_start, len);
                        num_str[len] = '\0';
                        sum += string_to_float(num_str);
                    }
                }
                num_start = i + 1;

                if (buffer[i] == '\n')
                {
                    char result[64];
                    float_to_string(sum, result);
                    if (!WriteFile(output_file, result, lstrlen(result), &bytes_written,
NULL))
                    {
                        WriteFile(GetStdHandle(STD_ERROR_HANDLE), "Failed to write to
file\n", 22, &bytes_written, NULL);
                        CloseHandle(output_file);
                        return 1;
                    }
                    sum = 0;
                }
            }
        }
    }

    CloseHandle(output_file);
    return 0;
}

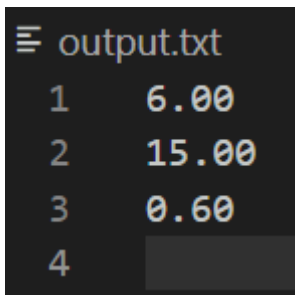
```


Протокол работы программы

Тестирование:

```
D:\code\osi>gcc child.c -o child.exe  
D:\code\osi>gcc parent.c -o parent.exe  
D:\code\osi>NtTrace D:\code\osi\parent.exe > trace.log  
output.txt  
1 2 3  
4 5 6  
0.1 0.2 0.3
```

(Скриншот консоли родительского процесса)



output.txt	
1	6.00
2	15.00
3	0.60
4	

(Содержимое файла output.txt)

nttrace:

NtCreateUserProcess

NtCreateNamedPipeFile

Process 8420 starting at 00007FF7324A13F0 with command line: "D:\code\osi\parent.exe"

D:\code\osi\parent.exe

Loaded DLL at 00007FF81B930000 C:\Windows\SYSTEM32\ntdll.dll

NtQueryPerformanceCounter(Counter=0xa3131ff940 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff988 [0x00007ff81bab4000], Size=0xa3131ff980 [0x1000], NewProtect=4, OldProtect=0xa3131ff9c0 [8]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff988 [0x00007ff81bab4000], Size=0xa3131ff980 [0x1000], NewProtect=8, OldProtect=0xa3131ff9c0 [4]) => 0

NtCreateEvent(EventHandle=0x7ff81ba9c478 [8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xa3131ff8f0, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0xa3131ff618, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0xa3131ff4f0, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81b930000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0xa3131ff400, Length=0x18, ReturnLength=null) =>
0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0xa3131ff4c0, Length=0x50,
ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff510 [0x00007ff81bab1000],
Size=0xa3131ff508 [0x4000], NewProtect=2, OldProtect=0xa3131ff500 [4]) => 0

NtOpenKey(KeyHandle=0xa3131fe150 [0xc], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xc, ValueName="RaiseExceptionOnPossibleDeadlock",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xa3131fe160,
Length=0x50, ResultLength=0xa3131fe158) => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtClose(Handle=0xc) => 0

NtOpenKey(KeyHandle=0xa3131fe0e8 [0x10], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options") => 0

NtOpenKey(KeyHandle=0xa3131fe1d0, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") =>
0xc0000034 [2 'Не удастся найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131fe130, DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager\Segment
Heap") => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x7ff81ba9d230, Length=4, ReturnLength=null) => 0

```

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0xa3131ff4a8, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0xa3131feee0, Length=0x330, ReturnLength=0xa3131fee98) =>
0xc0000225 [1168 'Элемент не найден.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0xa3131feee0, Length=0x330, ReturnLength=0xa3131fee98) =>
0xc0000225 [1168 'Элемент не найден.']

NtOpenKey(KeyHandle=0xa3131ff420 [0x14], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x14, ValueName="ResourcePolicies", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xa3131ff460, Length=0x18,
ResultLength=0xa3131ff428) => 0xc0000034 [2 'Не удается найти указанный файл.']

NtClose(Handle=0x14) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0xa3131ff500, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xa3131ff4a0, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation],
SystemInformation=0xa3131ff4d0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81ba9dc38 [0x00007ff506bc0000],
ZeroBits=0x000000a3131ff450, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0xa3131ff3b8, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81ba9dc30 [0x00007ff508bc0000],
ZeroBits=0x000000a3131ff458, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null,
DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81ba9dca0 [0x00007ff406ba0000],
ZeroBits=0x000000a3131ff400, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0xa3131ff368, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xa3131ff340, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fef00 [0x0000024026370000],
ZeroBits=0, pSize=0xa3131fef08 [0x00180000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fef00 [0x0000024026370000],
pSize=0xa3131feef8 [0x00080000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131feee8 [0x00000240263f0000],
ZeroBits=0, pSize=0xa3131feee0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5
[SystemHypervisorSharedPageInformation], SystemInformation=0xa3131ff6a8, Length=8,
ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap],
SystemInformation=0xa3131ff110, Length=0x408, ReturnLength=0xa3131ff530 [0x18]) => 0

```

```

NtCreateEvent(EventHandle=0xa3131ff348 [0x14],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x240263f0b20 [0x18],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xa3131ff0a0 [1], Alignment=4,
SystemInformation=0x240263f0ed0, Length=0x50, ReturnLength=0xa3131ff098 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x240263f0c00 [0x1c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=9) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x240263f0bf8 [0x20],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x1c, WorkerProcessHandle=-1, StartRoutine=0x7ff81b97d110,
StartParameter=0x240263f0bc0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x240263f0c50 [0x24], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x7ff800000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x240263f0c58 [0x28],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x28, IoCompletionHandle=0x1c,
TargetObjectHandle=0x24, KeyContext=0x240263f0c60, ApcContext=0x240263f0c30, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0xa3131ff060 [0]) => 0

NtCreateTimer2(TimerHandle=0x240263f0cc8 [0x2c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x24000000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x240263f0cd0 [0x30],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x30, IoCompletionHandle=0x1c,
TargetObjectHandle=0x2c, KeyContext=0x240263f0cd8, ApcContext=0x240263f0c30, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0xa3131ff060 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x20, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0xa3131ff168, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x20, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0xa3131ff168, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x20, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0xa3131ff288, BufferLength=4) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x18, IoCompletionHandle=0x1c,
TargetObjectHandle=0x14, KeyContext=0x240263f0b38, ApcContext=0x240263f09b0,
IoStatus=0x0000024000000000, IoStatusInformation=0, AlreadySignaled=0xa3131ff2d0
[0x263f0b00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0xa3131ff388, InputBufferLength=4,
OutputBuffer=null, OutputBufferLength=0, ReturnLength=0xa3131ff340 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131ff3e8, InputBufferLength=0xa0,
OutputBuffer=0xa3131ff3e8, OutputBufferLength=0xa0, ReturnLength=0xa3131ff3e0 [0xa0]) => 0

```

```

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131ff3e8, InputBufferLength=0xa0,
OutputBuffer=0xa3131ff3e8, OutputBufferLength=0xa0, ReturnLength=0xa3131ff3e0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131ff3e8, InputBufferLength=0xa0,
OutputBuffer=0xa3131ff3e8, OutputBufferLength=0xa0, ReturnLength=0xa3131ff3e0 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fed50 [0x00000240263f2000],
ZeroBits=0, pSize=0xa3131fedf8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131ff530 [0x0000024026310000],
pSize=0xa3131ff538 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff510 [0x00007ff81bab1000],
Size=0xa3131ff508 [0x4000], NewProtect=4, OldProtect=0xa3131ff500 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ff81bab1298 [0x40], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff510 [0x00007ff81bab1000],
Size=0xa3131ff508 [0x4000], NewProtect=2, OldProtect=0xa3131ff500 [4]) => 0

NtOpenSymbolicLinkObject(LinkHandle=0xa3131ff668 [0x44], DesiredAccess=0x1,
ObjectAttributes=0x40:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x44, LinkTarget="C:\Windows\System32",
ReturnedLength=0xa3131ff61c [0x28]) => 0

NtClose(Handle=0x44) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff4e0 [0x00007ff81bab1000],
Size=0xa3131ff4d8 [0x4000], NewProtect=4, OldProtect=0xa3131ff4d0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff510 [0x00007ff81bab1000],
Size=0xa3131ff508 [0x4000], NewProtect=2, OldProtect=0xa3131ff500 [4]) => 0

NtCreateEvent(EventHandle=0x7ff81ba9c380 [0x44],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ff81ba9c3b0 [0x48],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff470 [0x00007ff81bab1000],
Size=0xa3131ff468 [0x4000], NewProtect=4, OldProtect=0xa3131ff460 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff470 [0x00007ff81bab1000],
Size=0xa3131ff468 [0x4000], NewProtect=2, OldProtect=0xa3131ff460 [4]) => 0

NtOpenFile(FileHandle=0xa3131ff518 [0x4c], DesiredAccess=SYNCHRONIZE|0x20,
ObjectAttributes="???\D:\code\osi\", IoStatusBlock=0xa3131ff488 [0/1], ShareAccess=3,
OpenOptions=0x21) => 0

NtQueryVolumeInformationFile(FileHandle=0x4c, IoStatusBlock=0xa3131ff488 [0/8],
FsInformation=0xa3131ff470, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

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

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0xa3131ff1d0, Length=4) => 0

```

NtOpenSection(SectionHandle=0xa3131ff1a8 [0x50], DesiredAccess=0xd,
ObjectAttributes=0x40:"KERNEL32.DLL") => 0

Loaded DLL at 00007FF81A810000 C:\Windows\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x50, ProcessHandle=-1, BaseAddress=0x240263f3650
[0x00007ff81a810000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f35b0
[0x000c2000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0xa3131ff020 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff038 [0x00007ff81a8cf000],
Size=0xa3131ff030 [0x1000], NewProtect=2, OldProtect=0xa3131ff0a0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff030 [0x00007ff81bab1000],
Size=0xa3131ff028 [0x4000], NewProtect=4, OldProtect=0xa3131ff020 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff030 [0x00007ff81bab1000],
Size=0xa3131ff028 [0x4000], NewProtect=2, OldProtect=0xa3131ff020 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff080 [0x00007ff81a893000],
Size=0xa3131ff088 [0x4000], NewProtect=4, OldProtect=0x240263f3598 [2]) => 0

NtOpenSection(SectionHandle=0xa3131feb18 [0x60], DesiredAccess=0xd,
ObjectAttributes=0x40:"KERNELBASE.dll") => 0

Loaded DLL at 00007FF818FD0000 C:\Windows\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x60, ProcessHandle=-1, BaseAddress=0x240263f3d30
[0x00007ff818fd0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f3c90
[0x002fe000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0xa3131fe990 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe9a8 [0x00007ff8192a3000],
Size=0xa3131fe9a0 [0x1000], NewProtect=2, OldProtect=0xa3131fea10 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe9a0 [0x00007ff81bab1000],
Size=0xa3131fe998 [0x4000], NewProtect=4, OldProtect=0xa3131fe990 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe9a0 [0x00007ff81bab1000],
Size=0xa3131fe998 [0x4000], NewProtect=2, OldProtect=0xa3131fe990 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe9f0 [0x00007ff8191ba000],
Size=0xa3131fe9f8 [0x3000], NewProtect=4, OldProtect=0x240263f3c78 [2]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fdcd0 [0x00000240263f4000],
ZeroBits=0, pSize=0xa3131fdd78 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtClose(Handle=0x60) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f3578 [0x00007ff81a893000],
Size=0x240263f3580 [0x4000], NewProtect=2, OldProtect=0xa3131fef70 [4]) => 0

NtClose(Handle=0x50) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f3c58 [0x00007ff8191ba000],
Size=0x240263f3c60 [0x3000], NewProtect=2, OldProtect=0xa3131ff070 [4]) => 0

```

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0xa3131fefd0, Length=0x28) => 0

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

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff090, VmInformation=0xa3131ff168, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0xa3131fecf0, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ff81928ee60, Length=0x40, ReturnLength=null) => 0

NtOpenSection(SectionHandle=0xa3131feab0 [0x50], DesiredAccess=0x4,
ObjectAttributes="\Sessions\2\Windows\SharedSection") => 0

NtCreateSection(SectionHandle=0xa3131fead0 [0x64],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0xa3131feac0 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ff81ba9cc48 [0x60], PortName="\Sessions\2\Windows\ApiPort",
SecurityQos=0xa3131febfb0, ClientView=0xa3131feae8, ServerView=0xa3131feb18,
MaxMsgLength=0xa3131feae0 [0x3b8], ConnectionInfo=0xa3131feb60,
ConnectionInfoLength=0xa3131feab8 [0x30]) => 0

NtClose(Handle=0x64) => 0

NtMapViewOfSection(SectionHandle=0x50, ProcessHandle=-1, BaseAddress=0xa3131feac8
[0x00007ff406aa0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xa3131fead8
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x50) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x24026310000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0xa3131fe7a0, Length=0x30, ReturnLength=null) =>
0

NtInitializeNlsFiles(BaseAddress=0xa3131fec90 [0x00000240264f0000],
DefaultLocaleId=0x7ff8192908f0 [0x419], DefaultCasingTableSize=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fde50 [0x00000240263f5000],
ZeroBits=0, pSize=0xa3131fdef8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateFile(FileHandle=0xa3131fecf8 [0x50], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f,
ObjectAttributes=4:"\Connect", IoStatusBlock=0xa3131fe6b0 [0/0x18], AllocationSize=null,
FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20,
EaBuffer=0x240263f4ac0, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x50, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131fec40 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0xa3131fec60, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0xa3131fec68, Length=8) => 0

```

```

NtDeviceIoControlFile(FileHandle=0x50, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131fea30, IoControlCode=0x00500016, InputBuffer=0xa3131fea40,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 'Не
найденo указанное имя системного семафора.']]

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131feb58, InputBufferLength=0xa0,
OutputBuffer=0xa3131feb58, OutputBufferLength=0xa0, ReturnLength=0xa3131feb50 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131feb98, InputBufferLength=0x18,
OutputBuffer=0xa3131febb0, OutputBufferLength=0x78, ReturnLength=0xa3131feb90 [0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xa3131feb90 [0x68]) =>
0

NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0xc [TokenSessionId],
TokenInformation=0xa3131fe4b0, Length=4, ReturnLength=0xa3131fe490 [4]) => 0

NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0xa3131fe4f8, Length=4, ReturnLength=0xa3131fe490 [4]) => 0

NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0x2a
[TokenPrivateNameSpace], TokenInformation=0xa3131fe494, Length=4, ReturnLength=0xa3131fe490
[4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0xa3131fe4b8 [0x6c], DesiredAccess=0xf,
ObjectAttributes="\Sessions\2\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0x2c [TokenBnoIsolation],
TokenInformation=0xa3131fe7b0, Length=0x120, ReturnLength=0xa3131fe490 [0x10]) => 0

NtClose(Handle=0x68) => 0

NtCreateMutant(MutantHandle=0xa3131febe8 [0x68],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x6c:"Local\SM0:8420:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x68, Alertable=false, Timeout=null) => 0

NtOpenSemaphore(SemaphoreHandle=0xa3131fe9d8,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x6c:"Local\SM0:8420:304:WilStaging_02_p0") => 0xc0000034 [2 'Не удается
найти указанный файл.']]

NtCreateSemaphore(SemaphoreHandle=0xa3131fe8c8 [0x70],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x6c:"Local\SM0:8420:304:WilStaging_02_p0", InitialCount=0x098fd2fc,
MaxCount=0x098fd2fc) => 0

NtCreateSemaphore(SemaphoreHandle=0xa3131fe8c8 [0x74],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x6c:"Local\SM0:8420:304:WilStaging_02_p0h", InitialCount=0x120,
MaxCount=0x120) => 0

NtReleaseMutant(MutantHandle=0x68, PreviousCount=null) => 0

NtQueryWnfStateData(StateName=0xa3131fec40 [0xa3bc0875], TypeId=0xa3131fece8,
ExplicitScope=null, ChangeStamp=0xa3131fec34 [1], Buffer=0xa3131fdc30,
BufferSize=0xa3131fec30 [8]) => 0

```



```

NtCreateEvent(EventHandle=0xa3131feba0 [0x78],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x240263f5290 [0x7c],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x78) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x7c, IoCompletionHandle=0x1c,
TargetObjectHandle=0x78, KeyContext=0x240263f52a8, ApcContext=0x240263f5120,
IoStatus=0x0000024000000000, IoStatusInformation=0, AlreadySignaled=0xa3131feb20
[0x263f0b00]) => 0

NtSubscribeWnfStateChange(StateName=0x240263f5420 [0xa3bc0875], ChangeStamp=1,
EventMask=0x11, SubscriptionId=0xa3131fec10 [0xd75d]) => 0

NtQueryWnfStateData(StateName=0xa3131fed80 [0xa3bc7c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0xa3131fed78 [0], Buffer=null, BufferSize=0xa3131fed7c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x240263f5750 [0xa3bc7c75], ChangeStamp=0,
EventMask=0x11, SubscriptionId=0xa3131febf0 [0xd75e]) => 0

NtQueryWnfStateData(StateName=0xa3131fed80 [0xa3bc88f5], TypeId=null, ExplicitScope=null,
ChangeStamp=0xa3131fed78 [0], Buffer=null, BufferSize=0xa3131fed7c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x240263f5900 [0xa3bc88f5], ChangeStamp=0,
EventMask=0x11, SubscriptionId=0xa3131febf0 [0xd75f]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0xa3131feb30 [0], Alignment=0x18,
SystemInformation=0xa3131feb50, Length=0x50, ReturnLength=null) => 0

NtMapViewOfSection(SectionHandle=0xc, ProcessHandle=-1, BaseAddress=0xa3131feb00
[0x0000024026320000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xa3131feb08
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x80, ProcessHandle=-1, BaseAddress=0xa3131feb00
[0x0000024026370000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xa3131feb08
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x84, ProcessHandle=-1, BaseAddress=0xa3131feb00
[0x0000024026380000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xa3131feb08
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0xc) => 0

NtClose(Handle=0x80) => 0

NtClose(Handle=0x84) => 0

NtQueryWnfStateData(StateName=0xa3131feb38 [0xa3bc7c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0xa3131fecb8 [0], Buffer=0xa3131fec20, BufferSize=0xa3131feb20 [0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fe5b0 [0x00000240263f6000],
ZeroBits=0, pSize=0xa3131fe658 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtSetTimer2(TimerHandle=0x2c, DueTime=0xa3131febb0 [-3e+09], Period=null,
Parameters=0xa3131febb8) => 0

```

```
NtOpenKey(KeyHandle=0xa3131fed80, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\Redirect
tionMap\Keys") => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fed98, InputBufferLength=0xa0,
OutputBuffer=0xa3131fed98, OutputBufferLength=0xa0, ReturnLength=0xa3131fed90 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fedd8, InputBufferLength=0x18,
OutputBuffer=0xa3131fedf0, OutputBufferLength=0x78, ReturnLength=0xa3131fedd0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fedc8, InputBufferLength=0xa0,
OutputBuffer=0xa3131fedc8, OutputBufferLength=0xa0, ReturnLength=0xa3131fedc0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fee08, InputBufferLength=0x18,
OutputBuffer=0xa3131fee20, OutputBufferLength=0x78, ReturnLength=0xa3131fee00 [0]) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff0d0, VmInformation=0xa3131ffa8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fece0 [0x00007ff81bab1000],
Size=0xa3131fecd8 [0x4000], NewProtect=4, OldProtect=0xa3131fecd0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fece0 [0x00007ff81bab1000],
Size=0xa3131fecd8 [0x4000], NewProtect=2, OldProtect=0xa3131fecd0 [4]) => 0

NtOpenKey(KeyHandle=0xa3131fecb0, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") =>
0xc0000034 [2 'Не удастся найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131fed60 [0x90], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0

NtQueryValueKey(KeyHandle=0x90, ValueName="TSAppCompat", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x240263f6580, Length=0x224,
ResultLength=0xa3131fed58) => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtQueryValueKey(KeyHandle=0x90, ValueName="TSUserEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x240263f6580, Length=0x224,
ResultLength=0xa3131fed58 [0x10]) => 0

NtClose(Handle=0x90) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131febb8, InputBufferLength=0xa0,
OutputBuffer=0xa3131febb8, OutputBufferLength=0xa0, ReturnLength=0xa3131febb0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131febf8, InputBufferLength=0x18,
OutputBuffer=0xa3131fec10, OutputBufferLength=0x78, ReturnLength=0xa3131febf0 [0]) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ff81a8c7aa0, Length=0x40, ReturnLength=null) => 0

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

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0
```

```

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=4, OldProtect=0xa3131fedf8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff8192a3000],
Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fedf8 [4]) => 0

NtOpenKey(KeyHandle=0xa3131ff3d0, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131ff3b0, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131ff3a8 [0x94], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0

```

```

NtQueryValueKey(KeyHandle=0x94, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xa3131ff460, Length=0x50,
ResultLength=0xa3131ff3a0) => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtClose(Handle=0x94) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131ff2f0, Length=0x58, ReturnLength=0xa3131ff2e8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131ff3a8, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-
21-2308459876-1469942742-3350914452-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 'Не
удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131ff490 [0x94], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x94, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xa3131ff4d0, Length=0x14,
ResultLength=0xa3131ff498 [0x10]) => 0

NtClose(Handle=0x94) => 0

NtOpenKey(KeyHandle=0xa3131ff490 [0x94], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x94, ValueName="LPG0", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xa3131ff4d0, Length=0x14,
ResultLength=0xa3131ff498) => 0xc0000034 [2 'Не удастся найти указанный файл.']]

NtClose(Handle=0x94) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0xa3131ff470, Length=4) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0xa3131ff3f0 [1], Alignment=4,
SystemInformation=0x240263f3c70, Length=0x50, ReturnLength=0xa3131ff3e8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x240263f38b0 [0x94],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=9) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x240263f38a8 [0x84],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x94, WorkerProcessHandle=-1, StartRoutine=0x7ff81b97d110,
StartParameter=0x240263f3870, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x84, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0xa3131ff4b8, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x240263f3900 [0x80], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x240263f3908 [0x98],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x98, IoCompletionHandle=0x94,
TargetObjectHandle=0x80, KeyContext=0x240263f3910, ApcContext=0x240263f38e0, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0xa3131ff3b0 [0]) => 0

```

NtCreateTimer2(TimerHandle=0x240263f3978 [0x9c], Unknown1=null, ObjectAttributes=null, Attributes=8, DesiredAccess=SYNCHRONIZE|0x24000000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x240263f3980 [0xa0], DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xa0, IoCompletionHandle=0x94, TargetObjectHandle=0x9c, KeyContext=0x240263f3988, ApcContext=0x240263f38e0, IoStatus=0, IoStatusInformation=0, AlreadySignaled=0xa3131ff3b0 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x84, InformationClass=2 [WorkerFactoryIdleTimeout], Buffer=0xa3131ff4b8, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x84, InformationClass=5 [WorkerFactoryThreadMaximum], Buffer=0xa3131ff4b8, BufferLength=4) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=2, Buffer=0xa3131fef40, Length=0x330, ReturnLength=0xa3131feef8) => 0xc0000225 [1168 'Элемент не найден.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID", NumberOfAttributes=1, Buffer=0xa3131fef40, Length=0x330, ReturnLength=0xa3131feef8) => 0xc0000225 [1168 'Элемент не найден.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff4c0 [0x00007ff7324a8000], Size=0xa3131ff4c8 [0x1000], NewProtect=4, OldProtect=0xa3131ff858 [8]) => 0

NtOpenSection(SectionHandle=0xa3131fef58 [0xa4], DesiredAccess=0xd, ObjectAttributes=0x40:"msvcrt.dll") => 0

Loaded DLL at 00007FF81A640000 C:\Windows\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xa4, ProcessHandle=-1, BaseAddress=0x240263f66e0 [0x00007ff81a640000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f3b20 [0x0009e000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fedd0 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede0 [0x00007ff81bab1000], Size=0xa3131fedd8 [0x4000], NewProtect=4, OldProtect=0xa3131fedd0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede0 [0x00007ff81bab1000], Size=0xa3131fedd8 [0x4000], NewProtect=2, OldProtect=0xa3131fedd0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fee30 [0x00007ff81a6b6000], Size=0xa3131fee38 [0x2000], NewProtect=4, OldProtect=0x240263f3b08 [2]) => 0

NtClose(Handle=0xa4) => 0

NtOpenSection(SectionHandle=0xa3131fef58 [0xa4], DesiredAccess=0xd, ObjectAttributes=0x40:"USER32.dll") => 0

Loaded DLL at 00007FF81A4A0000 C:\Windows\System32\USER32.dll

NtMapViewOfSection(SectionHandle=0xa4, ProcessHandle=-1, BaseAddress=0x240263f6af0 [0x00007ff81a4a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f6a50 [0x0019d000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fedd0 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede8 [0x00007ff81a559000], Size=0xa3131fede0 [0x1000], NewProtect=2, OldProtect=0xa3131fee50 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede0 [0x00007ff81bab1000], Size=0xa3131fedd8 [0x4000], NewProtect=4, OldProtect=0xa3131fedd0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fede0 [0x00007ff81bab1000], Size=0xa3131fedd8 [0x4000], NewProtect=2, OldProtect=0xa3131fedd0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fee30 [0x00007ff81a52f000], Size=0xa3131fee38 [0x3000], NewProtect=4, OldProtect=0x240263f6a38 [2]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fe0d0 [0x00000240263f7000], ZeroBits=0, pSize=0xa3131fe178 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenSection(SectionHandle=0xa3131fe8c8 [0xa8], DesiredAccess=0xd, ObjectAttributes=0x40:"win32u.dll") => 0

Loaded DLL at 00007FF819920000 C:\Windows\System32\win32u.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x240263f7010 [0x00007ff819920000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f6f70 [0x00022000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fe740 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe750 [0x00007ff81bab1000], Size=0xa3131fe748 [0x4000], NewProtect=4, OldProtect=0xa3131fe740 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe750 [0x00007ff81bab1000], Size=0xa3131fe748 [0x4000], NewProtect=2, OldProtect=0xa3131fe740 [4]) => 0

NtClose(Handle=0xa8) => 0

NtOpenSection(SectionHandle=0xa3131fe8c8 [0xa8], DesiredAccess=0xd, ObjectAttributes=0x40:"GDI32.dll") => 0

Loaded DLL at 00007FF81AA20000 C:\Windows\System32\GDI32.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x240263f73b0 [0x00007ff81aa20000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f7310 [0x0002b000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fe740 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe758 [0x00007ff81aa47000], Size=0xa3131fe750 [0x2000], NewProtect=2, OldProtect=0xa3131fe7c0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe750 [0x00007ff81bab1000], Size=0xa3131fe748 [0x4000], NewProtect=4, OldProtect=0xa3131fe740 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe750 [0x00007ff81bab1000], Size=0xa3131fe748 [0x4000], NewProtect=2, OldProtect=0xa3131fe740 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe7a0 [0x00007ff81aa30000], Size=0xa3131fe7a8 [0x1000], NewProtect=4, OldProtect=0x240263f72f8 [2]) => 0

NtOpenSection(SectionHandle=0xa3131fe238 [0xac], DesiredAccess=0xd, ObjectAttributes=0x40:"gdi32full.dll") => 0

Loaded DLL at 00007FF8192D0000 C:\Windows\System32\gdi32full.dll

NtMapViewOfSection(SectionHandle=0xac, ProcessHandle=-1, BaseAddress=0x240263f7880 [0x00007ff8192d0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f77b0 [0x00117000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fe0b0 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe0c8 [0x00007ff8193d2000], Size=0xa3131fe0c0 [0x1000], NewProtect=2, OldProtect=0xa3131fe130 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe0c0 [0x00007ff81bab1000], Size=0xa3131fe0b8 [0x4000], NewProtect=4, OldProtect=0xa3131fe0b0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe0c0 [0x00007ff81bab1000], Size=0xa3131fe0b8 [0x4000], NewProtect=2, OldProtect=0xa3131fe0b0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe110 [0x00007ff819380000], Size=0xa3131fe118 [0x3000], NewProtect=4, OldProtect=0x240263f7798 [2]) => 0

NtOpenSection(SectionHandle=0xa3131fdb8 [0xb0], DesiredAccess=0xd, ObjectAttributes=0x40:"msvc_p_win.dll") => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fd2f0 [0x00000240263f8000], ZeroBits=0, pSize=0xa3131fd398 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

Loaded DLL at 00007FF819560000 C:\Windows\System32\msvc_p_win.dll

NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x240263f7df0 [0x00007ff819560000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f7d50 [0x0009d000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fda20 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fda38 [0x00007ff8195fa000], Size=0xa3131fda30 [0x1000], NewProtect=2, OldProtect=0xa3131fdaa0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fda30 [0x00007ff81bab1000], Size=0xa3131fda28 [0x4000], NewProtect=4, OldProtect=0xa3131fda20 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fda30 [0x00007ff81bab1000], Size=0xa3131fda28 [0x4000], NewProtect=2, OldProtect=0xa3131fda20 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fda80 [0x00007ff8195b6000], Size=0xa3131fda88 [0x2000], NewProtect=4, OldProtect=0x240263f7d38 [2]) => 0

NtOpenSection(SectionHandle=0xa3131fd518 [0xb4], DesiredAccess=0xd, ObjectAttributes=0x40:"ucrtbase.dll") => 0

Loaded DLL at 00007FF819820000 C:\Windows\System32\ucrtbase.dll

NtMapViewOfSection(SectionHandle=0xb4, ProcessHandle=-1, BaseAddress=0x240263f82e0 [0x00007ff819820000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f8210 [0x00100000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fd390 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fd3a0 [0x00007ff81bab1000], Size=0xa3131fd398 [0x4000], NewProtect=4, OldProtect=0xa3131fd390 [2]) => 0

```

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fd3a0 [0x00007ff81bab1000],
Size=0xa3131fd398 [0x4000], NewProtect=2, OldProtect=0xa3131fd390 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fd3f0 [0x00007ff8198d9000],
Size=0xa3131fd3f8 [0x1000], NewProtect=4, OldProtect=0x240263f81f8 [2]) => 0

NtClose(Handle=0xb4) => 0

NtClose(Handle=0xb0) => 0

NtClose(Handle=0xac) => 0

NtClose(Handle=0xa8) => 0

NtClose(Handle=0xa4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131ff838 [0x00007ff7324a8000],
Size=0xa3131ff840 [0x1000], NewProtect=8, OldProtect=0xa3131ff3b0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f3ae8 [0x00007ff81a6b6000],
Size=0x240263f3af0 [0x2000], NewProtect=2, OldProtect=0xa3131ff390 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0xa3131ff2f0, Length=0x28) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f81d8 [0x00007ff8198d9000],
Size=0x240263f81e0 [0x1000], NewProtect=2, OldProtect=0xa3131ff390 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f7d18 [0x00007ff8195b6000],
Size=0x240263f7d20 [0x2000], NewProtect=2, OldProtect=0xa3131ff390 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f7778 [0x00007ff819380000],
Size=0x240263f7780 [0x3000], NewProtect=2, OldProtect=0xa3131ff390 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f72d8 [0x00007ff81aa30000],
Size=0x240263f72e0 [0x1000], NewProtect=2, OldProtect=0xa3131ff390 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f6a18 [0x00007ff81a52f000],
Size=0x240263f6a20 [0x3000], NewProtect=2, OldProtect=0xa3131ff390 [4]) => 0

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

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

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

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

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

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

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

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff6f8, VmInformation=0xa3131ff620, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11
[ThreadHideFromDebugger], ThreadInformation=0xa3131ff530, Length=1, ReturnLength=null) => 0

```


Initial breakpoint

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

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0xa3131ff470 [0xa4]) => 0

NtQueryInformationToken(TokenHandle=0xa4, TokenInformationClass=0xa [TokenStatistics], TokenInformation=0xa3131ff480, Length=0x38, ReturnLength=0xa3131ff478 [0x38]) => 0

NtClose(Handle=0xa4) => 0

NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode", Type=0xa3131ff350 [4], Buffer=0xa3131ff340, Length=4, ReturnedLength=0xa3131ff358 [4]) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1, VirtualAddresses=0xa3131ff3f0, VmInformation=0xa3131ff4c8, VmInformationLength=4) => 0xc00000bb [50 'Такой запрос не поддерживается.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fec20 [0x00000240265c0000], ZeroBits=0, pSize=0xa3131fec28 [0x00120000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fec20 [0x00000240265c0000], pSize=0xa3131fec18 [0x00110000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fec08 [0x00000240266d0000], ZeroBits=0, pSize=0xa3131fec00 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xa3131ff1f0 [0/8], FsInformation=0xa3131ff210, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0xa3131ff1f0 [0/8], FsInformation=0xa3131ff210, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x5c, IoStatusBlock=0xa3131ff1f0 [0/8], FsInformation=0xa3131ff210, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fea90 [0x00000240263f9000], ZeroBits=0, pSize=0xa3131feb38 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenKey(KeyHandle=0xa3131fdeb0 [0xa4], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions") => 0

NtQueryValueKey(KeyHandle=0xa4, ValueName="", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0xa3131fe3a0, Length=0x214, ResultLength=0xa3131fe348 [0x2a]) => 0

NtQueryValueKey(KeyHandle=0xa4, ValueName="000603xx", KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0xa3131fe380, Length=0x214, ResultLength=0xa3131fe128 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fea60 [0x00000240266d2000], ZeroBits=0, pSize=0xa3131feb08 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fea40 [0x00000240266d3000], ZeroBits=0, pSize=0xa3131feae8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81a6c6998, MemoryInformationClass=6 [MemoryImageInformation], MemoryInformation=0xa3131fe3e0, Length=0x18, ReturnLength=null) => 0

```

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff3b0, VmInformation=0xa3131ff488, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff370, VmInformation=0xa3131ff448, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0xa3131ff190 [0/8],
FsInformation=0xa3131ff1b0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0xa3131ff190 [0/8],
FsInformation=0xa3131ff1b0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x5c, IoStatusBlock=0xa3131ff190 [0/8],
FsInformation=0xa3131ff1b0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fe980 [0x00000240263fb000],
ZeroBits=0, pSize=0xa3131fea28 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff3b0, VmInformation=0xa3131ff488, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fe2c0 [0x00000240263fd000],
ZeroBits=0, pSize=0xa3131fe368 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fe2c0 [0x00000240263fe000],
ZeroBits=0, pSize=0xa3131fe368 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff3f0, VmInformation=0xa3131ff4c8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff3f0, VmInformation=0xa3131ff4c8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x34
[ProcessMitigationPolicy], ProcessInformation=0xa3131ff270, Length=8, ReturnLength=null) =>
0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131ff3f0, VmInformation=0xa3131ff4c8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xa3131fee40, Length=0x40, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131feae0 [0x00007ff81bab1000],
Size=0xa3131fead8 [0x4000], NewProtect=4, OldProtect=0xa3131fead0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131feae0 [0x00007ff81bab1000],
Size=0xa3131fead8 [0x4000], NewProtect=2, OldProtect=0xa3131fead0 [4]) => 0

NtAlpcSendWaitReceivePort(PortHandle=0x60, SendFlags=0x00020000, SendMessage=0xa3131fe750 [2
[LPC_REPLY] (48b)], InMessageBuffer=null, ReceiveBuffer=0xa3131fe750,
ReceiveBufferSize=0xa3131fe710 [0x58], OutMessageBuffer=null, Timeout=null) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\system32\IMM32.DLL",
Attributes=0xa3131fe368 [ARCHIVE]) => 0

```

```
NtOpenFile(FileHandle=0xa3131fe3a8 [0xa8], DesiredAccess=SYNCHRONIZE|0x1,
ObjectAttributes="\??\C:\Windows\system32\IMM32.DLL", IoStatusBlock=0xa3131fe3b8 [0/1],
ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0xa3131fe3a0 [0xc], DesiredAccess=0x4, ObjectAttributes=null,
SectionSize=null, Protect=2, Attributes=0x08000000, FileHandle=0xa8) => 0

NtMapViewOfSection(SectionHandle=0xc, ProcessHandle=-1, BaseAddress=0xa3131fe420
[0x00000240263a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0xa3131fe438
[0x0002e000], InheritDisposition=1 [ViewShare], AllocationType=0, Protect=2) => 0

NtUnmapViewOfSection(ProcessHandle=-1, BaseAddress=0x240263a0000) => 0

NtClose(Handle=0xc) => 0

NtClose(Handle=0xa8) => 0

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0xa3131fe530, Length=0x330, ReturnLength=0xa3131fe4e8) =>
0xc0000225 [1168 'Элемент не найден.']

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0xa3131fe530, Length=0x330, ReturnLength=0xa3131fe4e8) =>
0xc0000225 [1168 'Элемент не найден.']

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0xa3131fe530, Length=4) => 0

NtOpenSection(SectionHandle=0xa3131fe508 [0xac], DesiredAccess=0xd,
ObjectAttributes=0x40:"IMM32.DLL") => 0

Loaded DLL at 00007FF819950000 C:\Windows\System32\IMM32.DLL

NtMapViewOfSection(SectionHandle=0xac, ProcessHandle=-1, BaseAddress=0x240263fe1c0
[0x00007ff819950000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263fe100
[0x0002f000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0xa3131fe380 [1.04909e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe398 [0x00007ff819978000],
Size=0xa3131fe390 [0x1000], NewProtect=2, OldProtect=0xa3131fe400 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe390 [0x00007ff81bab1000],
Size=0xa3131fe388 [0x4000], NewProtect=4, OldProtect=0xa3131fe380 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe390 [0x00007ff81bab1000],
Size=0xa3131fe388 [0x4000], NewProtect=2, OldProtect=0xa3131fe380 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe3e0 [0x00007ff81996f000],
Size=0xa3131fe3e8 [0x1000], NewProtect=4, OldProtect=0x240263fe0e8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263fe0c8 [0x00007ff81996f000],
Size=0x240263fe0d0 [0x1000], NewProtect=2, OldProtect=0xa3131fe2d0 [4]) => 0

NtClose(Handle=0xac) => 0

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131fe430, VmInformation=0xa3131fe508, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']
```

```
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0xa3131fe2d0, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x34
[ProcessMitigationPolicy], ProcessInformation=0xa3131fe250, Length=8, ReturnLength=null) =>
0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x34
[ProcessMitigationPolicy], ProcessInformation=0xa3131feb30, Length=8, ReturnLength=null) =>
0

NtOpenKey(KeyHandle=0xa3131feae8, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Error Message
Instrument\") => 0xc0000034 [2 'Не удается найти указанный файл.']]

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fe9e8, InputBufferLength=0xa0,
OutputBuffer=0xa3131fe9e8, OutputBufferLength=0xa0, ReturnLength=0xa3131fe9e0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fea28, InputBufferLength=0x18,
OutputBuffer=0xa3131fea40, OutputBufferLength=0x78, ReturnLength=0xa3131fea20 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fe9e8, InputBufferLength=0xa0,
OutputBuffer=0xa3131fe9e8, OutputBufferLength=0xa0, ReturnLength=0xa3131fe9e0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fea28, InputBufferLength=0x18,
OutputBuffer=0xa3131fea40, OutputBufferLength=0x78, ReturnLength=0xa3131fea20 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fe9e8, InputBufferLength=0xa0,
OutputBuffer=0xa3131fe9e8, OutputBufferLength=0xa0, ReturnLength=0xa3131fe9e0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fea28, InputBufferLength=0x18,
OutputBuffer=0xa3131fea40, OutputBufferLength=0x78, ReturnLength=0xa3131fea20 [0]) => 0

NtOpenKey(KeyHandle=0xa3131fe4f0, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131fe608, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131fe610, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131fe4f0, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131fe608, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131fe610, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131fea20 [0xb4], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows
NT\CurrentVersion\GRE_Initialize") => 0
```

```

NtQueryValueKey(KeyHandle=0xb4, ValueName="DisableMetaFiles", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xa3131fea70, Length=0x14,
ResultLength=0xa3131fea28) => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtClose(Handle=0xb4) => 0

NtOpenKey(KeyHandle=0xa3131fea20 [0xb4], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows
NT\CurrentVersion\GRE_Initialize") => 0

NtQueryValueKey(KeyHandle=0xb4, ValueName="DisableUmpdBufferSizeCheck",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xa3131fea70,
Length=0x14, ResultLength=0xa3131fea28) => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtClose(Handle=0xb4) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0xa3131fdc40, Length=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fd970 [0x00000240263ff000],
ZeroBits=0, pSize=0xa3131fda18 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe128 [0x00007ff81aa47000],
Size=0xa3131fe120 [0x2000], NewProtect=4, OldProtect=0xa3131fe138 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe128 [0x00007ff81aa47000],
Size=0xa3131fe120 [0x2000], NewProtect=2, OldProtect=0xa3131fe138 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0xa3131fdc10, Length=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe0f8 [0x00007ff81aa47000],
Size=0xa3131fe0f0 [0x1000], NewProtect=4, OldProtect=0xa3131fe108 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fe0f8 [0x00007ff81aa47000],
Size=0xa3131fe0f0 [0x1000], NewProtect=2, OldProtect=0xa3131fe108 [4]) => 0

NtQuerySystemInformation(SystemInformationClass=0x67 [SystemCodeIntegrityInformation],
SystemInformation=0xa3131fe7e0, Length=8, ReturnLength=null) => 0

NtOpenKey(KeyHandle=0xa3131fea70, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") =>
0xc0000034 [2 'Не удастся найти указанный файл.']

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

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x84, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0xa3131ffb58, BufferLength=4) => 0

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

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff7324a2220, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0xa3131ffb60, Length=0x30,
ReturnLength=0xa3131ffb10 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff7324a2220, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0xa3131ffb90, Length=0x30, ReturnLength=null)
=> 0

```

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff7324a2220, MemoryInformationClass=2 [MemoryMappedFilenameInformation], MemoryInformation=0xa3131ffc08, Length=0x21a, ReturnLength=null) => 0

NtOpenFile(FileHandle=0xa3131ff268 [0xc8], DesiredAccess=SYNCHRONIZE|GENERIC_READ, ObjectAttributes="\Device\NamedPipe\", IoStatusBlock=0xa3131ff280 [0/1], ShareAccess=3, OpenOptions=0x20) => 0

NtCreateNamedPipeFile(NamedPipeHandle=0xa3131ff220 [0xcc], DesiredAccess=SYNCHRONIZE|GENERIC_READ|0x100, ObjectAttributes=0xc8:"", IoStatusBlock=0xa3131ff280 [0/2], ShareAccess=3, CreateDisposition=2, CreateOptions=0x20, MessageType=false, MessageRead=false, NonBlocking=false, MaxInstances=1, InBufferSize=0x1000, OutBufferSize=0x1000, Timeout=0xa3131ff270 [-1.2e+09]) => 0

NtOpenFile(FileHandle=0xa3131ff278 [0xd0], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80, ObjectAttributes=0xcc:"", IoStatusBlock=0xa3131ff280 [0/1], ShareAccess=3, OpenOptions=0x60) => 0

NtReadFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null, IoStatusBlock=0xa3131ff280 [0/0xc], Buffer=0xa3131ff840, Length=0x104, ByteOffset=null, Key=null) => 0

NtQueryWnfStateData(StateName=0xa3131fd790 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xa3131fd828 [0], Buffer=0xa3131fd880, BufferSize=0xa3131fd780 [0]) => 0

NtQueryWnfStateData(StateName=0xa3131fd630 [0xa3bc7c75], TypeId=null, ExplicitScope=null, ChangeStamp=0xa3131fd6c8 [0], Buffer=0xa3131fd720, BufferSize=0xa3131fd620 [0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fd1e0 [0x0000024026400000], ZeroBits=0, pSize=0xa3131fd288 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryAttributesFile(ObjectAttributes="\??\D:\code\osi\child.exe", Attributes=0xa3131fd6d0 [ARCHIVE]) => 0

NtQueryAttributesFile(ObjectAttributes="\??\D:\code\osi\child.exe", Attributes=0xa3131fdac0 [ARCHIVE]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d [ProcessLoaderDetour], ProcessInformation=0xa3131fcf10, Length=4) => 0

NtOpenSection(SectionHandle=0xa3131fcee8 [0xd4], DesiredAccess=0xd, ObjectAttributes=0x40:"sechost.dll") => 0

Loaded DLL at 00007FF819B70000 C:\Windows\System32\sechost.dll

NtMapViewOfSection(SectionHandle=0xd4, ProcessHandle=-1, BaseAddress=0x240263f7710 [0x00007ff819b70000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f8210 [0x0009f000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fcd60 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fcd78 [0x00007ff819c0a000], Size=0xa3131fcd70 [0x1000], NewProtect=2, OldProtect=0xa3131fcde0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fcd70 [0x00007ff81bab1000], Size=0xa3131fcd68 [0x4000], NewProtect=4, OldProtect=0xa3131fcd60 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fcd70 [0x00007ff81bab1000], Size=0xa3131fcd68 [0x4000], NewProtect=2, OldProtect=0xa3131fcd60 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fcdc0 [0x00007ff819be4000], Size=0xa3131fcdc8 [0x1000], NewProtect=4, OldProtect=0x240263f81f8 [2]) => 0

NtOpenSection(SectionHandle=0xa3131fc858 [0xd8], DesiredAccess=0xd, ObjectAttributes=0x40:"RPCRT4.dll") => 0

Loaded DLL at 00007FF81A6E0000 C:\Windows\System32\RPCRT4.dll

NtMapViewOfSection(SectionHandle=0xd8, ProcessHandle=-1, BaseAddress=0x24026400a10 [0x00007ff81a6e0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f7d50 [0x00123000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fc6d0 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc6e8 [0x00007ff81a7fb000], Size=0xa3131fc6e0 [0x1000], NewProtect=2, OldProtect=0xa3131fc750 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc6e0 [0x00007ff81bab1000], Size=0xa3131fc6d8 [0x4000], NewProtect=4, OldProtect=0xa3131fc6d0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc6e0 [0x00007ff81bab1000], Size=0xa3131fc6d8 [0x4000], NewProtect=2, OldProtect=0xa3131fc6d0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc730 [0x00007ff81a7cc000], Size=0xa3131fc738 [0x2000], NewProtect=4, OldProtect=0x240263f7d38 [2]) => 0

NtClose(Handle=0xd8) => 0

NtOpenSection(SectionHandle=0xa3131fc858 [0xd8], DesiredAccess=0xd, ObjectAttributes=0x40:"bcrypt.dll") => 0

Loaded DLL at 00007FF8197F0000 C:\Windows\System32\bcrypt.dll

NtMapViewOfSection(SectionHandle=0xd8, ProcessHandle=-1, BaseAddress=0x24026400b60 [0x00007ff8197f0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x240263f6f70 [0x00027000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0xa3131fc6d0 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc6e8 [0x00007ff819814000], Size=0xa3131fc6e0 [0x1000], NewProtect=2, OldProtect=0xa3131fc750 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc6e0 [0x00007ff81bab1000], Size=0xa3131fc6d8 [0x4000], NewProtect=4, OldProtect=0xa3131fc6d0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc6e0 [0x00007ff81bab1000], Size=0xa3131fc6d8 [0x4000], NewProtect=2, OldProtect=0xa3131fc6d0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fc730 [0x00007ff81980b000], Size=0xa3131fc738 [0x1000], NewProtect=4, OldProtect=0x240263f6f58 [2]) => 0

NtClose(Handle=0xd8) => 0

NtClose(Handle=0xd4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f7d18 [0x00007ff81a7cc000], Size=0x240263f7d20 [0x2000], NewProtect=2, OldProtect=0xa3131fcdb0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f6f38 [0x00007ff81980b000], Size=0x240263f6f40 [0x1000], NewProtect=2, OldProtect=0xa3131fcdb0 [4]) => 0

```

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x240263f81d8 [0x00007ff819be4000],
Size=0x240263f81e0 [0x1000], NewProtect=2, OldProtect=0xa3131fcdb0 [4]) => 0

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

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

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131fcdd0, VmInformation=0xa3131fcea8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']]

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131fcdd0, VmInformation=0xa3131fcea8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']]

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fcab8, InputBufferLength=0xa0,
OutputBuffer=0xa3131fcab8, OutputBufferLength=0xa0, ReturnLength=0xa3131fcab0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fcb18, InputBufferLength=0xa0,
OutputBuffer=0xa3131fcb18, OutputBufferLength=0xa0, ReturnLength=0xa3131fcb10 [0xa0]) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x56
[ProcessEnclaveInformation], ProcessInformation=0xa3131fcb90, Length=0xb0,
ReturnLength=null) => 0xc0000003 [87 'Параметр задан неверно.']]

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0
[ProcessBasicInformation], ProcessInformation=0xa3131fcb10, Length=0x40, ReturnLength=null)
=> 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fcac8, InputBufferLength=0xa0,
OutputBuffer=0xa3131fcac8, OutputBufferLength=0xa0, ReturnLength=0xa3131fcac0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fcb08, InputBufferLength=0x18,
OutputBuffer=0xa3131fcb20, OutputBufferLength=0x78, ReturnLength=0xa3131fcb00 [0]) => 0

NtCreateSemaphore(SemaphoreHandle=0xa3131fcac8 [0xdc], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0

NtCreateSemaphore(SemaphoreHandle=0xa3131fcad8 [0xe0], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0

NtCreateEvent(EventHandle=0xa3131fcac8 [0xe4],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtOpenFile(FileHandle=0x7ff819811760 [0xe8], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes="\Device\KsecDD", IoStatusBlock=0xa3131fca10 [0/0], ShareAccess=7,
OpenOptions=0x20) => 0

NtDeviceIoControlFile(FileHandle=0xe8, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131fcab0 [0/0], IoControlCode=0x00390400, InputBuffer=0xa3131fcb90,
InputBufferLength=0x68, OutputBuffer=0xa3131fcac0, OutputBufferLength=8) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0xa3131fce10, VmInformation=0xa3131fcee8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']]

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fca38, InputBufferLength=0xa0,
OutputBuffer=0xa3131fca38, OutputBufferLength=0xa0, ReturnLength=0xa3131fca30 [0xa0]) => 0

```



```

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fca78, InputBufferLength=0x18,
OutputBuffer=0xa3131fca90, OutputBufferLength=0x78, ReturnLength=0xa3131fca70 [0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fc320 [0x0000024026401000],
ZeroBits=0, pSize=0xa3131fc3c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fc320 [0x0000024026402000],
ZeroBits=0, pSize=0xa3131fc3c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fc320 [0x0000024026403000],
ZeroBits=0, pSize=0xa3131fc3c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fca68, InputBufferLength=0xa0,
OutputBuffer=0xa3131fca68, OutputBufferLength=0xa0, ReturnLength=0xa3131fca60 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0xa3131fcaa8, InputBufferLength=0x18,
OutputBuffer=0xa3131fcac0, OutputBufferLength=0x78, ReturnLength=0xa3131fcaa0 [0]) => 0

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

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fd3f8 [0x00007ff8192a3000],
Size=0xa3131fd3f0 [0x1000], NewProtect=4, OldProtect=0xa3131fd408 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0xa3131fd3f8 [0x00007ff8192a3000],
Size=0xa3131fd3f0 [0x1000], NewProtect=2, OldProtect=0xa3131fd408 [4]) => 0

NtQueryAttributesFile(ObjectAttributes="\??\D:\code\osi", Attributes=0xa3131fdac0
[DIRECTORY]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0xa3131fcd50 [0x0000024026404000],
ZeroBits=0, pSize=0xa3131fcdf8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenKey(KeyHandle=0xa3131fda60, DesiredAccess=0x9, ObjectAttributes=0x10:"child.exe") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0xa3131fda40, DesiredAccess=0x101,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Wow64\x86\xtajit") => 0xc0000034 [2
'Не удается найти указанный файл.']]

NtCreateUserProcess(ProcessHandle=0xa3131fdbd8 [0xf8], ThreadHandle=0xa3131fdc30 [0xf4],
ProcessDesiredAccess=MAXIMUM_ALLOWED, ThreadDesiredAccess=MAXIMUM_ALLOWED,
ProcessObjectAttributes=null, ThreadObjectAttributes=null, ProcessFlags=0x204,
ThreadFlags=1, ProcessParameters=0x24026403aa0 ["D:\code\osi\child.exe"],
CreateInfo=0xa3131fdea0, AttributeList=0xa3131fe2d0) => 0

NtOpenKey(KeyHandle=0xa3131fdb08, DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session
Manager\AppCertDlls") => 0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0xa, TokenHandle=0xa3131fd7a0 [0x104]) =>
0

NtQueryInformationToken(TokenHandle=0x104, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fda10, Length=0x90, ReturnLength=0xa3131fd7e8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd7e0, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

```

```
NtOpenKey(KeyHandle=0xa3131fd7b0 [0x108], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0

NtQueryValueKey(KeyHandle=0x108, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xa3131fd8f0, Length=0x50,
ResultLength=0xa3131fd7a8) => 0xc0000034 [2 'Не удастся найти указанный файл.']]

NtQueryValueKey(KeyHandle=0x108, ValueName="AuthenticodeEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0xa3131fd8f0, Length=0x50,
ResultLength=0xa3131fd7a8 [0x10]) => 0

NtClose(Handle=0x108) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd6e0, Length=0x58, ReturnLength=0xa3131fd6d8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd7b0, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-
21-2308459876-1469942742-3350914452-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 'Не
удается найти указанный файл.']]

NtClose(Handle=0x104) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0xa3131fd888, InputBufferLength=0xa0,
OutputBuffer=0xa3131fd888, OutputBufferLength=0xa0, ReturnLength=0xa3131fd880 [0xa0]) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap],
ProcessInformation=0xa3131fd260, Length=0x24, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap],
ProcessInformation=0xa3131fd1f0, Length=0x24, ReturnLength=null) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd5c0, Length=0x58, ReturnLength=0xa3131fd5b8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd718 [0x104], DesiredAccess=0x1,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-
1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders") => 0

NtQueryValueKey(KeyHandle=0x104, ValueName="Cache", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x240264050b0, Length=0x208,
ResultLength=0xa3131fd710 [0x92]) => 0

NtClose(Handle=0x104) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd5c0, Length=0x58, ReturnLength=0xa3131fd5b8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd6c0 [0x104], DesiredAccess=0x8,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-
1001\Software\Microsoft\Windows NT\CurrentVersion") => 0

NtOpenKey(KeyHandle=0xa3131fd6c8 [0x110], DesiredAccess=0x101,
ObjectAttributes=0x104:"AppCompatFlags\Layers") => 0

NtQueryValueKey(KeyHandle=0x110, ValueName="D:\code\osi\child.exe",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xa3131fd728,
Length=0x10, ResultLength=0xa3131fd6d0) => 0xc0000034 [2 'Не удастся найти указанный файл.']]

NtClose(Handle=0x110) => 0
```

```

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

NtQueryInformationProcess(ProcessHandle=0xf8, ProcessInformationClass=0
[ProcessBasicInformation], ProcessInformation=0xa3131fda40, Length=0x40, ReturnLength=null)
=> 0

NtOpenKey(KeyHandle=0xa3131fd780 [0x110], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide")
=> 0

NtQueryValueKey(KeyHandle=0x110, ValueName="PreferExternalManifest",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0xa3131fd7d0,
Length=0x14, ResultLength=0xa3131fd788) => 0xc0000034 [2 'Не удается найти указанный файл.']

NtClose(Handle=0x110) => 0

NtQueryVolumeInformationFile(FileHandle=0xfc, IoStatusBlock=0xa3131fd7e0 [0/8],
FsInformation=0xa3131fd810, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtGetMUIRegistryInfo(Flags=0, BufferLength=0xa3131fd610 [0x4d0], Buffer=null) => 0

NtGetMUIRegistryInfo(Flags=0, BufferLength=0xa3131fd610 [0x4d0], Buffer=0x24026403aa0) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd460, Length=0x58, ReturnLength=0xa3131fd458 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd628 [0x110], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-1001") => 0

NtOpenKey(KeyHandle=0xa3131fd620, DesiredAccess=KEY_READ, ObjectAttributes=0x110:"Control
Panel\Desktop\MuiCached\MachineLanguageConfiguration") => 0xc0000034 [2 'Не удается найти
указанный файл.']

NtClose(Handle=0x110) => 0

NtOpenKey(KeyHandle=0xa3131fd4b8, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034
[2 'Не удается найти указанный файл.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd370, Length=0x58, ReturnLength=0xa3131fd368 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd4c0 [0x114], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-1001") => 0

NtOpenKey(KeyHandle=0xa3131fd4c8, DesiredAccess=KEY_READ,
ObjectAttributes=0x114:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2
'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131fd4b8 [0x108], DesiredAccess=KEY_READ,
ObjectAttributes=0x114:"Control Panel\Desktop\LanguageConfiguration") => 0

NtEnumerateValueKey(KeyHandle=0x108, Index=0, KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xa3131fd240, Length=0x200,
ResultLength=0xa3131fd200 [0x2e]) => 0

NtEnumerateValueKey(KeyHandle=0x108, Index=1, KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0xa3131fd240, Length=0x200,
ResultLength=0xa3131fd200) => 0x8000001a [259 'Дополнительные данные отсутствуют.']]

NtClose(Handle=0x108) => 0

```

```
NtClose(Handle=0x114) => 0

NtOpenKey(KeyHandle=0xa3131fd3c0, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd240, Length=0x58, ReturnLength=0xa3131fd238 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd3b8 [0x110], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-1001") => 0

NtOpenKey(KeyHandle=0xa3131fd2e0, DesiredAccess=KEY_READ,
ObjectAttributes=0x110:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131fd3b0 [0x114], DesiredAccess=KEY_READ,
ObjectAttributes=0x110:"Control Panel\Desktop") => 0

NtQueryValueKey(KeyHandle=0x114, ValueName="PreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x240263f6a20,
Length=0xc, ResultLength=0xa3131fd378) => 0x80000005 [234 'Имеются дополнительные данные.']

NtQueryValueKey(KeyHandle=0x114, ValueName="PreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x240263f7d70,
Length=0x1a, ResultLength=0xa3131fd378 [0x1a]) => 0

NtClose(Handle=0x114) => 0

NtClose(Handle=0x110) => 0

NtOpenKey(KeyHandle=0xa3131fd3c0, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd240, Length=0x58, ReturnLength=0xa3131fd238 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd3b8 [0x110], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-1001") => 0

NtOpenKey(KeyHandle=0xa3131fd3b0 [0x114], DesiredAccess=KEY_READ,
ObjectAttributes=0x110:"Control Panel\Desktop\MuiCached") => 0

NtQueryValueKey(KeyHandle=0x114, ValueName="MachinePreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x240263f6a20,
Length=0xc, ResultLength=0xa3131fd378) => 0x80000005 [234 'Имеются дополнительные данные.']

NtQueryValueKey(KeyHandle=0x114, ValueName="MachinePreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x240263f7d70,
Length=0x18, ResultLength=0xa3131fd378 [0x18]) => 0

NtClose(Handle=0x114) => 0

NtClose(Handle=0x110) => 0

NtOpenKey(KeyHandle=0xa3131fd460, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0xa3131fd2e0, Length=0x58, ReturnLength=0xa3131fd2d8 [0x2c]) => 0
```

NtOpenKey(KeyHandle=0xa3131fd458 [0x110], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-1001") => 0

NtOpenKey(KeyHandle=0xa3131fd380, DesiredAccess=KEY_READ, ObjectAttributes=0x110:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131fd450 [0x114], DesiredAccess=KEY_READ, ObjectAttributes=0x110:"Control Panel\Desktop") => 0

NtQueryValueKey(KeyHandle=0x114, ValueName="PreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x240263f6a20, Length=0xc, ResultLength=0xa3131fd418) => 0x80000005 [234 'Имя дополнительных данных.']

NtQueryValueKey(KeyHandle=0x114, ValueName="PreferredUILanguages", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x240263f7d70, Length=0x1a, ResultLength=0xa3131fd418 [0x1a]) => 0

NtClose(Handle=0x114) => 0

NtClose(Handle=0x110) => 0

NtOpenKey(KeyHandle=0xa3131fd538, DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0xa3131fd3f0, Length=0x58, ReturnLength=0xa3131fd3e8 [0x2c]) => 0

NtOpenKey(KeyHandle=0xa3131fd540 [0x110], DesiredAccess=MAXIMUM_ALLOWED, ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-1001") => 0

NtOpenKey(KeyHandle=0xa3131fd548, DesiredAccess=KEY_READ, ObjectAttributes=0x110:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0xa3131fd538 [0x114], DesiredAccess=KEY_READ, ObjectAttributes=0x110:"Control Panel\Desktop\LanguageConfiguration") => 0

NtEnumerateValueKey(KeyHandle=0x114, Index=0, KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0xa3131fd2c0, Length=0x200, ResultLength=0xa3131fd280 [0x2e]) => 0

NtEnumerateValueKey(KeyHandle=0x114, Index=1, KeyValueInformationClass=1 [KeyValueFullInformation], KeyValueInformation=0xa3131fd2c0, Length=0x200, ResultLength=0xa3131fd280) => 0x8000001a [259 'Дополнительные данные отсутствуют.']

NtClose(Handle=0x114) => 0

NtClose(Handle=0x110) => 0

NtAlpcSendWaitReceivePort(PortHandle=0x60, SendFlags=0x00020000, SendMessage=0xa3131fe6a0 [2 [LPC_REPLY] (560b)], InMessageBuffer=null, ReceiveBuffer=0xa3131fe6a0, ReceiveBufferSize=0xa3131fdae0 [0x258], OutMessageBuffer=null, Timeout=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap], ProcessInformation=0xa3131fd250, Length=0x24, ReturnLength=null) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser], TokenInformation=0xa3131fd620, Length=0x58, ReturnLength=0xa3131fd618 [0x2c]) => 0

```

NtOpenKey(KeyHandle=0xa3131fd778 [0x110], DesiredAccess=0x1,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-2308459876-1469942742-3350914452-
1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders") => 0

NtQueryValueKey(KeyHandle=0x110, ValueName="Cache", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x240264042c0, Length=0x208,
ResultLength=0xa3131fd770 [0x92]) => 0

NtClose(Handle=0x110) => 0

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

NtQueryLicenseValue(Name="Kernel-OneCore-DeviceFamilyID", Type=0xa3131fd6f8 [4],
Buffer=0xa3131fd6f0, Length=4, ReturnedLength=0xa3131fd740 [4]) => 0

NtAllocateVirtualMemory(ProcessHandle=0xf8, lpAddress=0xa3131fde20 [0x000001f52ec50000],
ZeroBits=0, pSize=0xa3131fd88 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtWriteVirtualMemory(ProcessHandle=0xf8, BaseAddress=0x1f52ec50000, Buffer=0x24026403fa0,
BufferLength=0x11c0, ReturnedLength=null) => 0

NtWriteVirtualMemory(ProcessHandle=0xf8, BaseAddress=0x3405d862d8, Buffer=0xa3131fde20,
BufferLength=8, ReturnedLength=null) => 0

NtResumeThread(ThreadHandle=0xf4, SuspendCount=null) => 0

Process 14816 starting at 00007FF6057213F0 with command line: "child.exe
"D:\code\osi\output.txt""

D:\code\osi\child.exe

NtClose(Handle=0xfc) => 0

Loaded DLL at 00007FF81B930000 C:\Windows\SYSTEM32\ntdll.dll

NtClose(Handle=0x100) => 0

NtQueryPerformanceCounter(Counter=0x3405fff310 [1.04914e+12], Freq=null) => 0

NtClose(Handle=0xcc) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405fff358 [0x00007ff81bab4000],
Size=0x3405fff350 [0x1000], NewProtect=4, OldProtect=0x3405fff390 [8]) => 0

NtClose(Handle=0xf4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405fff358 [0x00007ff81bab4000],
Size=0x3405fff350 [0x1000], NewProtect=8, OldProtect=0x3405fff390 [4]) => 0

NtCreateEvent(EventHandle=0x7ff81ba9c478 [8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x3405fff2c0, Length=0x40, ReturnLength=null) => 0

NtReadFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131ff280 [0/7], Buffer=0xa3131ff950, Length=0x400, ByteOffset=null,
Key=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x3405fffe8, Length=4, ReturnLength=null) => 0

```

```

NtWriteFile(FileHandle=0xd0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131ff290 [0/7], Buffer=0xa3131ff950, Length=7, ByteOffset=null, Key=null)
=> 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0x3405ffec0, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81b930000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x3405ffedd0, Length=0x18, ReturnLength=null) =>
0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0x3405ffee90, Length=0x50,
ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffeee0 [0x00007ff81bab1000],
Size=0x3405ffeed8 [0x4000], NewProtect=2, OldProtect=0x3405ffeed0 [4]) => 0

NtOpenKey(KeyHandle=0x3405ffdb20 [0xc], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xc, ValueName="RaiseExceptionOnPossibleDeadlock",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x3405ffdb30,
Length=0x50, ResultLength=0x3405ffdb28) => 0xc0000034 [2 'Не удается найти указанный файл.']]

NtClose(Handle=0xc) => 0

NtOpenKey(KeyHandle=0x3405ffdb00, DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager\Segment
Heap") => 0xc0000034 [2 'Не удается найти указанный файл.']]

NtReadFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131ff280 [0/7], Buffer=0xa3131ff950, Length=0x400, ByteOffset=null,
Key=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x7ff81ba9d230, Length=4, ReturnLength=null) => 0

NtWriteFile(FileHandle=0xd0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131ff290 [0/7], Buffer=0xa3131ff950, Length=7, ByteOffset=null, Key=null)
=> 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x3405ffee78, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x3405ffe8b0, Length=0x330, ReturnLength=0x3405ffe868) =>
0xc0000025 [1168 'Элемент не найден.']]

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x3405ffe8b0, Length=0x330, ReturnLength=0x3405ffe868) =>
0xc0000025 [1168 'Элемент не найден.']]

NtOpenKey(KeyHandle=0x3405ffedf0 [0x10], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x10, ValueName="ResourcePolicies", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x3405ffee30, Length=0x18,
ResultLength=0x3405ffedf8) => 0xc0000034 [2 'Не удается найти указанный файл.']]

NtClose(Handle=0x10) => 0

```

```

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x3405ffeed0, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x3405ffee70, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation],
SystemInformation=0x3405ffeea0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81ba9dc38 [0x00007ff560610000],
ZeroBits=0x0000003405ffee20, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x3405ffed88, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81ba9dc30 [0x00007ff562610000],
ZeroBits=0x0000003405ffee28, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null,
DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81ba9dca0 [0x00007ff4605f0000],
ZeroBits=0x0000003405ffedd0, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x3405ffed38, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x3405ffed10, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe8d0 [0x000001f52ec60000],
ZeroBits=0, pSize=0x3405ffe8d8 [0x00250000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe8d0 [0x000001f52ec60000],
pSize=0x3405ffe8c8 [0x00150000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe8b8 [0x000001f52edb0000],
ZeroBits=0, pSize=0x3405ffe8b0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5
[SystemHypervisorSharedPageInformation], SystemInformation=0x3405fff078, Length=8,
ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap],
SystemInformation=0x3405ffea0, Length=0x408, ReturnLength=0x3405ffef00 [0x18]) => 0

NtCreateEvent(EventHandle=0x3405ffed18 [0x10],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1f52edb0b20 [0x14],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x3405ffea70 [1], Alignment=4,
SystemInformation=0x1f52edb0ed0, Length=0x50, ReturnLength=0x3405ffea68 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x1f52edb0c00 [0x18],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=9) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1f52edb0bf8 [0x1c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x18, WorkerProcessHandle=-1, StartRoutine=0x7ff81b97d110,
StartParameter=0x1f52edb0bc0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

```



```

NtCreateTimer2(TimerHandle=0x1f52edb0c50 [0x20], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x7ff800000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1f52edb0c58 [0x24],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x24, IoCompletionHandle=0x18,
TargetObjectHandle=0x20, KeyContext=0x1f52edb0c60, ApcContext=0x1f52edb0c30, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x3405ffea30 [0]) => 0

NtCreateTimer2(TimerHandle=0x1f52edb0cc8 [0xc], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x1f5000000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1f52edb0cd0 [0x28],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x28, IoCompletionHandle=0x18,
TargetObjectHandle=0xc, KeyContext=0x1f52edb0cd8, ApcContext=0x1f52edb0c30, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x3405ffea30 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x3405ffeb38, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0x3405ffeb38, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x1c, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x3405ffec58, BufferLength=4) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x14, IoCompletionHandle=0x18,
TargetObjectHandle=0x10, KeyContext=0x1f52edb0b38, ApcContext=0x1f52edb09b0,
IoStatus=0x000001f500000000, IoStatusInformation=0, AlreadySignaled=0x3405ffeca0
[0x2edb0b00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0x3405ffed58, InputBufferLength=4,
OutputBuffer=null, OutputBufferLength=0, ReturnLength=0x3405ffed10 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffedb8, InputBufferLength=0xa0,
OutputBuffer=0x3405ffedb8, OutputBufferLength=0xa0, ReturnLength=0x3405ffedb0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffedb8, InputBufferLength=0xa0,
OutputBuffer=0x3405ffedb8, OutputBufferLength=0xa0, ReturnLength=0x3405ffedb0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffedb8, InputBufferLength=0xa0,
OutputBuffer=0x3405ffedb8, OutputBufferLength=0xa0, ReturnLength=0x3405ffedb0 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe720 [0x000001f52edb2000],
ZeroBits=0, pSize=0x3405ffe7c8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffef00 [0x000001f52ec00000],
pSize=0x3405ffef08 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffeee0 [0x00007ff81bab1000],
Size=0x3405ffeed8 [0x4000], NewProtect=4, OldProtect=0x3405ffeed0 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ff81bab1298 [0x38], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffeee0 [0x00007ff81bab1000],
Size=0x3405ffeed8 [0x4000], NewProtect=2, OldProtect=0x3405ffeed0 [4]) => 0

```

```

NtOpenSymbolicLinkObject(LinkHandle=0x3405fff038 [0x3c], DesiredAccess=0x1,
ObjectAttributes=0x38:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x3c, LinkTarget="C:\Windows\System32",
ReturnedLength=0x3405ffefec [0x28]) => 0

NtClose(Handle=0x3c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffeeb0 [0x00007ff81bab1000],
Size=0x3405ffeea8 [0x4000], NewProtect=4, OldProtect=0x3405ffeea0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffeee0 [0x00007ff81bab1000],
Size=0x3405ffeed8 [0x4000], NewProtect=2, OldProtect=0x3405ffeed0 [4]) => 0

NtCreateEvent(EventHandle=0x7ff81ba9c380 [0x3c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ff81ba9c3b0 [0x40],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffee40 [0x00007ff81bab1000],
Size=0x3405ffee38 [0x4000], NewProtect=4, OldProtect=0x3405ffee30 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffee40 [0x00007ff81bab1000],
Size=0x3405ffee38 [0x4000], NewProtect=2, OldProtect=0x3405ffee30 [4]) => 0

NtOpenFile(FileHandle=0x3405ffeee8 [0x44], DesiredAccess=SYNCHRONIZE|0x20,
ObjectAttributes="??\D:\code\osi\", IoStatusBlock=0x3405ffee58 [0/1], ShareAccess=3,
OpenOptions=0x21) => 0

NtQueryVolumeInformationFile(FileHandle=0x44, IoStatusBlock=0x3405ffee58 [0/8],
FsInformation=0x3405ffee40, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtSetEvent(EventHandle=0x3c, PrevState=null) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0x3405ffeba0, Length=4) => 0

NtOpenSection(SectionHandle=0x3405ffeb78 [0x48], DesiredAccess=0xd,
ObjectAttributes=0x38:"KERNEL32.DLL") => 0

Loaded DLL at 00007FF81A810000 C:\Windows\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x48, ProcessHandle=-1, BaseAddress=0x1f52edb3660
[0x00007ff81a810000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb35c0
[0x0000c2000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x3405ffe9f0 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffea08 [0x00007ff81a8cf000],
Size=0x3405ffea00 [0x1000], NewProtect=2, OldProtect=0x3405ffea70 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffea00 [0x00007ff81bab1000],
Size=0x3405ffe9f8 [0x4000], NewProtect=4, OldProtect=0x3405ffe9f0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffea00 [0x00007ff81bab1000],
Size=0x3405ffe9f8 [0x4000], NewProtect=2, OldProtect=0x3405ffe9f0 [4]) => 0

```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffea50 [0x00007ff81a893000],
Size=0x3405ffea58 [0x4000], NewProtect=4, OldProtect=0x1f52edb35a8 [2]) => 0

NtOpenSection(SectionHandle=0x3405ffe4e8 [0x4c], DesiredAccess=0xd,
ObjectAttributes=0x38:"KERNELBASE.dll") => 0

Loaded DLL at 00007FF818FD0000 C:\Windows\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x4c, ProcessHandle=-1, BaseAddress=0x1f52edb3d40
[0x00007ff818fd0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb3ca0
[0x002fe000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x3405ffe360 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe378 [0x00007ff8192a3000],
Size=0x3405ffe370 [0x1000], NewProtect=2, OldProtect=0x3405ffe3e0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe370 [0x00007ff81bab1000],
Size=0x3405ffe368 [0x4000], NewProtect=4, OldProtect=0x3405ffe360 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe370 [0x00007ff81bab1000],
Size=0x3405ffe368 [0x4000], NewProtect=2, OldProtect=0x3405ffe360 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe3c0 [0x00007ff8191ba000],
Size=0x3405ffe3c8 [0x3000], NewProtect=4, OldProtect=0x1f52edb3c88 [2]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffd6a0 [0x000001f52edb4000],
ZeroBits=0, pSize=0x3405ffd748 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtClose(Handle=0x4c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb3588 [0x00007ff81a893000],
Size=0x1f52edb3590 [0x4000], NewProtect=2, OldProtect=0x3405ffe940 [4]) => 0

NtClose(Handle=0x48) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb3c68 [0x00007ff8191ba000],
Size=0x1f52edb3c70 [0x3000], NewProtect=2, OldProtect=0x3405ffea40 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x3405ffe9a0, Length=0x28) => 0

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

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffea60, VmInformation=0x3405ffeb38, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0x3405ffe6c0, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ff81928ee60, Length=0x40, ReturnLength=null) => 0

NtOpenSection(SectionHandle=0x3405ffe480 [0x48], DesiredAccess=0x4,
ObjectAttributes="\Sessions\2\Windows\SharedSection") => 0
```

```

NtCreateSection(SectionHandle=0x3405ffe4a0 [0x4c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0x3405ffe490 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ff81ba9cc48 [0x50], PortName="\Sessions\2\Windows\ApiPort",
SecurityQos=0x3405ffe5c0, ClientView=0x3405ffe4b8, ServerView=0x3405ffe4e8,
MaxMsgLength=0x3405ffe4b0 [0x3b8], ConnectionInfo=0x3405ffe530,
ConnectionInfoLength=0x3405ffe488 [0x30]) => 0

NtClose(Handle=0x4c) => 0

NtMapViewOfSection(SectionHandle=0x48, ProcessHandle=-1, BaseAddress=0x3405ffe498
[0x00007ff4604f0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x3405ffe4a8
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x48) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52ec00000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x3405ffe170, Length=0x30, ReturnLength=null) =>
0

NtInitializeNlsFiles(BaseAddress=0x3405ffe660 [0x000001f52ec60000],
DefaultLocaleId=0x7ff8192908f0 [0x419], DefaultCasingTableSize=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffd820 [0x000001f52edb5000],
ZeroBits=0, pSize=0x3405ffd8c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateFile(FileHandle=0x3405ffe6c8 [0x48], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f,
ObjectAttributes=4:"\Connect", IoStatusBlock=0x3405ffe080 [0/0x18], AllocationSize=null,
FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20,
EaBuffer=0x1f52edb4ae0, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x48, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x3405ffe610 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0x3405ffe630, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0x3405ffe638, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x48, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x3405ffe400, IoControlCode=0x00500016, InputBuffer=0x3405ffe410,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 'He
найдено указанное имя системного семафора.']]

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffe528, InputBufferLength=0xa0,
OutputBuffer=0x3405ffe528, OutputBufferLength=0xa0, ReturnLength=0x3405ffe520 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x3405ffe568, InputBufferLength=0x18,
OutputBuffer=0x3405ffe580, OutputBufferLength=0x78, ReturnLength=0x3405ffe560 [0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x3405ffe560 [0x60]) =>
0

NtQueryInformationToken(TokenHandle=0x60, TokenInformationClass=0xc [TokenSessionId],
TokenInformation=0x3405ffde80, Length=4, ReturnLength=0x3405ffde60 [4]) => 0

NtQueryInformationToken(TokenHandle=0x60, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0x3405ffdec8, Length=4, ReturnLength=0x3405ffde60 [4]) => 0

```

```

NtQueryInformationToken(TokenHandle=0x60, TokenInformationClass=0x2a
[TokenPrivateNameSpace], TokenInformation=0x3405ffde64, Length=4, ReturnLength=0x3405ffde60
[4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x3405ffde88 [0x64], DesiredAccess=0xf,
ObjectAttributes="\Sessions\2\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x60, TokenInformationClass=0x2c [TokenBnoIsolation],
TokenInformation=0x3405ffe180, Length=0x120, ReturnLength=0x3405ffde60 [0x10]) => 0

NtClose(Handle=0x60) => 0

NtCreateMutant(MutantHandle=0x3405ffe5b8 [0x60],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x64:"Local\SM0:14816:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x60, Alertable=false, Timeout=null) => 0

NtOpenSemaphore(SemaphoreHandle=0x3405ffe3a8,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x64:"Local\SM0:14816:304:WilStaging_02_p0") => 0xc0000034 [2 'Не удается
найти указанный файл.']]

NtCreateSemaphore(SemaphoreHandle=0x3405ffe298 [0x68],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x64:"Local\SM0:14816:304:WilStaging_02_p0", InitialCount=0x4bb6d304,
MaxCount=0x4bb6d304) => 0

NtCreateSemaphore(SemaphoreHandle=0x3405ffe298 [0x6c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x64:"Local\SM0:14816:304:WilStaging_02_p0h", InitialCount=0xfa,
MaxCount=0xfa) => 0

NtReleaseMutant(MutantHandle=0x60, PreviousCount=null) => 0

NtQueryWnfStateData(StateName=0x3405ffe610 [0xa3bc0875], TypeId=0x3405ffe6b8,
ExplicitScope=null, ChangeStamp=0x3405ffe604 [1], Buffer=0x3405ffd600,
BufferSize=0x3405ffe600 [8]) => 0

NtCreateEvent(EventHandle=0x3405ffe570 [0x70],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1f52edb52b0 [0x74],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x70) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x74, IoCompletionHandle=0x18,
TargetObjectHandle=0x70, KeyContext=0x1f52edb52c8, ApcContext=0x1f52edb5140,
IoStatus=0x000001f500000000, IoStatusInformation=0, AlreadySignaled=0x3405ffe4f0
[0x2edb0b00]) => 0

NtSubscribeWnfStateChange(StateName=0x1f52edb5440 [0xa3bc0875], ChangeStamp=1,
EventMask=0x11, SubscriptionId=0x3405ffe5e0 [0xd78b]) => 0

NtQueryWnfStateData(StateName=0x3405ffe750 [0xa3bc7c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0x3405ffe748 [0], Buffer=null, BufferSize=0x3405ffe74c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x1f52edb5770 [0xa3bc7c75], ChangeStamp=0,
EventMask=0x11, SubscriptionId=0x3405ffe5c0 [0xd78c]) => 0

```

```

NtQueryWnfStateData(StateName=0x3405ffe750 [0xa3bc88f5], TypeId=null, ExplicitScope=null,
ChangeStamp=0x3405ffe748 [0], Buffer=null, BufferSize=0x3405ffe74c [0]) => 0

NtSubscribeWnfStateChange(StateName=0x1f52edb5920 [0xa3bc88f5], ChangeStamp=0,
EventMask=0x11, SubscriptionId=0x3405ffe5c0 [0xd78d]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0x3405ffe500 [0], Alignment=0x18,
SystemInformation=0x3405ffe520, Length=0x50, ReturnLength=null) => 0

NtMapViewOfSection(SectionHandle=0x78, ProcessHandle=-1, BaseAddress=0x3405ffe4d0
[0x000001f52ec1000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x3405ffe4d8
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x7c, ProcessHandle=-1, BaseAddress=0x3405ffe4d0
[0x000001f52ed3000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x3405ffe4d8
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x80, ProcessHandle=-1, BaseAddress=0x3405ffe4d0
[0x000001f52ed4000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x3405ffe4d8
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0x78) => 0

NtClose(Handle=0x7c) => 0

NtClose(Handle=0x80) => 0

NtQueryWnfStateData(StateName=0x3405ffe508 [0xa3bc7c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0x3405ffe598 [0], Buffer=0x3405ffe5f0, BufferSize=0x3405ffe4f0 [0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffdf80 [0x000001f52edb6000],
ZeroBits=0, pSize=0x3405ffe028 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtSetTimer2(TimerHandle=0xc, DueTime=0x3405ffe580 [-3e+09], Period=null,
Parameters=0x3405ffe588) => 0

NtOpenKey(KeyHandle=0x3405ffe750, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\Redirect
tionMap\Keys") => 0xc0000034 [2 'Не удается найти указанный файл.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffe768, InputBufferLength=0xa0,
OutputBuffer=0x3405ffe768, OutputBufferLength=0xa0, ReturnLength=0x3405ffe760 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x3405ffe7a8, InputBufferLength=0x18,
OutputBuffer=0x3405ffe7c0, OutputBufferLength=0x78, ReturnLength=0x3405ffe7a0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffe798, InputBufferLength=0xa0,
OutputBuffer=0x3405ffe798, OutputBufferLength=0xa0, ReturnLength=0x3405ffe790 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x3405ffe7d8, InputBufferLength=0x18,
OutputBuffer=0x3405ffe7f0, OutputBufferLength=0x78, ReturnLength=0x3405ffe7d0 [0]) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffeaa0, VmInformation=0x3405ffeb78, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe6b0 [0x00007ff81bab1000],
Size=0x3405ffe6a8 [0x4000], NewProtect=4, OldProtect=0x3405ffe6a0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe6b0 [0x00007ff81bab1000],
Size=0x3405ffe6a8 [0x4000], NewProtect=2, OldProtect=0x3405ffe6a0 [4]) => 0

```

NtOpenKey(KeyHandle=0x3405ffe730 [0x78], DesiredAccess=KEY_READ, ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0

NtQueryValueKey(KeyHandle=0x78, ValueName="TSAppCompat", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1f52edb65a0, Length=0x224, ResultLength=0x3405ffe728) => 0xc0000034 [2 'Не удается найти указанный файл.']

NtQueryValueKey(KeyHandle=0x78, ValueName="TSUserEnabled", KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1f52edb65a0, Length=0x224, ResultLength=0x3405ffe728 [0x10]) => 0

NtClose(Handle=0x78) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffe588, InputBufferLength=0xa0, OutputBuffer=0x3405ffe588, OutputBufferLength=0xa0, ReturnLength=0x3405ffe580 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x3405ffe5c8, InputBufferLength=0x18, OutputBuffer=0x3405ffe5e0, OutputBufferLength=0x78, ReturnLength=0x3405ffe5c0 [0]) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation], SystemInformation=0x7ff81a8c7aa0, Length=0x40, ReturnLength=null) => 0

NtSetEvent(EventHandle=0x3c, PrevState=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000], Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

```

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000],
Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000],
Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000],
Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000],
Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000],
Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000],
Size=0x3405ffe7b0 [0x1000], NewProtect=4, OldProtect=0x3405ffe7c8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff8192a3000],
Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe7c8 [4]) => 0

NtOpenKey(KeyHandle=0x3405ffeda0, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0x3405ffed80, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") =>
0xc0000034 [2 'Не удается найти указанный файл.']]

NtOpenKey(KeyHandle=0x3405ffed78 [0x84], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0

NtQueryValueKey(KeyHandle=0x84, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x3405ffee30, Length=0x50,
ResultLength=0x3405ffed70) => 0xc0000034 [2 'Не удается найти указанный файл.']]

NtClose(Handle=0x84) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x3405ffec0, Length=0x58, ReturnLength=0x3405ffecb8 [0x2c]) => 0

NtOpenKey(KeyHandle=0x3405ffed78, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-
21-2308459876-1469942742-3350914452-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 'Не
удается найти указанный файл.']]

NtOpenKey(KeyHandle=0x3405ffee60 [0x84], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x84, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x3405ffeea0, Length=0x14,
ResultLength=0x3405ffee68 [0x10]) => 0

NtClose(Handle=0x84) => 0

NtOpenKey(KeyHandle=0x3405ffee60 [0x84], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

```



```

NtQueryValueKey(KeyHandle=0x84, ValueName="LPG0", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x3405ffeea0, Length=0x14,
ResultLength=0x3405ffee68) => 0xc0000034 [2 'Не удается найти указанный файл.']

NtClose(Handle=0x84) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0x3405ffee40, Length=4) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x3405ffedc0 [1], Alignment=4,
SystemInformation=0x1f52edb3c80, Length=0x50, ReturnLength=0x3405ffedb8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x1f52edb38c0 [0x84],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=9) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1f52edb38b8 [0x88],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x84, WorkerProcessHandle=-1, StartRoutine=0x7ff81b97d110,
StartParameter=0x1f52edb3880, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x88, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0x3405ffee88, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x1f52edb3910 [0x8c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1f52edb3918 [0x90],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x90, IoCompletionHandle=0x84,
TargetObjectHandle=0x8c, KeyContext=0x1f52edb3920, ApcContext=0x1f52edb38f0, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x3405ffed80 [0]) => 0

NtCreateTimer2(TimerHandle=0x1f52edb3988 [0x94], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x1f500000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1f52edb3990 [0x98],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x98, IoCompletionHandle=0x84,
TargetObjectHandle=0x94, KeyContext=0x1f52edb3998, ApcContext=0x1f52edb38f0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x3405ffed80 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x88, InformationClass=2
[WorkerFactoryIdleTimeout], Buffer=0x3405ffee88, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x88, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x3405ffee88, BufferLength=4) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x3405ffe910, Length=0x330, ReturnLength=0x3405ffe8c8) =>
0xc00000225 [1168 'Элемент не найден.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x3405ffe910, Length=0x330, ReturnLength=0x3405ffe8c8) =>
0xc00000225 [1168 'Элемент не найден.']

```

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffee90 [0x00007ff605728000], Size=0x3405ffee98 [0x1000], NewProtect=4, OldProtect=0x3405fff228 [8]) => 0

NtOpenSection(SectionHandle=0x3405ffe928 [0x9c], DesiredAccess=0xd, ObjectAttributes=0x38:"msvcrt.dll") => 0

Loaded DLL at 00007FF81A640000 C:\Windows\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0x9c, ProcessHandle=-1, BaseAddress=0x1f52edb6700 [0x00007ff81a640000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb3b30 [0x0009e000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x3405ffe7a0 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b0 [0x00007ff81bab1000], Size=0x3405ffe7a8 [0x4000], NewProtect=4, OldProtect=0x3405ffe7a0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b0 [0x00007ff81bab1000], Size=0x3405ffe7a8 [0x4000], NewProtect=2, OldProtect=0x3405ffe7a0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe800 [0x00007ff81a6b6000], Size=0x3405ffe808 [0x2000], NewProtect=4, OldProtect=0x1f52edb3b18 [2]) => 0

NtClose(Handle=0x9c) => 0

NtOpenSection(SectionHandle=0x3405ffe928 [0x9c], DesiredAccess=0xd, ObjectAttributes=0x38:"USER32.dll") => 0

Loaded DLL at 00007FF81A4A0000 C:\Windows\System32\USER32.dll

NtMapViewOfSection(SectionHandle=0x9c, ProcessHandle=-1, BaseAddress=0x1f52edb6b10 [0x00007ff81a4a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb6a70 [0x0019d000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x3405ffe7a0 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b8 [0x00007ff81a559000], Size=0x3405ffe7b0 [0x1000], NewProtect=2, OldProtect=0x3405ffe820 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b0 [0x00007ff81bab1000], Size=0x3405ffe7a8 [0x4000], NewProtect=4, OldProtect=0x3405ffe7a0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe7b0 [0x00007ff81bab1000], Size=0x3405ffe7a8 [0x4000], NewProtect=2, OldProtect=0x3405ffe7a0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe800 [0x00007ff81a52f000], Size=0x3405ffe808 [0x3000], NewProtect=4, OldProtect=0x1f52edb6a58 [2]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffdab0 [0x000001f52edb7000], ZeroBits=0, pSize=0x3405ffdb48 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenSection(SectionHandle=0x3405ffe298 [0xa0], DesiredAccess=0xd, ObjectAttributes=0x38:"win32u.dll") => 0

Loaded DLL at 00007FF819920000 C:\Windows\System32\win32u.dll

NtMapViewOfSection(SectionHandle=0xa0, ProcessHandle=-1, BaseAddress=0x1f52edb7030 [0x00007ff819920000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb6f90 [0x00022000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

```

NtQueryPerformanceCounter(Counter=0x3405ffe110 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe120 [0x00007ff81bab1000],
Size=0x3405ffe118 [0x4000], NewProtect=4, OldProtect=0x3405ffe110 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe120 [0x00007ff81bab1000],
Size=0x3405ffe118 [0x4000], NewProtect=2, OldProtect=0x3405ffe110 [4]) => 0

NtClose(Handle=0xa0) => 0

NtOpenSection(SectionHandle=0x3405ffe298 [0xa4], DesiredAccess=0xd,
ObjectAttributes=0x38:"GDI32.dll") => 0

Loaded DLL at 00007FF81AA20000 C:\Windows\System32\GDI32.dll

NtMapViewOfSection(SectionHandle=0xa4, ProcessHandle=-1, BaseAddress=0x1f52edb73d0
[0x00007ff81aa20000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb7330
[0x0002b000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x3405ffe110 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe128 [0x00007ff81aa47000],
Size=0x3405ffe120 [0x2000], NewProtect=2, OldProtect=0x3405ffe190 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe120 [0x00007ff81bab1000],
Size=0x3405ffe118 [0x4000], NewProtect=4, OldProtect=0x3405ffe110 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe120 [0x00007ff81bab1000],
Size=0x3405ffe118 [0x4000], NewProtect=2, OldProtect=0x3405ffe110 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe170 [0x00007ff81aa30000],
Size=0x3405ffe178 [0x1000], NewProtect=4, OldProtect=0x1f52edb7318 [2]) => 0

NtOpenSection(SectionHandle=0x3405ffdc08 [0xa8], DesiredAccess=0xd,
ObjectAttributes=0x38:"gdi32full.dll") => 0

Loaded DLL at 00007FF8192D0000 C:\Windows\System32\gdi32full.dll

NtMapViewOfSection(SectionHandle=0xa8, ProcessHandle=-1, BaseAddress=0x1f52edb78a0
[0x00007ff8192d0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb77d0
[0x00117000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x3405ffda80 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffda98 [0x00007ff8193d2000],
Size=0x3405ffda90 [0x1000], NewProtect=2, OldProtect=0x3405ffdb00 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffda90 [0x00007ff81bab1000],
Size=0x3405ffda88 [0x4000], NewProtect=4, OldProtect=0x3405ffda80 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffda90 [0x00007ff81bab1000],
Size=0x3405ffda88 [0x4000], NewProtect=2, OldProtect=0x3405ffda80 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdae0 [0x00007ff819380000],
Size=0x3405ffdae8 [0x3000], NewProtect=4, OldProtect=0x1f52edb77b8 [2]) => 0

NtOpenSection(SectionHandle=0x3405ffd578 [0xac], DesiredAccess=0xd,
ObjectAttributes=0x38:"msvc_p_win.dll") => 0

```

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffccc0 [0x000001f52edb8000], ZeroBits=0, pSize=0x3405ffcd68 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

Loaded DLL at 00007FF819560000 C:\Windows\System32\msvc_p_win.dll

NtMapViewOfSection(SectionHandle=0xac, ProcessHandle=-1, BaseAddress=0x1f52edb7e10 [0x00007ff819560000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb7d70 [0x0009d000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x3405ffd3f0 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffd408 [0x00007ff8195fa000], Size=0x3405ffd400 [0x1000], NewProtect=2, OldProtect=0x3405ffd470 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffd400 [0x00007ff81bab1000], Size=0x3405ffd3f8 [0x4000], NewProtect=4, OldProtect=0x3405ffd3f0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffd400 [0x00007ff81bab1000], Size=0x3405ffd3f8 [0x4000], NewProtect=2, OldProtect=0x3405ffd3f0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffd450 [0x00007ff8195b6000], Size=0x3405ffd458 [0x2000], NewProtect=4, OldProtect=0x1f52edb7d58 [2]) => 0

NtOpenSection(SectionHandle=0x3405ffcee8 [0xb0], DesiredAccess=0xd, ObjectAttributes=0x38:"ucrtbase.dll") => 0

Loaded DLL at 00007FF819820000 C:\Windows\System32\ucrtbase.dll

NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x1f52edb8300 [0x00007ff819820000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edb8230 [0x00100000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) => 0

NtQueryPerformanceCounter(Counter=0x3405ffcd60 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffcd70 [0x00007ff81bab1000], Size=0x3405ffcd68 [0x4000], NewProtect=4, OldProtect=0x3405ffcd60 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffcd70 [0x00007ff81bab1000], Size=0x3405ffcd68 [0x4000], NewProtect=2, OldProtect=0x3405ffcd60 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffcdc0 [0x00007ff8198d9000], Size=0x3405ffcdc8 [0x1000], NewProtect=4, OldProtect=0x1f52edb8218 [2]) => 0

NtClose(Handle=0xb0) => 0

NtClose(Handle=0xac) => 0

NtClose(Handle=0xa8) => 0

NtClose(Handle=0xa4) => 0

NtClose(Handle=0x9c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405fff208 [0x00007ff605728000], Size=0x3405fff210 [0x1000], NewProtect=8, OldProtect=0x3405ffed80 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb3af8 [0x00007ff81a6b6000], Size=0x1f52edb3b00 [0x2000], NewProtect=2, OldProtect=0x3405ffed60 [4]) => 0

```

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x3405ffecc0, Length=0x28) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb81f8 [0x00007ff8198d9000],
Size=0x1f52edb8200 [0x1000], NewProtect=2, OldProtect=0x3405ffed60 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb7d38 [0x00007ff8195b6000],
Size=0x1f52edb7d40 [0x2000], NewProtect=2, OldProtect=0x3405ffed60 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb7798 [0x00007ff819380000],
Size=0x1f52edb77a0 [0x3000], NewProtect=2, OldProtect=0x3405ffed60 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb72f8 [0x00007ff81aa30000],
Size=0x1f52edb7300 [0x1000], NewProtect=2, OldProtect=0x3405ffed60 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edb6a38 [0x00007ff81a52f000],
Size=0x1f52edb6a40 [0x3000], NewProtect=2, OldProtect=0x3405ffed60 [4]) => 0

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

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

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

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

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

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

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

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405fff0c8, VmInformation=0x3405ffeff0, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11
[ThreadHideFromDebugger], ThreadInformation=0x3405ffef00, Length=1, ReturnLength=null) => 0

Initial breakpoint

NtSetEvent(EventHandle=0x3c, PrevState=null) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x3405ffee40 [0x9c]) =>
0

NtQueryInformationToken(TokenHandle=0x9c, TokenInformationClass=0xa [TokenStatistics],
TokenInformation=0x3405ffee50, Length=0x38, ReturnLength=0x3405ffee48 [0x38]) => 0

NtClose(Handle=0x9c) => 0

NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode",
Type=0x3405ffed20 [4], Buffer=0x3405ffed10, Length=4, ReturnedLength=0x3405ffed28 [4]) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffedc0, VmInformation=0x3405ffee98, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe5f0 [0x000001f52eeb0000],
ZeroBits=0, pSize=0x3405ffe5f8 [0x001f0000], flAllocationType=0x2000, flProtect=4) => 0

```

```

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe5f0 [0x000001f52eeb0000],
pSize=0x3405ffe5e8 [0x001e0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe5d8 [0x000001f52f090000],
ZeroBits=0, pSize=0x3405ffe5d0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0xcc, IoStatusBlock=0x3405ffebc0 [0/8],
FsInformation=0x3405ffeb0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0x3405ffebc0 [0/8],
FsInformation=0x3405ffeb0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x5c, IoStatusBlock=0x3405ffebc0 [0/8],
FsInformation=0x3405ffeb0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe460 [0x000001f52edb9000],
ZeroBits=0, pSize=0x3405ffe508 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenKey(KeyHandle=0x3405ffd880 [0x9c], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions")
=> 0

NtQueryValueKey(KeyHandle=0x9c, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x3405ffdd60, Length=0x214,
ResultLength=0x3405ffdd18 [0x2a]) => 0

NtQueryValueKey(KeyHandle=0x9c, ValueName="000603xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x3405ffdd40, Length=0x214,
ResultLength=0x3405ffdaf8 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe430 [0x000001f52f092000],
ZeroBits=0, pSize=0x3405ffe4d8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe410 [0x000001f52f093000],
ZeroBits=0, pSize=0x3405ffe4b8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81a6c6998, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x3405ffe9b0, Length=0x18, ReturnLength=null) =>
0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffed80, VmInformation=0x3405ffee58, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffed40, VmInformation=0x3405ffee18, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQueryVolumeInformationFile(FileHandle=0xcc, IoStatusBlock=0x3405ffeb60 [0/8],
FsInformation=0x3405ffeb80, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x58, IoStatusBlock=0x3405ffeb60 [0/8],
FsInformation=0x3405ffeb80, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x5c, IoStatusBlock=0x3405ffeb60 [0/8],
FsInformation=0x3405ffeb80, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffe350 [0x000001f52edbb000],
ZeroBits=0, pSize=0x3405ffe3f8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

```

```

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffed80, VmInformation=0x3405ffee58, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffdc90 [0x000001f52edbd000],
ZeroBits=0, pSize=0x3405ffdd38 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffdc90 [0x000001f52edbe000],
ZeroBits=0, pSize=0x3405ffdd38 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffedc0, VmInformation=0x3405ffee98, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffedc0, VmInformation=0x3405ffee98, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x34
[ProcessMitigationPolicy], ProcessInformation=0x3405ffec40, Length=8, ReturnLength=null) =>
0

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffedc0, VmInformation=0x3405ffee98, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x3405ffe810, Length=0x40, ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe4b0 [0x00007ff81bab1000],
Size=0x3405ffe4a8 [0x4000], NewProtect=4, OldProtect=0x3405ffe4a0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffe4b0 [0x00007ff81bab1000],
Size=0x3405ffe4a8 [0x4000], NewProtect=2, OldProtect=0x3405ffe4a0 [4]) => 0

NtAlpcSendWaitReceivePort(PortHandle=0x50, SendFlags=0x00020000, SendMessage=0x3405ffe120 [2
[LPC_REPLY] (48b)], InMessageBuffer=null, ReceiveBuffer=0x3405ffe120,
ReceiveBufferSize=0x3405ffe0e0 [0x58], OutMessageBuffer=null, Timeout=null) => 0

NtQueryAttributesFile(ObjectAttributes="\??\C:\Windows\system32\IMM32.DLL",
Attributes=0x3405ffdd38 [ARCHIVE]) => 0

NtOpenFile(FileHandle=0x3405ffdd78 [0xa8], DesiredAccess=SYNCHRONIZE|0x1,
ObjectAttributes="\??\C:\Windows\system32\IMM32.DLL", IoStatusBlock=0x3405ffdd88 [0/1],
ShareAccess=5, OpenOptions=0x60) => 0

NtCreateSection(SectionHandle=0x3405ffdd70 [0xa4], DesiredAccess=0x4, ObjectAttributes=null,
SectionSize=null, Protect=2, Attributes=0x08000000, FileHandle=0xa8) => 0

NtMapViewOfSection(SectionHandle=0xa4, ProcessHandle=-1, BaseAddress=0x3405ffddf0
[0x000001f52ed60000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x3405ffde08
[0x0002e000], InheritDisposition=1 [ViewShare], AllocationType=0, Protect=2) => 0

NtUnmapViewOfSection(ProcessHandle=-1, BaseAddress=0x1f52ed60000) => 0

NtClose(Handle=0xa4) => 0

NtClose(Handle=0xa8) => 0

```

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x3405ffdf00, Length=0x330, ReturnLength=0x3405ffdeb8) =>
0xc0000225 [1168 'Элемент не найден.']

NtQuerySecurityAttributesToken(TokenHandle=-6, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x3405ffdf00, Length=0x330, ReturnLength=0x3405ffdeb8) =>
0xc0000225 [1168 'Элемент не найден.']

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0x3405ffdf00, Length=4) => 0

NtOpenSection(SectionHandle=0x3405ffded8 [0xac], DesiredAccess=0xd,
ObjectAttributes=0x38:"IMM32.DLL") => 0

Loaded DLL at 00007FF819950000 C:\Windows\System32\IMM32.DLL

NtMapViewOfSection(SectionHandle=0xac, ProcessHandle=-1, BaseAddress=0x1f52edbe1e0
[0x00007ff819950000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1f52edbe120
[0x0002f000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x3405ffdd50 [1.04914e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdd68 [0x00007ff819978000],
Size=0x3405ffdd60 [0x1000], NewProtect=2, OldProtect=0x3405ffddd0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdd60 [0x00007ff81bab1000],
Size=0x3405ffdd58 [0x4000], NewProtect=4, OldProtect=0x3405ffdd50 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdd60 [0x00007ff81bab1000],
Size=0x3405ffdd58 [0x4000], NewProtect=2, OldProtect=0x3405ffdd50 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffddb0 [0x00007ff81996f000],
Size=0x3405ffddb8 [0x1000], NewProtect=4, OldProtect=0x1f52edbe108 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1f52edbe0e8 [0x00007ff81996f000],
Size=0x1f52edbe0f0 [0x1000], NewProtect=2, OldProtect=0x3405ffdc0 [4]) => 0

NtClose(Handle=0xac) => 0

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

NtSetInformationVirtualMemory(ProcessHandle=-1, VmInformationClass=4, NumberOfEntries=1,
VirtualAddresses=0x3405ffde00, VmInformation=0x3405ffded8, VmInformationLength=4) =>
0xc00000bb [50 'Такой запрос не поддерживается.']

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x3405ffdc0, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x34
[ProcessMitigationPolicy], ProcessInformation=0x3405ffdc20, Length=8, ReturnLength=null) =>
0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x34
[ProcessMitigationPolicy], ProcessInformation=0x3405ffe500, Length=8, ReturnLength=null) =>
0

NtOpenKey(KeyHandle=0x3405ffe4b8, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Error Message
Instrument\") => 0xc0000034 [2 'Не удается найти указанный файл.']


```

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffe3b8, InputBufferLength=0xa0,
OutputBuffer=0x3405ffe3b8, OutputBufferLength=0xa0, ReturnLength=0x3405ffe3b0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x3405ffe3f8, InputBufferLength=0x18,
OutputBuffer=0x3405ffe410, OutputBufferLength=0x78, ReturnLength=0x3405ffe3f0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffe3b8, InputBufferLength=0xa0,
OutputBuffer=0x3405ffe3b8, OutputBufferLength=0xa0, ReturnLength=0x3405ffe3b0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x3405ffe3f8, InputBufferLength=0x18,
OutputBuffer=0x3405ffe410, OutputBufferLength=0x78, ReturnLength=0x3405ffe3f0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x3405ffe3b8, InputBufferLength=0xa0,
OutputBuffer=0x3405ffe3b8, OutputBufferLength=0xa0, ReturnLength=0x3405ffe3b0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x3405ffe3f8, InputBufferLength=0x18,
OutputBuffer=0x3405ffe410, OutputBufferLength=0x78, ReturnLength=0x3405ffe3f0 [0]) => 0

NtOpenKey(KeyHandle=0x3405ffddd8 [0xb0], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options") => 0

NtOpenKey(KeyHandle=0x3405ffdec0, DesiredAccess=0x9, ObjectAttributes=0xb0:"child.exe") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0x3405ffdfd8, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0x3405ffdfef, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0x3405ffdec0, DesiredAccess=0x9, ObjectAttributes=0xb0:"child.exe") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0x3405ffdfd8, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0x3405ffdfef, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Display") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtOpenKey(KeyHandle=0x3405ffe3f0 [0xa8], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows
NT\CurrentVersion\GRE_Initialize") => 0

NtQueryValueKey(KeyHandle=0xa8, ValueName="DisableMetaFiles", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x3405ffe440, Length=0x14,
ResultLength=0x3405ffe3f8) => 0xc0000034 [2 'Не удается найти указанный файл.']

NtClose(Handle=0xa8) => 0

NtOpenKey(KeyHandle=0x3405ffe3f0 [0xa4], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows
NT\CurrentVersion\GRE_Initialize") => 0

NtQueryValueKey(KeyHandle=0xa4, ValueName="DisableUmpdBufferSizeCheck",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x3405ffe440,
Length=0x14, ResultLength=0x3405ffe3f8) => 0xc0000034 [2 'Не удается найти указанный файл.']

```

NtClose(Handle=0xa4) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0x3405ffd610, Length=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x3405ffd340 [0x000001f52edbf000],
ZeroBits=0, pSize=0x3405ffd3e8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdaf8 [0x00007ff81aa47000],
Size=0x3405ffdaf0 [0x2000], NewProtect=4, OldProtect=0x3405ffdb08 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdaf8 [0x00007ff81aa47000],
Size=0x3405ffdaf0 [0x2000], NewProtect=2, OldProtect=0x3405ffdb08 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x5d
[ProcessLoaderDetour], ProcessInformation=0x3405ffd5e0, Length=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdac8 [0x00007ff81aa47000],
Size=0x3405ffdac0 [0x1000], NewProtect=4, OldProtect=0x3405ffdad8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x3405ffdac8 [0x00007ff81aa47000],
Size=0x3405ffdac0 [0x1000], NewProtect=2, OldProtect=0x3405ffdad8 [4]) => 0

NtQuerySystemInformation(SystemInformationClass=0x67 [SystemCodeIntegrityInformation],
SystemInformation=0x3405ffe1b0, Length=8, ReturnLength=null) => 0

NtOpenKey(KeyHandle=0x3405ffe440, DesiredAccess=0x9, ObjectAttributes=0xb0:"child.exe") =>
0xc0000034 [2 'Не удается найти указанный файл.']

NtSetEvent(EventHandle=0x3c, PrevState=null) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x88, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x3405fff228, BufferLength=4) => 0

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

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff605722540, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x3405fff530, Length=0x30,
ReturnLength=0x3405fff4e0 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff605722540, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x3405fff560, Length=0x30, ReturnLength=null)
=> 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff605722540, MemoryInformationClass=2
[MemoryMappedFilenameInformation], MemoryInformation=0x3405fff5d8, Length=0x21a,
ReturnLength=null) => 0

NtCreateFile(FileHandle=0x3405ffeff0 [0xd4], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80,
ObjectAttributes="\??\D:\code\osi\output.txt", IoStatusBlock=0x3405ffeff8 [0/2],
AllocationSize=null, FileAttributes=0x80, ShareAccess=0, CreateDisposition=5,
CreateOptions=0x60, EaBuffer=null, EaLength=0) => 0

NtReadFile(FileHandle=0xcc, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x3405fff120 [0/0xe], Buffer=0x3405fff2c0, Length=0x400, ByteOffset=null,
Key=null) => 0

NtWriteFile(FileHandle=0xd4, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x3405fff130 [0/5], Buffer=0x3405fff190, Length=5, ByteOffset=null, Key=null)
=> 0

```
NtWriteFile(FileHandle=0xd4, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x3405fff130 [0/6], Buffer=0x3405fff190, Length=6, ByteOffset=null, Key=null)
=> 0
```

```
NtReadFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131ff280 [0/0xd], Buffer=0xa3131ff950, Length=0x400, ByteOffset=null,
Key=null) => 0
```

```
NtWriteFile(FileHandle=0xd0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131ff290 [0/0xd], Buffer=0xa3131ff950, Length=0xd, ByteOffset=null,
Key=null) => 0
```

```
NtReadFile(FileHandle=0xcc, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x3405fff120 [0/0xd], Buffer=0x3405fff2c0, Length=0x400, ByteOffset=null,
Key=null) => 0
```

```
NtWriteFile(FileHandle=0xd4, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x3405fff130 [0/5], Buffer=0x3405fff190, Length=5, ByteOffset=null, Key=null)
=> 0
```

```
NtReadFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0xa3131ff280 [0x101/0], Buffer=0xa3131ff950, Length=0x400, ByteOffset=null,
Key=null) => 0x101 [739 'ERROR_ALERTED']
```

```
Created thread: 9832 at 00007FF819063950
```

```
Created thread: 11116 at 00007FF819063950
```

```
NtDeviceIoControlFile(FileHandle=0x48, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x34061fef90, IoControlCode=0x00500016, InputBuffer=0x34061fef90,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 'He
найдено указанное имя системного семафора.']
```

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

```
NtSetEvent(EventHandle=0x3c, PrevState=null) => 0
```

```
NtTestAlert() => 0
```

```
Exception: c000001d at 00007FF81B9CD6A4 (first chance)
```

```
Exception: c000001d at 00007FF81B9CD6A4 (last chance)
```

```
NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=3 [ThreadBasePriority],
ThreadInformation=0x34061ff9c8, Length=4) => 0
```

```
Exception: 40010005 at 00007FF8190B4747 (first chance)
```

```
NtTerminateProcess(ProcessHandle=0, ExitStatus=0xc000013a) => 0
```

```
Thread 7192 exit code: 3221225786
```

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

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

```
NtClose(Handle=0xa0) => 0
```

```
NtOpenKey(KeyHandle=0x34061fef10 [0xa0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows
NT\CurrentVersion\GRE_Initialize") => 0
```

```
NtQueryValueKey(KeyHandle=0xa0, ValueName="DisableMetaFiles", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x34061fef60, Length=0x14,
ResultLength=0x34061fef18) => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtClose(Handle=0xa0) => 0

NtOpenKey(KeyHandle=0x34061fef10 [0xa0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows
NT\CurrentVersion\GRE_Initialize") => 0

NtQueryValueKey(KeyHandle=0xa0, ValueName="DisableUmpdBufferSizeCheck",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x34061fef60,
Length=0x14, ResultLength=0x34061fef18) => 0xc0000034 [2 'Не удастся найти указанный файл.']

NtClose(Handle=0xa0) => 0

NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0xa [ThreadZeroTlsCell],
ThreadInformation=0x34061fe0, Length=4) => 0

NtSetInformationThread(ThreadHandle=-2, ThreadInformationClass=0xa [ThreadZeroTlsCell],
ThreadInformation=0x34061ff6f0, Length=4) => 0

NtClose(Handle=0x78) => 0

NtClose(Handle=0x4c) => 0

NtClose(Handle=0x80) => 0

NtClose(Handle=0x7c) => 0

NtQueryWnfStateData(StateName=0x34061ff500 [0xa3bc1c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0x34061fe444 [0x00017748], Buffer=0x34061fe4a0, BufferSize=0x34061fe440 [0x8c4])
=> 0

NtQueryWnfStateData(StateName=0x34061ff388 [0xa3bc7c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0x34061ff418 [0], Buffer=0x34061ff470, BufferSize=0x34061ff370 [0]) => 0

Process 14816 exit code: 3221225786

Detached
```

Вывод

В ходе выполнения работы была разработана программа, реализующая взаимодействие между родительским и дочерним процессами через pipe в Windows. Родительский процесс передает данные дочернему, который обрабатывает их и записывает результат в файл. Были использованы системные вызовы CreateProcess, CreatePipe, ReadFile, WriteFile, CloseHandle, WaitForSingleObject.

Возникли сложности с корректной обработкой имени файла, переданного дочернему процессу. Потребовалось уделить внимание обработке переносов строк (CRLF) в Windows, чтобы избежать ошибок при чтении имени файла.