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: Демидов М.С.

Преподаватель: Бахарев В.Д. (ФИИТ)

Оценка: ____________________

Дата: 19.10.24

Москва, 2024

Постановка задачи

Вариант 3.

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 принеобходимости 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». Далее эти числа передаются от родительского процесса в дочерний. Дочерний процесс производит деление первого числа, на последующие, а результат выводит в файл. Если происходит деление на 0, то тогда дочерний и родительский процесс завершают свою работу. Проверка деления на 0 должна осуществляться на стороне дочернего процесса. Числа имеют тип int. Количество чисел может быть произвольным.

Общий метод и алгоритм решения

Использованные системные вызовы:

- CreateNamedPipe; – создает канал.
- WriteFile; – записывает данные в канал.
- ReadFile; – читает данные из канала.
- CloseHandle; – закрывает хендлеры, в том числе и каналы.
- ConnectNamedPipe; – позволяет работать с ранее созданным каналом.
- GetStdHandle; – Возвращает хендлер по DWORD.
- CreateFile; – Создает файл.

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

Затем шла работа над parent.c. Вся суть заключается в том, чтобы считать имя файла, в который выведется результат, затем считать строку с числами. После этого все данные отправляются в child.c, который, в свою очередь, создает и открывает файл, а потом записывает в него через пробел результаты деления первого числа на остальные.

Код программы

demidovStdio.h

```
#define INITIAL_BUFFER_SIZE 128

  #include <windows.h>
  #include <stdarg.h>
  #include <string.h>

  enum ret_type_t{
      SUCCESS,    //Successful end
      ERROR_ARGS_COUNT,    //Wrong args number
      ERROR_CREATE_PIPE,  //Failed to create a new pipeline
      ERROR_CREATE_CHILD_PROCESS, //Failed to create a child process
      ERROR_READ, //Failed to read from pipe
      ERROR_DEV_ZERO, //Devision by zero detected
      ERROR_FULL, //Overflow
      ERROR_OPEN_FILE,    //Error with file opening
      ERROR_CLOSE_FILE,   //Error with closing file
      ERROR_FILE_WRITE,   //Error with file writing
      ERROR_HANDLER_INHERITED, //Error handler reading
      ERROR_PIPE_WRITE,   //Failed to write smth in the pipe
      ERROR_HEAP,         //Failed to malloc
  };

  //THE MOST POWERFUL PRINTF IN HISTORY
  void demidov_printf(const char *format, ...) {
      va_list args;
      va_start(args, format);

      char buffer[1024];
      char* buf_ptr = buffer;
      const char* fmt_ptr = format;
      int buffer_size = sizeof(buffer);

      while (*fmt_ptr) {
          if (*fmt_ptr == '%') {

              fmt_ptr++;

              switch (*fmt_ptr) {

                  case 'd': {

                      int value = va_arg(args, int);

                      char num_buffer[20];

                      char* num_ptr = num_buffer;

                      if (value < 0) {

                          *buf_ptr++ = '-';

                          value = -value;

                      }

                      do {

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

                          value /= 10;

                      } while (value > 0);

                      while (num_ptr > num_buffer) {

                          *buf_ptr++ = *--num_ptr;

                      }

                      break;

                  }

                  case 's': {

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

                      while (*str) {

                          *buf_ptr++ = *str++;

                      }

                      break;

                  }

                  case 'c': {

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

                      *buf_ptr++ = ch;

                      break;

                  }

                  case '%': {
                      *buf_ptr++ = '%';
                      break;
                  }
                  default:
                      *buf_ptr++ = *fmt_ptr;
                      break;
              }
          } else {
              *buf_ptr++ = *fmt_ptr;
          }
          fmt_ptr++;
      }
      *buf_ptr = '\0';

      va_end(args);

      HANDLE hConsole = GetStdHandle(STD_OUTPUT_HANDLE);
      DWORD bytesWritten;
      WriteConsoleA(hConsole, buffer, (DWORD)(buf_ptr - buffer), &bytesWritten, NULL);
}

//Printf for files
int demidov_file_printf(HANDLE fileHandle, const char *format, ...) {
    va_list args;
    va_start(args, format);

    char buffer[1024];
    char* buf_ptr = buffer;
    const char* fmt_ptr = format;
    int buffer_size = sizeof(buffer);

    while (*fmt_ptr) {
        if (*fmt_ptr == '%') {
```

```
        fmt_ptr++;
        switch (*fmt_ptr) {
            case 'd': {
                int value = va_arg(args, int);
                char num_buffer[20];
                char* num_ptr = num_buffer;
                if (value < 0) {
                    *buf_ptr++ = '-';
                    value = -value;
                }
                do {
                    *num_ptr++ = (char)((value % 10) + '0');
                    value /= 10;
                } while (value > 0);
                while (num_ptr > num_buffer) {
                    *buf_ptr++ = *--num_ptr;
                }
                break;
            }
            case 's': {
                const char* str = va_arg(args, const char*);
                while (*str) {
                    *buf_ptr++ = *str++;
                }
                break;
            }
            case 'c': {
                char ch = (char)va_arg(args, int);
                *buf_ptr++ = ch;
                break;
            }
            case '%': {
                *buf_ptr++ = '%';
```

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

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

    va_end(args);
}
```

parent.c

```
#include <windows.h>
#include <string.h>
#include <stdio.h>
#include "demidovStdio.h"

#define BUFFER_SIZE 1024

int main() {
    HANDLE hPipe1, hPipe2;
    char pipeName1[] = "\\\\.\\pipe\\Pipe1";
    char pipeName2[] = "\\\\.\\pipe\\Pipe2";
    char fileName[BUFFER_SIZE];
    char buffer[BUFFER_SIZE];
    DWORD bytesRead, bytesWritten;

    hPipe1 = CreateNamedPipe(pipeName1, PIPE_ACCESS_OUTBOUND, PIPE_TYPE_BYTE | PIPE_WAIT, 1, 0, 0, 0, NULL);
    if (hPipe1 == INVALID_HANDLE_VALUE) {
        demidov_printf("Failed to create named pipe");
        return ERROR_CREATE_PIPE;
    }

    hPipe2 = CreateNamedPipe(pipeName2, PIPE_ACCESS_INBOUND, PIPE_TYPE_BYTE | PIPE_WAIT, 1, 0, 0, 0, NULL);
    if (hPipe2 == INVALID_HANDLE_VALUE) {
        CloseHandle(hPipe1);
        demidov_printf("Failed to create named pipe");
        return ERROR_CREATE_PIPE;
    }

    WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), "Enter file name: ", strlen("Enter file name: "), &bytesWritten, NULL);
    ReadFile(GetStdHandle(STD_INPUT_HANDLE), fileName, BUFFER_SIZE, &bytesRead, NULL);
    fileName[bytesRead - 2] = '\0';

    STARTUPINFO si;
    PROCESS_INFORMATION pi;
    ZeroMemory(&si, sizeof(si));
    si.cb = sizeof(si);
    ZeroMemory(&pi, sizeof(pi));

    char cmdLine[BUFFER_SIZE];
    snprintf(cmdLine, BUFFER_SIZE, "child.exe %s", fileName);


    if (!CreateProcess(NULL, cmdLine, NULL, NULL, FALSE, 0, NULL, NULL, &si, &pi)) {
        CloseHandle(hPipe1);
        CloseHandle(hPipe2);
        demidov_printf("Failed to create process");
        return ERROR_CREATE_CHILD_PROCESS;
    }


    ConnectNamedPipe(hPipe1, NULL);


    ConnectNamedPipe(hPipe2, NULL);


    WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), "Enter command: ", strlen("Enter command: "), &bytesWritten, NULL);
    ReadFile(GetStdHandle(STD_INPUT_HANDLE), buffer, BUFFER_SIZE, &bytesRead, NULL);


    WriteFile(hPipe1, buffer, bytesRead, &bytesWritten, NULL);


    char response[BUFFER_SIZE];
    ReadFile(hPipe2, response, BUFFER_SIZE, &bytesRead, NULL);
    if (strcmp(response, "DIVIDE_BY_ZERO") == 0) {
        WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), "Division by zero detected. Exiting...\n", strlen("Division by zero detected. Exiting...\n"), &bytesWritten, NULL);
    }


    CloseHandle(hPipe1);
    CloseHandle(hPipe2);
    CloseHandle(pi.hProcess);
    CloseHandle(pi.hThread);
    return SUCCESS;
}
```

child.c

```
#include <windows.h>
#include <string.h>
#include <stdio.h>
#include "demidovStdio.h"

#define BUFFER_SIZE 1024

int main(int argc, char* argv[]) {
    HANDLE hPipe1, hPipe2;
    char pipeName1[] = "\\\\.\\pipe\\Pipe1";
    char pipeName2[] = "\\\\.\\pipe\\Pipe2";
    char buffer[BUFFER_SIZE];
    DWORD bytesRead, bytesWritten;
    char* fileName = (char*)malloc(BUFFER_SIZE * sizeof(char*));

    //Проверка на память

    HANDLE hFile;

    if (argc < 2) {
        demidov_printf("Wrong args count");
        return ERROR_ARGS_COUNT;
    }

    //snprintf(fileName, BUFFER_SIZE, argv[1]);
    fileName = argv[1];


    hPipe1 = CreateFile(pipeName1, GENERIC_READ, 0, NULL, OPEN_EXISTING, 0, NULL);
    if (hPipe1 == INVALID_HANDLE_VALUE) {
        demidov_printf("Failed to create named pipe");
        return ERROR_CREATE_PIPE;
    }


    hPipe2 = CreateFile(pipeName2, GENERIC_WRITE, 0, NULL, OPEN_EXISTING, 0, NULL);
    if (hPipe2 == INVALID_HANDLE_VALUE) {
        CloseHandle(hPipe1);
        demidov_printf("Failed to create named pipe");
        return ERROR_CREATE_PIPE;
    }


    hFile = CreateFile(((fileName)), GENERIC_WRITE, 0, NULL, CREATE_ALWAYS, FILE_ATTRIBUTE_NORMAL, NULL);


    if (hFile == INVALID_HANDLE_VALUE) {
        CloseHandle(hPipe1);
        CloseHandle(hPipe2);
        demidov_printf("Failed to open file");
        return ERROR_OPEN_FILE;
    }


    ReadFile(hPipe1, buffer, BUFFER_SIZE, &bytesRead, NULL);


    int numbers[BUFFER_SIZE];
    int count = 0;
    char* token = strtok(buffer, " ");
```

```
        while (token != NULL) {
            numbers[count++] = atoi(token);
            token = strtok(NULL, " ");
        }

        int result = numbers[0];
        char* write = (char*)malloc(BUFFER_SIZE * sizeof(char*));

        for (int i = 1; i < count; i++) {
            if (numbers[i] == 0) {
                WriteFile(hPipe2, "DIVIDE_BY_ZERO", strlen("DIVIDE_BY_ZERO"), &bytesWritten, NULL);
                CloseHandle(hPipe1);
                CloseHandle(hPipe2);
                CloseHandle(hFile);
                return ERROR_DEV_ZERO;
            }
            snprintf(write, BUFFER_SIZE, "%d ", result / numbers[i]);
            demidov_file_printf(hFile, write, strlen(write), &bytesWritten, NULL);
        }

        CloseHandle(hPipe1);
        CloseHandle(hPipe2);
        CloseHandle(hFile);

        return SUCCESS;
    }
```

Протокол работы программы

```
Process 118680 starting at 00007FF62EC213E0 with command line:
"D:\Users\lenovo\Desktop\try\OSmai\parent.exe"

D:\Users\lenovo\Desktop\try\OSmai\parent.exe

Loaded DLL at 00007FF81A370000 ntdll.dll

NtQueryPerformanceCounter(Counter=0x248fdff8f0 [4.15848e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff938 [0x00007ff81a50e000],
Size=0x248fdff930 [0x1000], NewProtect=4, OldProtect=0x248fdff970 [8]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff938 [0x00007ff81a50e000],
Size=0x248fdff930 [0x1000], NewProtect=8, OldProtect=0x248fdff970 [4]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81a414140, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x248fdff8c0, Length=0x18, ReturnLength=null) =>
0

NtCreateEvent(EventHandle=0x7ff81a4f6398 [8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtManageHotPatch(Unknown=9, Unknown=0x248fdff758 [1], Unknown=8, Unknown=0x248fdff750) =>
0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

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

NtCreateEvent(EventHandle=0x7ff81a4f63e8 [0xc],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x248fdff670, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x248fdff368, Length=4, ReturnLength=null) => 0

NtOpenKey(KeyHandle=0x248fdff218 [0x10], DesiredAccess=GENERIC_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\CodePage") => 0

NtQueryValueKey(KeyHandle=0x10, ValueName="ACP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff280, Length=0x24,
ResultLength=0x248fdff210 [0x16]) => 0

NtQueryValueKey(KeyHandle=0x10, ValueName="OEMCP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff280, Length=0x24,
ResultLength=0x248fdff210 [0x14]) => 0

NtClose(Handle=0x10) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x7ff81a4f37e0 [0x000001eb8c600000], SectionSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x7ff81a4f37e8 [0x000001eb8c620000], SectionSize=null) => 0
```

```
NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x248fdff308 [0x000001eb8c640000], SectionSize=null) => 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0x248fdff2c0, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81a370000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x248fdff250, Length=0x18, ReturnLength=null) =>
0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0x248fdff290, Length=0x50,
ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff2e0 [0x00007ff81a50b000],
Size=0x248fdff2d8 [0x4000], NewProtect=2, OldProtect=0x248fdff2d0 [4]) => 0

NtOpenKey(KeyHandle=0x248fdfef90 [0x10], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x10, ValueName="RaiseExceptionOnPossibleDeadlock",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x248fdfefa0,
Length=0x50, ResultLength=0x248fdfef98) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x10) => 0

NtOpenKey(KeyHandle=0x248fdfef28 [0x10], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options") => 0

NtOpenKey(KeyHandle=0x248fdff010, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdfef70, DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager\Segment
Heap") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x7ff81a4f7268, Length=4, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x248fdff278, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x248fdfec10, Length=0x330, ReturnLength=0x248fdfebc8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x248fdfec10, Length=0x330, ReturnLength=0x248fdfebc8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtOpenKey(KeyHandle=0x248fdff1c0 [0x14], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x14, ValueName="ResourcePolicies", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff200, Length=0x18,
ResultLength=0x248fdff1c8) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x14) => 0
```

```
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x248fdff2d0, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x248fdff270, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation],
SystemInformation=0x248fdff2a0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81a4f7a88 [0x00007ff520350000],
ZeroBits=0x000000248fdff220, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x248fdff168, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81a4f7a80 [0x00007ff522350000],
ZeroBits=0x000000248fdff228, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null,
DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81a4f7af0 [0x00007ff420330000],
ZeroBits=0x000000248fdff1d0, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x248fdff118, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x248fdff110, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfecf0 [0x000001eb8c650000],
ZeroBits=0, pSize=0x248fdfecf8 [0x00220000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfecf0 [0x000001eb8c650000],
pSize=0x248fdfece8 [0x00120000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfecd8 [0x000001eb8c770000],
ZeroBits=0, pSize=0x248fdfecd0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5
[SystemHypervisorSharedPageInformation], SystemInformation=0x248fdff470, Length=8,
ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap],
SystemInformation=0x248fdfeee0, Length=0x408, ReturnLength=0x248fdff300 [0x18]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x248fdfeec8 [4], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x248fdfeec0) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x248fdfeec8 [4], Alignment=4,
SystemInformation=0x1eb8c770880, Length=0x50, ReturnLength=0x248fdfeec0 [0x50]) => 0

NtCreateEvent(EventHandle=0x248fdff0b8 [0x14],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1eb8c770c40 [0x18],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x248fdfee30 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x248fdfee28) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']
```

```
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x248fdfee30 [6], Alignment=4,
SystemInformation=0x1eb8c770ff0, Length=0x30, ReturnLength=0x248fdfee28 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x1eb8c770d20 [0x1c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1eb8c770d18 [0x20],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x1c, WorkerProcessHandle=-1, StartRoutine=0x7ff81a3a5550,
StartParameter=0x1eb8c770ce0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x1eb8c770d70 [0x24], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1eb8c770d78 [0x28],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x28, IoCompletionHandle=0x1c,
TargetObjectHandle=0x24, KeyContext=0x1eb8c770d80, ApcContext=0x1eb8c770d50, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x248fdfedf0 [0]) => 0

NtCreateTimer2(TimerHandle=0x1eb8c770de8 [0x2c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x1eb00000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1eb8c770df0 [0x30],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x30, IoCompletionHandle=0x1c,
TargetObjectHandle=0x2c, KeyContext=0x1eb8c770df8, ApcContext=0x1eb8c770d50, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x248fdfedf0 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x20, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x248fdfeed8, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x20, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0x248fdfeed8, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x20, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x248fdfeff8, BufferLength=4) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x18, IoCompletionHandle=0x1c,
TargetObjectHandle=0x14, KeyContext=0x1eb8c770c58, ApcContext=0x1eb8c770ad0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x248fdff040 [0x8c770c00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0x248fdff0f8, InputBufferLength=4,
OutputBuffer=null, OutputBufferLength=0, ReturnLength=0x248fdff0b0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdff158, InputBufferLength=0xa0,
OutputBuffer=0x248fdff158, OutputBufferLength=0xa0, ReturnLength=0x248fdff150 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdff1a8, InputBufferLength=0x18,
OutputBuffer=0x248fdff1c0, OutputBufferLength=0x78, ReturnLength=0x248fdff1a0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdff1a8, InputBufferLength=0xa0,
OutputBuffer=0x248fdff1a8, OutputBufferLength=0xa0, ReturnLength=0x248fdff1a0 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdff1a8, InputBufferLength=0xa0,
OutputBuffer=0x248fdff1a8, OutputBufferLength=0xa0, ReturnLength=0x248fdff1a0 [0xa0]) => 0
```

```
NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdff158, InputBufferLength=0xa0,
OutputBuffer=0x248fdff158, OutputBufferLength=0xa0, ReturnLength=0x248fdff150 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdff1a8, InputBufferLength=0x18,
OutputBuffer=0x248fdff1c0, OutputBufferLength=0x78, ReturnLength=0x248fdff1a0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdff1a8, InputBufferLength=0xa0,
OutputBuffer=0x248fdff1a8, OutputBufferLength=0xa0, ReturnLength=0x248fdff1a0 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfeae0 [0x000001eb8c772000],
ZeroBits=0, pSize=0x248fdfeb88 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfe700 [0x000001eb8c774000],
ZeroBits=0, pSize=0x248fdfe7a8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdff300 [0x000001eb8c590000],
pSize=0x248fdff308 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff2e0 [0x00007ff81a50b000],
Size=0x248fdff2d8 [0x4000], NewProtect=4, OldProtect=0x248fdff2d0 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ff81a50b2b0 [0x48], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff2e0 [0x00007ff81a50b000],
Size=0x248fdff2d8 [0x4000], NewProtect=2, OldProtect=0x248fdff2d0 [4]) => 0

NtOpenSymbolicLinkObject(LinkHandle=0x248fdff458 [0x4c], DesiredAccess=0x1,
ObjectAttributes=0x48:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x4c, LinkTarget="C:\WINDOWS\System32",
ReturnedLength=0x248fdff3f0 [0x28]) => 0

NtClose(Handle=0x4c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff2b0 [0x00007ff81a50b000],
Size=0x248fdff2a8 [0x4000], NewProtect=4, OldProtect=0x248fdff2a0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff2e0 [0x00007ff81a50b000],
Size=0x248fdff2d8 [0x4000], NewProtect=2, OldProtect=0x248fdff2d0 [4]) => 0

NtCreateEvent(EventHandle=0x7ff81a4f62d8 [0x4c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ff81a4f6310 [0x50],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfeae0 [0x000001eb8c775000],
ZeroBits=0, pSize=0x248fdfeb88 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff240 [0x00007ff81a50b000],
Size=0x248fdff238 [0x4000], NewProtect=4, OldProtect=0x248fdff230 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff240 [0x00007ff81a50b000],
Size=0x248fdff238 [0x4000], NewProtect=2, OldProtect=0x248fdff230 [4]) => 0

NtOpenFile(FileHandle=0x248fdff2e8 [0x54], DesiredAccess=SYNCHRONIZE|0x20,
ObjectAttributes="\??\D:\Users\lenovo\Desktop\try\OSmai\", IoStatusBlock=0x248fdff258 [0/1],
ShareAccess=3, OpenOptions=0x21) => 0
```

```
NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0x248fdff258 [0/8],
FsInformation=0x248fdff240, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

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

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x248fdfefb0) => 0xc000007c [1008 '╧юя√Єъp ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

NtOpenSection(SectionHandle=0x248fdfef48 [0x58], DesiredAccess=0xd,
ObjectAttributes=0x48:"KERNEL32.DLL") => 0

Loaded DLL at 00007FF818C40000 C:\WINDOWS\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x58, ProcessHandle=-1, BaseAddress=0x1eb8c775500
[0x00007ff818c40000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1eb8c775458
[0x000c4000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x248fdfeda0 [4.15848e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfed30 [0x00007ff818d01000],
Size=0x248fdfed28 [0x1000], NewProtect=2, OldProtect=0x248fdfed20 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfedb0 [0x00007ff81a50b000],
Size=0x248fdfeda8 [0x4000], NewProtect=4, OldProtect=0x248fdfeda0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfedb0 [0x00007ff81a50b000],
Size=0x248fdfeda8 [0x4000], NewProtect=2, OldProtect=0x248fdfeda0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfedf0 [0x00007ff818cc3000],
Size=0x248fdfedf8 [0x4000], NewProtect=4, OldProtect=0x1eb8c775440 [2]) => 0

NtOpenSection(SectionHandle=0x248fdfe7e8 [0x5c], DesiredAccess=0xd,
ObjectAttributes=0x48:"KERNELBASE.dll") => 0

Loaded DLL at 00007FF817890000 C:\WINDOWS\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x1eb8c775c40
[0x00007ff817890000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1eb8c775b98
[0x003b7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x248fdfe640 [4.15848e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfe5d0 [0x00007ff817c15000],
Size=0x248fdfe5c8 [0x1000], NewProtect=2, OldProtect=0x248fdfe5c0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfe650 [0x00007ff81a50b000],
Size=0x248fdfe648 [0x4000], NewProtect=4, OldProtect=0x248fdfe640 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfe650 [0x00007ff81a50b000],
Size=0x248fdfe648 [0x4000], NewProtect=2, OldProtect=0x248fdfe640 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfe690 [0x00007ff817afe000],
Size=0x248fdfe698 [0x2000], NewProtect=4, OldProtect=0x1eb8c775b80 [2]) => 0

NtClose(Handle=0x5c) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1eb8c775420 [0x00007ff818cc3000],
Size=0x1eb8c775428 [0x4000], NewProtect=2, OldProtect=0x248fdfebf0 [4]) => 0

NtClose(Handle=0x58) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1eb8c775b60 [0x00007ff817afe000],
Size=0x1eb8c775b68 [0x2000], NewProtect=2, OldProtect=0x248fdfed30 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x248fdfec90, Length=0x28) => 0

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

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

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0x248fdfea70, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ff817bf6e80, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfdff0 [0x000001eb8c776000],
ZeroBits=0, pSize=0x248fdfe098 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenSection(SectionHandle=0x248fdfe830 [0x5c], DesiredAccess=0x4,
ObjectAttributes="\Sessions\8\Windows\SharedSection") => 0

NtCreateSection(SectionHandle=0x248fdfe850 [0x60],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0x248fdfe840 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ff81a4f6c08 [0x70], PortName="\Sessions\8\Windows\ApiPort",
SecurityQos=0x248fdfe970, ClientView=0x248fdfe868, ServerView=0x248fdfe898,
MaxMsgLength=0x248fdfe860 [0x3b8], ConnectionInfo=0x248fdfe8e0,
ConnectionInfoLength=0x248fdfe838 [0x30]) => 0

NtClose(Handle=0x60) => 0

NtMapViewOfSection(SectionHandle=0x5c, ProcessHandle=-1, BaseAddress=0x248fdfe848
[0x00007ff420230000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x248fdfe858
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x5c) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x1eb8c590000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x248fdfe530, Length=0x30, ReturnLength=null) =>
0

NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x248fdfea18 [0x000001eb8c5a0000], SectionSize=null) => 0

NtInitializeNlsFiles(BaseAddress=0x248fdfea10 [0x000001eb8c650000],
DefaultLocaleId=0x7ff817bf8b88 [0x419], DefaultCasingTableSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x248fdfe9f0 [0x000001eb8c720000], SectionSize=0x248fdfe9b8 [0x00011000]) =>
0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x248fdfe9f0 [0x000001eb8c740000], SectionSize=0x248fdfe9b8 [0x00011000]) =>
0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfe160 [0x000001eb8c777000],
ZeroBits=0, pSize=0x248fdfe208 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
```

```
NtCreateFile(FileHandle=0x248fdfea78 [0x5c], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f,
ObjectAttributes=4:"\Connect", IoStatusBlock=0x248fdfe430 [0/0x18], AllocationSize=null,
FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20,
EaBuffer=0x1eb8c7770f0, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x5c, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfe9c0 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0x248fdfe9e0, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0x248fdfe9e8, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x5c, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfe7b0, IoControlCode=0x00500016, InputBuffer=0x248fdfe7c0,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfe8c8, InputBufferLength=0xa0,
OutputBuffer=0x248fdfe8c8, OutputBufferLength=0xa0, ReturnLength=0x248fdfe8c0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfe918, InputBufferLength=0x18,
OutputBuffer=0x248fdfe930, OutputBufferLength=0x78, ReturnLength=0x248fdfe910 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfeb28, InputBufferLength=0xa0,
OutputBuffer=0x248fdfeb28, OutputBufferLength=0xa0, ReturnLength=0x248fdfeb20 [0xa0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x248fdfe8d0 [0x74]) =>
0

NtQueryInformationToken(TokenHandle=0x74, TokenInformationClass=0xc [TokenSessionId],
TokenInformation=0x248fdfe1f0, Length=4, ReturnLength=0x248fdfe1d0 [4]) => 0

NtQueryInformationToken(TokenHandle=0x74, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0x248fdfe238, Length=4, ReturnLength=0x248fdfe1d0 [4]) => 0

NtQueryInformationToken(TokenHandle=0x74, TokenInformationClass=0x2a
[TokenPrivateNameSpace], TokenInformation=0x248fdfe1d4, Length=4, ReturnLength=0x248fdfe1d0
[4]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x248fdfe1f8 [0x78], DesiredAccess=0xf,
ObjectAttributes="\Sessions\8\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x74, TokenInformationClass=0x2c [TokenBnoIsolation],
TokenInformation=0x248fdfe4f0, Length=0x120, ReturnLength=0x248fdfe1d0 [0x10]) => 0

NtClose(Handle=0x74) => 0

NtCreateMutant(MutantHandle=0x248fdfe928 [0x74],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x78:"Local\SM0:118680:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x74, Alertable=false, Timeout=null) => 0

NtOpenSemaphore(SemaphoreHandle=0x248fdfe6e8,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x78:"Local\SM0:118680:304:WilStaging_02_p0") => 0xc0000034 [2 '=x
єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
```

```
NtCreateSemaphore(SemaphoreHandle=0x248fdfe648 [0x7c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x78:"Local\SM0:118680:304:WilStaging_02_p0", InitialCount=0x631ddcd4,
MaxCount=0x631ddcd4) => 0

NtCreateSemaphore(SemaphoreHandle=0x248fdfe648 [0x80],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x78:"Local\SM0:118680:304:WilStaging_02_p0h", InitialCount=0xf5,
MaxCount=0xf5) => 0

NtReleaseMutant(MutantHandle=0x74, PreviousCount=null) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfeb08, InputBufferLength=0xa0,
OutputBuffer=0x248fdfeb08, OutputBufferLength=0xa0, ReturnLength=0x248fdfeb00 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfeb58, InputBufferLength=0x18,
OutputBuffer=0x248fdfeb70, OutputBufferLength=0x78, ReturnLength=0x248fdfeb50 [0]) => 0

NtQueryWnfStateData(StateName=0x248fdfe9f0 [0xa3bc0875], TypeId=0x248fdfea98,
ExplicitScope=null, ChangeStamp=0x248fdfe9e4 [0xe], Buffer=0x248fdfd9e0,
BufferSize=0x248fdfe9e0 [8]) => 0

NtCreateEvent(EventHandle=0x248fdfe960 [0x88],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1eb8c777b20 [0x8c],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x88) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x8c, IoCompletionHandle=0x1c,
TargetObjectHandle=0x88, KeyContext=0x1eb8c777b38, ApcContext=0x1eb8c7779b0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x248fdfe8e0 [0x8c770c00]) => 0

NtSubscribeWnfStateChange(StateName=0x1eb8c777cb0 [0xa3bc0875], ChangeStamp=0xe,
EventMask=0x11, SubscriptionId=0x248fdfe9d0 [0x00019974]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0x248fdfe850 [0], Alignment=0x18,
SystemInformation=0x248fdfe870, Length=0x50, ReturnLength=null) => 0

NtMapViewOfSection(SectionHandle=0x90, ProcessHandle=-1, BaseAddress=0x248fdfe7e0
[0x000001eb8c760000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x248fdfe7f0
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x94, ProcessHandle=-1, BaseAddress=0x248fdfe7e0
[0x000001eb8c870000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x248fdfe7f0
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x98, ProcessHandle=-1, BaseAddress=0x248fdfe7e0
[0x000001eb8c880000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x248fdfe7f0
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0x90) => 0

NtClose(Handle=0x94) => 0

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

```
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfd4a0 [0x000001eb8c778000],
ZeroBits=0, pSize=0x248fdfd548 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtSetTimer2(TimerHandle=0x2c, DueTime=0x248fdfe960 [-3e+09], Period=null,
Parameters=0x248fdfe968) => 0

NtOpenKey(KeyHandle=0x248fdfeb00, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\Redirec
tionMap\Keys") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfeb08, InputBufferLength=0xa0,
OutputBuffer=0x248fdfeb08, OutputBufferLength=0xa0, ReturnLength=0x248fdfeb00 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfeb58, InputBufferLength=0x18,
OutputBuffer=0x248fdfeb70, OutputBufferLength=0x78, ReturnLength=0x248fdfeb50 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfeb38, InputBufferLength=0xa0,
OutputBuffer=0x248fdfeb38, OutputBufferLength=0xa0, ReturnLength=0x248fdfeb30 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfeb88, InputBufferLength=0x18,
OutputBuffer=0x248fdfeba0, OutputBufferLength=0x78, ReturnLength=0x248fdfeb80 [0]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfea50 [0x00007ff81a50b000],
Size=0x248fdfea48 [0x4000], NewProtect=4, OldProtect=0x248fdfea40 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfea50 [0x00007ff81a50b000],
Size=0x248fdfea48 [0x4000], NewProtect=2, OldProtect=0x248fdfea40 [4]) => 0

NtOpenKey(KeyHandle=0x248fdfea20, DesiredAccess=0x9, ObjectAttributes=0x10:"parent.exe") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdfead8 [0xa0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0

NtQueryValueKey(KeyHandle=0xa0, ValueName="TSAppCompat", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x1eb8c778860, Length=0x224,
ResultLength=0x248fdfeac8) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xa0, ValueName="TSUserEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x1eb8c778860, Length=0x224,
ResultLength=0x248fdfeac8 [0x10]) => 0

NtClose(Handle=0xa0) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ff818cf9a80, Length=0x40, ReturnLength=null) => 0

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

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=4, OldProtect=0x248fdfebe8 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfebd8 [0x00007ff817c15000],
Size=0x248fdfebd0 [0x1000], NewProtect=2, OldProtect=0x248fdfebe8 [4]) => 0

NtOpenKey(KeyHandle=0x248fdff1a0, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdff180 [0x94], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0
```

```
NtQueryKey(KeyHandle=0x94, KeyInformationClass=2 [KeyFullInformation],
KeyInformation=0x248fdff1f8, Length=0x30, ResultLength=0x248fdff170 [0x2c]) => 0

NtClose(Handle=0x94) => 0

NtOpenKey(KeyHandle=0x248fdff178 [0x94], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0

NtQueryValueKey(KeyHandle=0x94, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff230, Length=0x50,
ResultLength=0x248fdff170) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x94) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdff0a0, Length=0x58, ReturnLength=0x248fdff098 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdff178, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-
21-3512441621-816733789-498939024-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '=х
єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdff250 [0xa0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0xa0, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff290, Length=0x14,
ResultLength=0x248fdff258 [0x10]) => 0

NtClose(Handle=0xa0) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x248fdff1e0 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x248fdff1d8) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x248fdff1e0 [6], Alignment=4,
SystemInformation=0x1eb8c775bb0, Length=0x30, ReturnLength=0x248fdff1d8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x1eb8c775780 [0xa4],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1eb8c775778 [0xa0],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0xa4, WorkerProcessHandle=-1, StartRoutine=0x7ff81a3a5550,
StartParameter=0x1eb8c775740, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0x248fdff288, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x1eb8c7757d0 [0xa8], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1eb8c7757d8 [0x94],
DesiredAccess=0x1, ObjectAttributes=null) => 0
```

```
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x94, IoCompletionHandle=0xa4,
TargetObjectHandle=0xa8, KeyContext=0x1eb8c7757e0, ApcContext=0x1eb8c7757b0, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x248fdff1a0 [0]) => 0

NtCreateTimer2(TimerHandle=0x1eb8c775848 [0xac], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x1eb00000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1eb8c775850 [0x90],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x90, IoCompletionHandle=0xa4,
TargetObjectHandle=0xac, KeyContext=0x1eb8c775858, ApcContext=0x1eb8c7757b0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x248fdff1a0 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=2
[WorkerFactoryIdleTimeout], Buffer=0x248fdff288, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x248fdff288, BufferLength=4) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x248fdff300) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·щщ Єюъхэ.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff280 [0x00007ff62ec2f000],
Size=0x248fdff288 [0x1000], NewProtect=4, OldProtect=0x248fdff5d0 [8]) => 0

NtOpenSection(SectionHandle=0x248fdfec78 [0xb0], DesiredAccess=0xd,
ObjectAttributes=0x48:"msvcrt.dll") => 0

Loaded DLL at 00007FF8190A0000 C:\WINDOWS\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x1eb8c778890
[0x00007ff8190a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1eb8c7759f8
[0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x248fdfead0 [4.15848e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfeae0 [0x00007ff81a50b000],
Size=0x248fdfead8 [0x4000], NewProtect=4, OldProtect=0x248fdfead0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfeae0 [0x00007ff81a50b000],
Size=0x248fdfead8 [0x4000], NewProtect=2, OldProtect=0x248fdfead0 [4]) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x248fdfe590, Length=0x330, ReturnLength=0x248fdfe548) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x248fdfe590, Length=0x330, ReturnLength=0x248fdfe548) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff8190a0000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x248fdfe808, Length=0x30, ReturnLength=null)
=> 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfeb20 [0x00007ff81911e000],
Size=0x248fdfeb28 [0x1000], NewProtect=4, OldProtect=0x1eb8c7759e0 [2]) => 0

NtClose(Handle=0xb0) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdff5b0 [0x00007ff62ec2f000],
Size=0x248fdff5b8 [0x1000], NewProtect=8, OldProtect=0x248fdff080 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1eb8c7759c0 [0x00007ff81911e000],
Size=0x1eb8c7759c8 [0x1000], NewProtect=2, OldProtect=0x248fdff080 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x248fdfefe0, Length=0x28) => 0

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

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

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11
[ThreadHideFromDebugger], ThreadInformation=0x248fdff300, Length=1, ReturnLength=null) => 0

Initial breakpoint

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

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x248fdff270 [0xb0]) =>
0

NtQueryInformationToken(TokenHandle=0xb0, TokenInformationClass=0xa [TokenStatistics],
TokenInformation=0x248fdff280, Length=0x38, ReturnLength=0x248fdff278 [0x38]) => 0

NtClose(Handle=0xb0) => 0

NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode",
Type=0x248fdfee7c [4], Buffer=0x248fdfee70, Length=4, ReturnedLength=0x248fdfee74 [4]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfea10 [0x000001eb8c890000],
ZeroBits=0, pSize=0x248fdfea18 [0x001b0000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfea10 [0x000001eb8c890000],
pSize=0x248fdfea08 [0x001a0000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfe9f8 [0x000001eb8ca30000],
ZeroBits=0, pSize=0x248fdfe9f0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0x248fdfefc0 [0/8],
FsInformation=0x248fdfefe0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0xbe0, IoStatusBlock=0x248fdfefc0 [0/8],
FsInformation=0x248fdfefe0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0x6c, IoStatusBlock=0x248fdfefc0 [0/8],
FsInformation=0x248fdfefe0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfe820 [0x000001eb8c779000],
ZeroBits=0, pSize=0x248fdfe8c8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfe7d0 [0x000001eb8ca32000],
ZeroBits=0, pSize=0x248fdfe878 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenKey(KeyHandle=0x248fdfdd00 [0xb0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions")
=> 0

NtQueryValueKey(KeyHandle=0xb0, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x248fdfe1e0, Length=0x214,
ResultLength=0x248fdfe188 [0x2a]) => 0
```

```
NtQueryValueKey(KeyHandle=0xb0, ValueName="000604xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x248fdfe1c0, Length=0x214,
ResultLength=0x248fdfdf68 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfe7d0 [0x000001eb8ca33000],
ZeroBits=0, pSize=0x248fdfe878 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81912ed28, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x248fdfedf0, Length=0x18, ReturnLength=null) =>
0

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

NtOpenKey(KeyHandle=0x248fdff300 [0xb4], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelaySleepLoopWindowSize",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x248fdff260,
Length=0x50, ResultLength=0x248fdff250) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelaySpinCountThreshold",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x248fdff260,
Length=0x50, ResultLength=0x248fdff250) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelayBaseYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff260, Length=0x50,
ResultLength=0x248fdff250) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtFactorYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff260, Length=0x50,
ResultLength=0x248fdff250) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelayMaxYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdff260, Length=0x50,
ResultLength=0x248fdff250) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xb4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa0, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x248fdff5d8, BufferLength=4) => 0

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

NtTestAlert() => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff62ec22790, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x248fdffb20, Length=0x30,
ReturnLength=0x248fdffad0 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff62ec22790, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x248fdffb50, Length=0x30, ReturnLength=null)
=> 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff62ec22790, MemoryInformationClass=2
[MemoryMappedFilenameInformation], MemoryInformation=0x248fdffbc8, Length=0x21a,
ReturnLength=null) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=4 [TokenOwner],
TokenInformation=0x1eb8c778a90, Length=0x4c, ReturnLength=0x248fdfeaf4 [0x24]) => 0
```

```
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0x248fdfeaf0, Length=4, ReturnLength=0x248fdfeaf4 [4]) => 0

NtCreateNamedPipeFile(NamedPipeHandle=0x248fdfebd0 [0xb8],
DesiredAccess=SYNCHRONIZE|GENERIC_WRITE, ObjectAttributes="\??\pipe\Pipe1",
IoStatusBlock=0x248fdfec20 [0/2], ShareAccess=1, CreateDisposition=3, CreateOptions=0x20,
MessageType=false, MessageRead=false, NonBlocking=false, MaxInstances=1, InBufferSize=0,
OutBufferSize=0, Timeout=0x248fdfebc8 [-500000]) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=4 [TokenOwner],
TokenInformation=0x1eb8c778a90, Length=0x4c, ReturnLength=0x248fdfeaf4 [0x24]) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0x248fdfeaf0, Length=4, ReturnLength=0x248fdfeaf4 [4]) => 0

NtCreateNamedPipeFile(NamedPipeHandle=0x248fdfebd0 [0xb4],
DesiredAccess=SYNCHRONIZE|GENERIC_READ, ObjectAttributes="\??\pipe\Pipe2",
IoStatusBlock=0x248fdfec20 [0/2], ShareAccess=2, CreateDisposition=3, CreateOptions=0x20,
MessageType=false, MessageRead=false, NonBlocking=false, MaxInstances=1, InBufferSize=0,
OutBufferSize=0, Timeout=0x248fdfebc8 [-500000]) => 0

Enter file name: NtWriteFile(FileHandle=0xbe0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfecc0 [0/0x11], Buffer=0x7ff62ec2a01c, Length=0x11, ByteOffset=null,
Key=null) => 0

NtReadFile(FileHandle=0x64, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfecc0 [0/0xa], Buffer=0x248fdff9c0, Length=0x400, ByteOffset=null,
Key=null) => 0

NtQueryAttributesFile(ObjectAttributes="\??\D:\Users\lenovo\Desktop\try\OSmai\child.exe",
Attributes=0x248fdfccc0 [ARCHIVE]) => 0

NtQueryAttributesFile(ObjectAttributes="\??\D:\Users\lenovo\Desktop\try\OSmai\child.exe",
Attributes=0x248fdfd098 [ARCHIVE]) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x248fdfc520) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

NtOpenSection(SectionHandle=0x248fdfc4b8 [0xbc], DesiredAccess=0xd,
ObjectAttributes=0x48:"sechost.dll") => 0

Loaded DLL at 00007FF81A0F0000 C:\WINDOWS\System32\sechost.dll

NtMapViewOfSection(SectionHandle=0xbc, ProcessHandle=-1, BaseAddress=0x1eb8c77a990
[0x00007ff81a0f0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1eb8c7759f8
[0x000a8000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x248fdfc310 [4.15881e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfc2a0 [0x00007ff81a193000],
Size=0x248fdfc298 [0x1000], NewProtect=2, OldProtect=0x248fdfc290 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfc320 [0x00007ff81a50b000],
Size=0x248fdfc318 [0x4000], NewProtect=4, OldProtect=0x248fdfc310 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfc320 [0x00007ff81a50b000],
Size=0x248fdfc318 [0x4000], NewProtect=2, OldProtect=0x248fdfc310 [4]) => 0
```

```
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81a0f0000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x248fdfc048, Length=0x30, ReturnLength=null)
=> 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfc360 [0x00007ff81a16d000],
Size=0x248fdfc368 [0x2000], NewProtect=4, OldProtect=0x1eb8c7759e0 [2]) => 0

NtOpenSection(SectionHandle=0x248fdfbd58 [0xc0], DesiredAccess=0xd,
ObjectAttributes=0x48:"bcrypt.dll") => 0

Loaded DLL at 00007FF8177C0000 C:\WINDOWS\System32\bcrypt.dll

NtMapViewOfSection(SectionHandle=0xc0, ProcessHandle=-1, BaseAddress=0x1eb8c77ae20
[0x00007ff8177c0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1eb8c77ad88
[0x00028000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x248fdfbbb0 [4.15881e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfbb40 [0x00007ff8177e5000],
Size=0x248fdfbb38 [0x1000], NewProtect=2, OldProtect=0x248fdfbb30 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfbbc0 [0x00007ff81a50b000],
Size=0x248fdfbbb8 [0x4000], NewProtect=4, OldProtect=0x248fdfbbb0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfbbc0 [0x00007ff81a50b000],
Size=0x248fdfbbb8 [0x4000], NewProtect=2, OldProtect=0x248fdfbbb0 [4]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff8177c0000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x248fdfb8e8, Length=0x30, ReturnLength=null)
=> 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfbc00 [0x00007ff8177dc000],
Size=0x248fdfbc08 [0x1000], NewProtect=4, OldProtect=0x1eb8c77ad70 [2]) => 0

NtClose(Handle=0xc0) => 0

NtClose(Handle=0xbc) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1eb8c77ad50 [0x00007ff8177dc000],
Size=0x1eb8c77ad58 [0x1000], NewProtect=2, OldProtect=0x248fdfc2a0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1eb8c7759c0 [0x00007ff81a16d000],
Size=0x1eb8c7759c8 [0x2000], NewProtect=2, OldProtect=0x248fdfc2a0 [4]) => 0

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

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

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfc078, InputBufferLength=0xa0,
OutputBuffer=0x248fdfc078, OutputBufferLength=0xa0, ReturnLength=0x248fdfc070 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfc0d8, InputBufferLength=0xa0,
OutputBuffer=0x248fdfc0d8, OutputBufferLength=0xa0, ReturnLength=0x248fdfc0d0 [0xa0]) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x56
[ProcessEnclaveInformation], ProcessInformation=0x248fdfc160, Length=0xb0,
ReturnLength=null) => 0xc0000003 [87 '╧рЁрьхЄЁ чрфрэ эхтхЁэю.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0
[ProcessBasicInformation], ProcessInformation=0x248fdfc0e0, Length=0x40, ReturnLength=null)
=> 0
```

```
NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfc088, InputBufferLength=0xa0,
OutputBuffer=0x248fdfc088, OutputBufferLength=0xa0, ReturnLength=0x248fdfc080 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfc0d8, InputBufferLength=0x18,
OutputBuffer=0x248fdfc0f0, OutputBufferLength=0x78, ReturnLength=0x248fdfc0d0 [0]) => 0

NtCreateSemaphore(SemaphoreHandle=0x248fdfc098 [0xbc], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0

NtCreateSemaphore(SemaphoreHandle=0x248fdfc0a8 [0xcc], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0

NtCreateEvent(EventHandle=0x248fdfc098 [0xd0],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtOpenFile(FileHandle=0x7ff8177e27a0 [0xd4], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes="\Device\KsecDD", IoStatusBlock=0x248fdfbfe0 [0/0], ShareAccess=7,
OpenOptions=0x20) => 0

NtDeviceIoControlFile(FileHandle=0xd4, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfc080 [0/0], IoControlCode=0x00390400, InputBuffer=0x248fdfc160,
InputBufferLength=0x68, OutputBuffer=0x248fdfc090, OutputBufferLength=8) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfb910 [0x000001eb8c77b000],
ZeroBits=0, pSize=0x248fdfb9b8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfc038, InputBufferLength=0xa0,
OutputBuffer=0x248fdfc038, OutputBufferLength=0xa0, ReturnLength=0x248fdfc030 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfc088, InputBufferLength=0x18,
OutputBuffer=0x248fdfc0a0, OutputBufferLength=0x78, ReturnLength=0x248fdfc080 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfc038, InputBufferLength=0xa0,
OutputBuffer=0x248fdfc038, OutputBufferLength=0xa0, ReturnLength=0x248fdfc030 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfc088, InputBufferLength=0x18,
OutputBuffer=0x248fdfc0a0, OutputBufferLength=0x78, ReturnLength=0x248fdfc080 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfc068, InputBufferLength=0xa0,
OutputBuffer=0x248fdfc068, OutputBufferLength=0xa0, ReturnLength=0x248fdfc060 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x248fdfc0b8, InputBufferLength=0x18,
OutputBuffer=0x248fdfc0d0, OutputBufferLength=0x78, ReturnLength=0x248fdfc0b0 [0]) => 0

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

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfc9f8 [0x00007ff817c15000],
Size=0x248fdfc9f0 [0x1000], NewProtect=4, OldProtect=0x248fdfca08 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x248fdfc9f8 [0x00007ff817c15000],
Size=0x248fdfc9f0 [0x1000], NewProtect=2, OldProtect=0x248fdfca08 [4]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfc300 [0x000001eb8c77c000],
ZeroBits=0, pSize=0x248fdfc3a8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenKey(KeyHandle=0x248fdfd050, DesiredAccess=0x9, ObjectAttributes=0x10:"child.exe") =>
0xc0000034 [2 '=x єфрxЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdfd030, DesiredAccess=0x101,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Wow64\x86\xtajit") => 0xc0000034 [2
'=x єфрxЄё  эрщЄш єърчрээ√щ Їрщы.']
```

```
NtCreateUserProcess(ProcessHandle=0x248fdfd1e0 [0xe8], ThreadHandle=0x248fdfd260 [0xe4],
ProcessDesiredAccess=MAXIMUM_ALLOWED, ThreadDesiredAccess=MAXIMUM_ALLOWED,
ProcessObjectAttributes=null, ThreadObjectAttributes=null, ProcessFlags=0x200,
ThreadFlags=1, ProcessParameters=0x1eb8c77b850
["D:\Users\lenovo\Desktop\try\OSmai\child.exe"], CreateInfo=0x248fdfd530,
AttributeList=0x248fdfd9d0) => 0

NtOpenKey(KeyHandle=0x248fdfd0f8, DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session
Manager\AppCertDlls") => 0xc0000034 [2 '=x єфрxЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0xa, TokenHandle=0x248fdfcdb0 [0xf4]) =>
0

NtQueryInformationToken(TokenHandle=0xf4, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfd000, Length=0x90, ReturnLength=0x248fdfcdd8 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfcdd0, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '=x єфрxЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdfcd98 [0xf8], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0

NtQueryValueKey(KeyHandle=0xf8, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdfcee0, Length=0x50,
ResultLength=0x248fdfcd90) => 0xc0000034 [2 '=x єфрxЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xf8, ValueName="AuthenticodeEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x248fdfcee0, Length=0x50,
ResultLength=0x248fdfcd90 [0x10]) => 0

NtClose(Handle=0xf8) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfccc0, Length=0x58, ReturnLength=0x248fdfccb8 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfcd98, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-
21-3512441621-816733789-498939024-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '=x
єфрxЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xf4) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x248fdfce58, InputBufferLength=0xa0,
OutputBuffer=0x248fdfce58, OutputBufferLength=0xa0, ReturnLength=0x248fdfce50 [0xa0]) => 0

NtQueryInformationProcess(ProcessHandle=0xe8, ProcessInformationClass=0x3c
[ProcessCommandLineInformation], ProcessInformation=0x1eb8c77d0b0, Length=0x400,
ReturnLength=0x248fdfcd80 [0x36]) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap],
ProcessInformation=0x248fdfc860, Length=0x24, ReturnLength=null) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfca00, Length=0x54, ReturnLength=0x248fdfc9e0 [0x2c]) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap],
ProcessInformation=0x248fdfc7f0, Length=0x24, ReturnLength=null) => 0
```

```
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfcba0, Length=0x58, ReturnLength=0x248fdfcb98 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfcd18 [0xf4], DesiredAccess=0x1,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-
1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders") => 0

NtQueryValueKey(KeyHandle=0xf4, ValueName="Cache", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x1eb8c77d720, Length=0x208,
ResultLength=0x248fdfcd10 [0x94]) => 0

NtClose(Handle=0xf4) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfcba0, Length=0x58, ReturnLength=0x248fdfcb98 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfccc0 [0xf4], DesiredAccess=0x8,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-
1001\Software\Microsoft\Windows NT\CurrentVersion") => 0

NtOpenKey(KeyHandle=0x248fdfccc8 [0xf8], DesiredAccess=0x101,
ObjectAttributes=0xf4:"AppCompatFlags\Layers") => 0

NtQueryValueKey(KeyHandle=0xf8, ValueName="D:\Users\lenovo\Desktop\try\OSmai\child.exe",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x248fdfcd28,
Length=0x10, ResultLength=0x248fdfccd0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xf8) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x248fdfc580 [0x000001eb8c77e000],
ZeroBits=0, pSize=0x248fdfc628 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

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

NtQueryInformationProcess(ProcessHandle=0xe8, ProcessInformationClass=0
[ProcessBasicInformation], ProcessInformation=0x248fdfd020, Length=0x40, ReturnLength=null)
=> 0

NtOpenKey(KeyHandle=0x248fdfcdd0 [0x100], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide")
=> 0

NtQueryValueKey(KeyHandle=0x100, ValueName="PreferExternalManifest",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x248fdfce20,
Length=0x14, ResultLength=0x248fdfcdd8) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x100) => 0

NtQueryVolumeInformationFile(FileHandle=0xec, IoStatusBlock=0x248fdfce30 [0/8],
FsInformation=0x248fdfce60, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtGetMUIRegistryInfo(Flags=0, BufferLength=0x248fdfcc50 [0x4d0], Buffer=null) => 0

NtGetMUIRegistryInfo(Flags=0, BufferLength=0x248fdfcc50 [0x4d0], Buffer=0x1eb8c77b850) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfca80, Length=0x58, ReturnLength=0x248fdfca78 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfcc68 [0x100], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0
```

```
NtOpenKey(KeyHandle=0x248fdfcc60, DesiredAccess=KEY_READ, ObjectAttributes=0x100:"Control
Panel\Desktop\MuiCached\MachineLanguageConfiguration") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш
єърчрээ√щ Їрщы.']

NtClose(Handle=0x100) => 0

NtOpenKey(KeyHandle=0x248fdfcaf8, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034
[2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfc990, Length=0x58, ReturnLength=0x248fdfc988 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfcb00 [0xf8], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0

NtOpenKey(KeyHandle=0x248fdfcb08, DesiredAccess=KEY_READ,
ObjectAttributes=0xf8:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2
'=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdfcaf8, DesiredAccess=KEY_READ, ObjectAttributes=0xf8:"Control
Panel\Desktop\LanguageConfiguration") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xf8) => 0

NtOpenKey(KeyHandle=0x248fdfca98, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034
[2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfc900, Length=0x58, ReturnLength=0x248fdfc8f8 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfca90 [0x100], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0

NtOpenKey(KeyHandle=0x248fdfc9c0, DesiredAccess=KEY_READ,
ObjectAttributes=0x100:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2
'=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x248fdfca88 [0xf8], DesiredAccess=KEY_READ,
ObjectAttributes=0x100:"Control Panel\Desktop") => 0

NtQueryValueKey(KeyHandle=0xf8, ValueName="PreferredUILanguages", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x1eb8c779a00, Length=0xc,
ResultLength=0x248fdfca58) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xf8) => 0

NtClose(Handle=0x100) => 0

NtOpenKey(KeyHandle=0x248fdfca98, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\MUI\Settings") => 0xc0000034
[2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x248fdfc900, Length=0x58, ReturnLength=0x248fdfc8f8 [0x2c]) => 0

NtOpenKey(KeyHandle=0x248fdfca90 [0x100], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0

NtOpenKey(KeyHandle=0x248fdfca88 [0xf8], DesiredAccess=KEY_READ,
ObjectAttributes=0x100:"Control Panel\Desktop\MuiCached") => 0
```

```
NtQueryValueKey(KeyHandle=0xf8, ValueName="MachinePreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1eb8c779a00,
Length=0xc, ResultLength=0x248fdfca58) => 0x80000005 [234 '╚ьх■Єё  фюяюыэшЄхы№э√х фрээ√х.']

NtQueryValueKey(KeyHandle=0xf8, ValueName="MachinePreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1eb8c778200,
Length=0x18, ResultLength=0x248fdfca58 [0x18]) => 0

NtClose(Handle=0xf8) => 0

NtClose(Handle=0x100) => 0

NtAlpcSendWaitReceivePort(PortHandle=0x70, SendFlags=0x00020000, SendMessage=0x248fdfddc0 [2
[LPC_REPLY] (560b)], InMessageBuffer=null, ReceiveBuffer=0x248fdfddc0,
ReceiveBufferSize=0x248fdfd0d0 [0x258], OutMessageBuffer=null, Timeout=null) => 0

NtQueryLicenseValue(Name="Kernel-OneCore-DeviceFamilyID", Type=0x248fdfcce8 [4],
Buffer=0x248fdfcce0, Length=4, ReturnedLength=0x248fdfcd30 [4]) => 0

NtAllocateVirtualMemory(ProcessHandle=0xe8, lpAddress=0x248fdfd488 [0x000001d5a8860000],
ZeroBits=0, pSize=0x248fdfd640 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtWriteVirtualMemory(ProcessHandle=0xe8, BaseAddress=0x1d5a8860000, Buffer=0x1eb8c77bd50,
BufferLength=0x11c0, ReturnedLength=null) => 0

NtWriteVirtualMemory(ProcessHandle=0xe8, BaseAddress=0x11a07ce2d8, Buffer=0x248fdfd488,
BufferLength=8, ReturnedLength=null) => 0

NtResumeThread(ThreadHandle=0xe4, SuspendCount=null) => 0

Process 116932 starting at 00007FF6D0DB13E0 with command line: "child.exe smth.txt"

D:\Users\lenovo\Desktop\try\OSmai\child.exe

NtClose(Handle=0xec) => 0

Loaded DLL at 00007FF81A370000 ntdll.dll

NtClose(Handle=0xf0) => 0

NtQueryPerformanceCounter(Counter=0x11a09ff8a0 [4.15881e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff8e8 [0x00007ff81a50e000],
Size=0x11a09ff8e0 [0x1000], NewProtect=4, OldProtect=0x11a09ff920 [8]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff8e8 [0x00007ff81a50e000],
Size=0x11a09ff8e0 [0x1000], NewProtect=8, OldProtect=0x11a09ff920 [4]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81a414140, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x11a09ff870, Length=0x18, ReturnLength=null) =>
0

NtCreateEvent(EventHandle=0x7ff81a4f6398 [0x14],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtManageHotPatch(Unknown=9, Unknown=0x11a09ff708 [1], Unknown=8, Unknown=0x11a09ff700) =>
0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']

NtSetEvent(EventHandle=0x14, PrevState=null) => 0
```

```
NtCreateEvent(EventHandle=0x7ff81a4f63e8 [0x18],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x11a09ff620, Length=0x40, ReturnLength=null) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x11a09ff318, Length=4, ReturnLength=null) => 0

NtOpenKey(KeyHandle=0x11a09ff1c8 [0x1c], DesiredAccess=GENERIC_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\CodePage") => 0

NtQueryValueKey(KeyHandle=0x1c, ValueName="ACP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff230, Length=0x24,
ResultLength=0x11a09ff1c0 [0x16]) => 0

NtQueryValueKey(KeyHandle=0x1c, ValueName="OEMCP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff230, Length=0x24,
ResultLength=0x11a09ff1c0 [0x14]) => 0

NtClose(Handle=0x1c) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x7ff81a4f37e0 [0x000001d5a8870000], SectionSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x7ff81a4f37e8 [0x000001d5a8890000], SectionSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x11a09ff2b8 [0x000001d5a88b0000], SectionSize=null) => 0

NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0x11a09ff270, Length=0x20, ReturnLength=null) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81a370000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x11a09ff200, Length=0x18, ReturnLength=null) =>
0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0x11a09ff240, Length=0x50,
ReturnLength=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff290 [0x00007ff81a50b000],
Size=0x11a09ff288 [0x4000], NewProtect=2, OldProtect=0x11a09ff280 [4]) => 0

NtOpenKey(KeyHandle=0x11a09fef40 [0x1c], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x1c, ValueName="RaiseExceptionOnPossibleDeadlock",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x11a09fef50,
Length=0x50, ResultLength=0x11a09fef48) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Ïрщы.']

NtClose(Handle=0x1c) => 0

NtOpenKey(KeyHandle=0x11a09fef20, DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager\Segment
Heap") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Ïрщы.']

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x7ff81a4f7268, Length=4, ReturnLength=null) => 0
```

```
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x11a09ff228, Length=4, ReturnLength=null) => 0

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x11a09febc0, Length=0x330, ReturnLength=0x11a09feb78) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x11a09febc0, Length=0x330, ReturnLength=0x11a09feb78) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtOpenKey(KeyHandle=0x11a09ff170 [0x1c], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0x1c, ValueName="ResourcePolicies", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff1b0, Length=0x18,
ResultLength=0x11a09ff178) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x1c) => 0

NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x11a09ff280, Length=4, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x11a09ff220, Length=0x40, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation],
SystemInformation=0x11a09ff250, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81a4f7a88 [0x00007ff578540000],
ZeroBits=0x00000011a09ff1d0, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x11a09ff118, DataCount=1) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81a4f7a80 [0x00007ff57a540000],
ZeroBits=0x00000011a09ff1d8, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null,
DataCount=0) => 0

NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ff81a4f7af0 [0x00007ff478520000],
ZeroBits=0x00000011a09ff180, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x11a09ff0c8, DataCount=1) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x11a09ff0c0, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09feca0 [0x000001d5a88c0000],
ZeroBits=0, pSize=0x11a09feca8 [0x00100000], flAllocationType=0x2000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fec88 [0x000001d5a88c0000],
ZeroBits=0, pSize=0x11a09fec80 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQuerySystemInformation(SystemInformationClass=0xc5
[SystemHypervisorSharedPageInformation], SystemInformation=0x11a09ff420, Length=8,
ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap],
SystemInformation=0x11a09fee90, Length=0x408, ReturnLength=0x11a09ff2b0 [0x18]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x11a09fee78 [4], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x11a09fee70) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']
```

```
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x11a09fee78 [4], Alignment=4,
SystemInformation=0x1d5a88c0880, Length=0x50, ReturnLength=0x11a09fee70 [0x50]) => 0

NtCreateEvent(EventHandle=0x11a09ff068 [0x1c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1d5a88c0c40 [0x20],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x11a09fede0 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x11a09fedd8) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x11a09fede0 [6], Alignment=4,
SystemInformation=0x1d5a88c0ff0, Length=0x30, ReturnLength=0x11a09fedd8 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x1d5a88c0d20 [0x24],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0

NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1d5a88c0d18 [0x28],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x24, WorkerProcessHandle=-1, StartRoutine=0x7ff81a3a5550,
StartParameter=0x1d5a88c0ce0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtCreateTimer2(TimerHandle=0x1d5a88c0d70 [0x2c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1d5a88c0d78 [0x30],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x30, IoCompletionHandle=0x24,
TargetObjectHandle=0x2c, KeyContext=0x1d5a88c0d80, ApcContext=0x1d5a88c0d50, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x11a09feda0 [0]) => 0

NtCreateTimer2(TimerHandle=0x1d5a88c0de8 [0x34], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x1d500000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1d5a88c0df0 [0x38],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x38, IoCompletionHandle=0x24,
TargetObjectHandle=0x34, KeyContext=0x1d5a88c0df8, ApcContext=0x1d5a88c0d50, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x11a09feda0 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x28, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x11a09fee88, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x28, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0x11a09fee88, BufferLength=4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x28, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x11a09fefa8, BufferLength=4) => 0
```

```
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x20, IoCompletionHandle=0x24,
TargetObjectHandle=0x1c, KeyContext=0x1d5a88c0c58, ApcContext=0x1d5a88c0ad0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x11a09feff0 [0xa88c0c00]) => 0

NtTraceControl(CtrlCode=0x1b, InputBuffer=0x11a09ff0a8, InputBufferLength=4,
OutputBuffer=null, OutputBufferLength=0, ReturnLength=0x11a09ff060 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09ff108, InputBufferLength=0xa0,
OutputBuffer=0x11a09ff108, OutputBufferLength=0xa0, ReturnLength=0x11a09ff100 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x11a09ff158, InputBufferLength=0x18,
OutputBuffer=0x11a09ff170, OutputBufferLength=0x78, ReturnLength=0x11a09ff150 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09ff158, InputBufferLength=0xa0,
OutputBuffer=0x11a09ff158, OutputBufferLength=0xa0, ReturnLength=0x11a09ff150 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09ff158, InputBufferLength=0xa0,
OutputBuffer=0x11a09ff158, OutputBufferLength=0xa0, ReturnLength=0x11a09ff150 [0xa0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09ff108, InputBufferLength=0xa0,
OutputBuffer=0x11a09ff108, OutputBufferLength=0xa0, ReturnLength=0x11a09ff100 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x11a09ff158, InputBufferLength=0x18,
OutputBuffer=0x11a09ff170, OutputBufferLength=0x78, ReturnLength=0x11a09ff150 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09ff158, InputBufferLength=0xa0,
OutputBuffer=0x11a09ff158, OutputBufferLength=0xa0, ReturnLength=0x11a09ff150 [0xa0]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fea90 [0x000001d5a88c2000],
ZeroBits=0, pSize=0x11a09feb38 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe6b0 [0x000001d5a88c4000],
ZeroBits=0, pSize=0x11a09fe758 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09ff2b0 [0x000001d5a8800000],
pSize=0x11a09ff2b8 [0x00020000], flFreeType=0x8000) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff290 [0x00007ff81a50b000],
Size=0x11a09ff288 [0x4000], NewProtect=4, OldProtect=0x11a09ff280 [2]) => 0

NtOpenDirectoryObject(DirectoryHandle=0x7ff81a50b2b0 [0x50], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff290 [0x00007ff81a50b000],
Size=0x11a09ff288 [0x4000], NewProtect=2, OldProtect=0x11a09ff280 [4]) => 0

NtOpenSymbolicLinkObject(LinkHandle=0x11a09ff408 [0x54], DesiredAccess=0x1,
ObjectAttributes=0x50:"KnownDllPath") => 0

NtQuerySymbolicLinkObject(LinkHandle=0x54, LinkTarget="C:\WINDOWS\System32",
ReturnedLength=0x11a09ff3a0 [0x28]) => 0

NtClose(Handle=0x54) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff260 [0x00007ff81a50b000],
Size=0x11a09ff258 [0x4000], NewProtect=4, OldProtect=0x11a09ff250 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff290 [0x00007ff81a50b000],
Size=0x11a09ff288 [0x4000], NewProtect=2, OldProtect=0x11a09ff280 [4]) => 0
```

```
NtCreateEvent(EventHandle=0x7ff81a4f62d8 [0x54],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateEvent(EventHandle=0x7ff81a4f6310 [0x58],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff1f0 [0x00007ff81a50b000],
Size=0x11a09ff1e8 [0x4000], NewProtect=4, OldProtect=0x11a09ff1e0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff1f0 [0x00007ff81a50b000],
Size=0x11a09ff1e8 [0x4000], NewProtect=2, OldProtect=0x11a09ff1e0 [4]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe690 [0x000001d5a88c5000],
ZeroBits=0, pSize=0x11a09fe738 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenFile(FileHandle=0x11a09ff298 [0x5c], DesiredAccess=SYNCHRONIZE|0x20,
ObjectAttributes="\??\D:\Users\lenovo\Desktop\try\OSmai\", IoStatusBlock=0x11a09ff208 [0/1],
ShareAccess=3, OpenOptions=0x21) => 0

NtQueryVolumeInformationFile(FileHandle=0x5c, IoStatusBlock=0x11a09ff208 [0/8],
FsInformation=0x11a09ff1f0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtSetEvent(EventHandle=0x54, PrevState=null) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x11a09fef60) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

NtOpenSection(SectionHandle=0x11a09feef8 [0x60], DesiredAccess=0xd,
ObjectAttributes=0x50:"KERNEL32.DLL") => 0

Loaded DLL at 00007FF818C40000 C:\WINDOWS\System32\KERNEL32.DLL

NtMapViewOfSection(SectionHandle=0x60, ProcessHandle=-1, BaseAddress=0x1d5a88c54d0
[0x00007ff818c40000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1d5a88c5428
[0x000c4000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x11a09fed50 [4.15881e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fece0 [0x00007ff818d01000],
Size=0x11a09fecd8 [0x1000], NewProtect=2, OldProtect=0x11a09fecd0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fed60 [0x00007ff81a50b000],
Size=0x11a09fed58 [0x4000], NewProtect=4, OldProtect=0x11a09fed50 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fed60 [0x00007ff81a50b000],
Size=0x11a09fed58 [0x4000], NewProtect=2, OldProtect=0x11a09fed50 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feda0 [0x00007ff818cc3000],
Size=0x11a09feda8 [0x4000], NewProtect=4, OldProtect=0x1d5a88c5410 [2]) => 0

NtOpenSection(SectionHandle=0x11a09fe798 [0x64], DesiredAccess=0xd,
ObjectAttributes=0x50:"KERNELBASE.dll") => 0

Loaded DLL at 00007FF817890000 C:\WINDOWS\System32\KERNELBASE.dll

NtMapViewOfSection(SectionHandle=0x64, ProcessHandle=-1, BaseAddress=0x1d5a88c5c10
[0x00007ff817890000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1d5a88c5b68
[0x003b7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
```

```
NtQueryPerformanceCounter(Counter=0x11a09fe5f0 [4.15881e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fe580 [0x00007ff817c15000],
Size=0x11a09fe578 [0x1000], NewProtect=2, OldProtect=0x11a09fe570 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fe600 [0x00007ff81a50b000],
Size=0x11a09fe5f8 [0x4000], NewProtect=4, OldProtect=0x11a09fe5f0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fe600 [0x00007ff81a50b000],
Size=0x11a09fe5f8 [0x4000], NewProtect=2, OldProtect=0x11a09fe5f0 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fe640 [0x00007ff817afe000],
Size=0x11a09fe648 [0x2000], NewProtect=4, OldProtect=0x1d5a88c5b50 [2]) => 0

NtClose(Handle=0x64) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1d5a88c53f0 [0x00007ff818cc3000],
Size=0x1d5a88c53f8 [0x4000], NewProtect=2, OldProtect=0x11a09feba0 [4]) => 0

NtClose(Handle=0x60) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1d5a88c5b30 [0x00007ff817afe000],
Size=0x1d5a88c5b38 [0x2000], NewProtect=2, OldProtect=0x11a09fece0 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x11a09fec40, Length=0x28) => 0

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

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

NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0x11a09fea20, Length=8, ReturnLength=null) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ff817bf6e80, Length=0x40, ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fdfa0 [0x000001d5a88c6000],
ZeroBits=0, pSize=0x11a09fe048 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenSection(SectionHandle=0x11a09fe7e0 [0x68], DesiredAccess=0x4,
ObjectAttributes="\Sessions\8\Windows\SharedSection") => 0

NtCreateSection(SectionHandle=0x11a09fe800 [0x64],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0x11a09fe7f0 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0

NtConnectPort(PortHandle=0x7ff81a4f6c08 [0x6c], PortName="\Sessions\8\Windows\ApiPort",
SecurityQos=0x11a09fe920, ClientView=0x11a09fe818, ServerView=0x11a09fe848,
MaxMsgLength=0x11a09fe810 [0x3b8], ConnectionInfo=0x11a09fe890,
ConnectionInfoLength=0x11a09fe7e8 [0x30]) => 0

NtClose(Handle=0x64) => 0

NtMapViewOfSection(SectionHandle=0x68, ProcessHandle=-1, BaseAddress=0x11a09fe7f8
[0x00007ff478420000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x11a09fe808
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0

NtClose(Handle=0x68) => 0
```

```
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x1d5a8800000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x11a09fe4e0, Length=0x30, ReturnLength=null) =>
0

NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x11a09fe9c8 [0x000001d5a8810000], SectionSize=null) => 0

NtInitializeNlsFiles(BaseAddress=0x11a09fe9c0 [0x000001d5a89c0000],
DefaultLocaleId=0x7ff817bf8b88 [0x419], DefaultCasingTableSize=null) => 0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x11a09fe9a0 [0x000001d5a8a90000], SectionSize=0x11a09fe968 [0x00011000]) =>
0

NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x11a09fe9a0 [0x000001d5a8ab0000], SectionSize=0x11a09fe968 [0x00011000]) =>
0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe110 [0x000001d5a88c7000],
ZeroBits=0, pSize=0x11a09fe1b8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtCreateFile(FileHandle=0x11a09fea28 [0x70], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f,
ObjectAttributes=4:"\Connect", IoStatusBlock=0x11a09fe3e0 [0/0x18], AllocationSize=null,
FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20,
EaBuffer=0x1d5a88c70a0, EaLength=0x54b) => 0

NtDeviceIoControlFile(FileHandle=0x70, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x11a09fe970 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0x11a09fe990, OutputBufferLength=8) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0x11a09fe998, Length=8) => 0

NtDeviceIoControlFile(FileHandle=0x70, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x11a09fe760, IoControlCode=0x00500016, InputBuffer=0x11a09fe770,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09fe878, InputBufferLength=0xa0,
OutputBuffer=0x11a09fe878, OutputBufferLength=0xa0, ReturnLength=0x11a09fe870 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x11a09fe8c8, InputBufferLength=0x18,
OutputBuffer=0x11a09fe8e0, OutputBufferLength=0x78, ReturnLength=0x11a09fe8c0 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09fead8, InputBufferLength=0xa0,
OutputBuffer=0x11a09fead8, OutputBufferLength=0xa0, ReturnLength=0x11a09fead0 [0xa0]) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x11a09fe880 [0x78]) =>
0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0xc [TokenSessionId],
TokenInformation=0x11a09fe1a0, Length=4, ReturnLength=0x11a09fe180 [4]) => 0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0x11a09fe1e8, Length=4, ReturnLength=0x11a09fe180 [4]) => 0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x2a
[TokenPrivateNameSpace], TokenInformation=0x11a09fe184, Length=4, ReturnLength=0x11a09fe180
[4]) => 0
```

```
NtOpenDirectoryObject(DirectoryHandle=0x11a09fe1a8 [0x64], DesiredAccess=0xf,
ObjectAttributes="\Sessions\8\BaseNamedObjects") => 0

NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x2c [TokenBnoIsolation],
TokenInformation=0x11a09fe4a0, Length=0x120, ReturnLength=0x11a09fe180 [0x10]) => 0

NtClose(Handle=0x78) => 0

NtCreateMutant(MutantHandle=0x11a09fe8d8 [0x7c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x64:"Local\SM0:116932:304:WilStaging_02", InitialOwner=false) => 0

NtWaitForSingleObject(Handle=0x7c, Alertable=false, Timeout=null) => 0

NtOpenSemaphore(SemaphoreHandle=0x11a09fe698,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x64:"Local\SM0:116932:304:WilStaging_02_p0") => 0xc0000034 [2 '=x
єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtCreateSemaphore(SemaphoreHandle=0x11a09fe5f8 [0x80],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x64:"Local\SM0:116932:304:WilStaging_02_p0", InitialCount=0x6a231cc0,
MaxCount=0x6a231cc0) => 0

NtCreateSemaphore(SemaphoreHandle=0x11a09fe5f8 [0x78],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x64:"Local\SM0:116932:304:WilStaging_02_p0h", InitialCount=0xea,
MaxCount=0xea) => 0

NtReleaseMutant(MutantHandle=0x7c, PreviousCount=null) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09feab8, InputBufferLength=0xa0,
OutputBuffer=0x11a09feab8, OutputBufferLength=0xa0, ReturnLength=0x11a09feab0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x11a09feb08, InputBufferLength=0x18,
OutputBuffer=0x11a09feb20, OutputBufferLength=0x78, ReturnLength=0x11a09feb00 [0]) => 0

NtQueryWnfStateData(StateName=0x11a09fe9a0 [0xa3bc0875], TypeId=0x11a09fea48,
ExplicitScope=null, ChangeStamp=0x11a09fe994 [0xe], Buffer=0x11a09fd990,
BufferSize=0x11a09fe990 [8]) => 0

NtCreateEvent(EventHandle=0x11a09fe910 [0x84],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1d5a88c7ad0 [0x88],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtSetWnfProcessNotificationEvent(NotificationEvent=0x84) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x88, IoCompletionHandle=0x24,
TargetObjectHandle=0x84, KeyContext=0x1d5a88c7ae8, ApcContext=0x1d5a88c7960, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x11a09fe890 [0xa88c0c00]) => 0

NtSubscribeWnfStateChange(StateName=0x1d5a88c7c60 [0xa3bc0875], ChangeStamp=0xe,
EventMask=0x11, SubscriptionId=0x11a09fe980 [0x0001998f]) => 0

NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0x11a09fe800 [0], Alignment=0x18,
SystemInformation=0x11a09fe820, Length=0x50, ReturnLength=null) => 0
```

```
NtMapViewOfSection(SectionHandle=0x8c, ProcessHandle=-1, BaseAddress=0x11a09fe790
[0x000001d5a8ad0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x11a09fe7a0
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x90, ProcessHandle=-1, BaseAddress=0x11a09fe790
[0x000001d5a8ae0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x11a09fe7a0
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtMapViewOfSection(SectionHandle=0x94, ProcessHandle=-1, BaseAddress=0x11a09fe790
[0x000001d5a8af0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x11a09fe7a0
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0

NtClose(Handle=0x8c) => 0

NtClose(Handle=0x90) => 0

NtClose(Handle=0x94) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fd450 [0x000001d5a88c8000],
ZeroBits=0, pSize=0x11a09fd4f8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtSetTimer2(TimerHandle=0x34, DueTime=0x11a09fe910 [-3e+09], Period=null,
Parameters=0x11a09fe918) => 0

NtOpenKey(KeyHandle=0x11a09feab0, DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\StateSeparation\Redirec
tionMap\Keys") => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09feab8, InputBufferLength=0xa0,
OutputBuffer=0x11a09feab8, OutputBufferLength=0xa0, ReturnLength=0x11a09feab0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x11a09feb08, InputBufferLength=0x18,
OutputBuffer=0x11a09feb20, OutputBufferLength=0x78, ReturnLength=0x11a09feb00 [0]) => 0

NtTraceControl(CtrlCode=0xf, InputBuffer=0x11a09feae8, InputBufferLength=0xa0,
OutputBuffer=0x11a09feae8, OutputBufferLength=0xa0, ReturnLength=0x11a09feae0 [0xa0]) => 0

NtTraceControl(CtrlCode=0x1e, InputBuffer=0x11a09feb38, InputBufferLength=0x18,
OutputBuffer=0x11a09feb50, OutputBufferLength=0x78, ReturnLength=0x11a09feb30 [0]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fea00 [0x00007ff81a50b000],
Size=0x11a09fe9f8 [0x4000], NewProtect=4, OldProtect=0x11a09fe9f0 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fea00 [0x00007ff81a50b000],
Size=0x11a09fe9f8 [0x4000], NewProtect=2, OldProtect=0x11a09fe9f0 [4]) => 0

NtOpenKey(KeyHandle=0x11a09fea88 [0x8c], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0

NtQueryValueKey(KeyHandle=0x8c, ValueName="TSAppCompat", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x1d5a88c8810, Length=0x224,
ResultLength=0x11a09fea78) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0x8c, ValueName="TSUserEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x1d5a88c8810, Length=0x224,
ResultLength=0x11a09fea78 [0x10]) => 0

NtClose(Handle=0x8c) => 0

NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ff818cf9a80, Length=0x40, ReturnLength=null) => 0
```

```
NtSetEvent(EventHandle=0x54, PrevState=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=4, OldProtect=0x11a09feb98 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09feb88 [0x00007ff817c15000],
Size=0x11a09feb80 [0x1000], NewProtect=2, OldProtect=0x11a09feb98 [4]) => 0

NtOpenKey(KeyHandle=0x11a09ff150, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x11a09ff130 [0x98], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0

NtQueryKey(KeyHandle=0x98, KeyInformationClass=2 [KeyFullInformation],
KeyInformation=0x11a09ff1a8, Length=0x30, ResultLength=0x11a09ff120 [0x2c]) => 0

NtClose(Handle=0x98) => 0

NtOpenKey(KeyHandle=0x11a09ff128 [0x8c], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0

NtQueryValueKey(KeyHandle=0x8c, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff1e0, Length=0x50,
ResultLength=0x11a09ff120) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0x8c) => 0

NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x11a09ff050, Length=0x58, ReturnLength=0x11a09ff048 [0x2c]) => 0

NtOpenKey(KeyHandle=0x11a09ff128, DesiredAccess=0x1, ObjectAttributes="\REGISTRY\USER\S-1-5-
21-3512441621-816733789-498939024-
1001\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers") => 0xc0000034 [2 '=x
єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtOpenKey(KeyHandle=0x11a09ff200 [0x8c], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0

NtQueryValueKey(KeyHandle=0x8c, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff240, Length=0x14,
ResultLength=0x11a09ff208 [0x10]) => 0

NtClose(Handle=0x8c) => 0

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x11a09ff190 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x11a09ff188) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']

NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x11a09ff190 [6], Alignment=4,
SystemInformation=0x1d5a88c5b80, Length=0x30, ReturnLength=0x11a09ff188 [0x30]) => 0

NtCreateIoCompletion(IoHandle=0x1d5a88c5750 [0x98],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0
```

```
NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1d5a88c5748 [0x9c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x98, WorkerProcessHandle=-1, StartRoutine=0x7ff81a3a5550,
StartParameter=0x1d5a88c5710, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0x11a09ff238, BufferLength=4) => 0

NtCreateTimer2(TimerHandle=0x1d5a88c57a0 [0x8c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1d5a88c57a8 [0xa0],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xa0, IoCompletionHandle=0x98,
TargetObjectHandle=0x8c, KeyContext=0x1d5a88c57b0, ApcContext=0x1d5a88c5780, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x11a09ff150 [0]) => 0

NtCreateTimer2(TimerHandle=0x1d5a88c5818 [0xa4], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x1d500000002) => 0

NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1d5a88c5820 [0xa8],
DesiredAccess=0x1, ObjectAttributes=null) => 0

NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xa8, IoCompletionHandle=0x98,
TargetObjectHandle=0xa4, KeyContext=0x1d5a88c5828, ApcContext=0x1d5a88c5780, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x11a09ff150 [0]) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=2
[WorkerFactoryIdleTimeout], Buffer=0x11a09ff238, BufferLength=8) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x11a09ff238, BufferLength=4) => 0

NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x11a09ff2b0) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff230 [0x00007ff6d0dbf000],
Size=0x11a09ff238 [0x1000], NewProtect=4, OldProtect=0x11a09ff580 [8]) => 0

NtOpenSection(SectionHandle=0x11a09fec28 [0xac], DesiredAccess=0xd,
ObjectAttributes=0x50:"msvcrt.dll") => 0

Loaded DLL at 00007FF8190A0000 C:\WINDOWS\System32\msvcrt.dll

NtMapViewOfSection(SectionHandle=0xac, ProcessHandle=-1, BaseAddress=0x1d5a88c8840
[0x00007ff8190a0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1d5a88c59c8
[0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0

NtQueryPerformanceCounter(Counter=0x11a09fea80 [4.15881e+12], Freq=null) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fea90 [0x00007ff81a50b000],
Size=0x11a09fea88 [0x4000], NewProtect=4, OldProtect=0x11a09fea80 [2]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fea90 [0x00007ff81a50b000],
Size=0x11a09fea88 [0x4000], NewProtect=2, OldProtect=0x11a09fea80 [4]) => 0
```

```
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x11a09fe540, Length=0x330, ReturnLength=0x11a09fe4f8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x11a09fe540, Length=0x330, ReturnLength=0x11a09fe4f8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff8190a0000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x11a09fe7b8, Length=0x30, ReturnLength=null)
=> 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09fead0 [0x00007ff81911e000],
Size=0x11a09fead8 [0x1000], NewProtect=4, OldProtect=0x1d5a88c59b0 [2]) => 0

NtClose(Handle=0xac) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x11a09ff560 [0x00007ff6d0dbf000],
Size=0x11a09ff568 [0x1000], NewProtect=8, OldProtect=0x11a09ff030 [4]) => 0

NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1d5a88c5990 [0x00007ff81911e000],
Size=0x1d5a88c5998 [0x1000], NewProtect=2, OldProtect=0x11a09ff030 [4]) => 0

NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x11a09fef90, Length=0x28) => 0

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

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

NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11
[ThreadHideFromDebugger], ThreadInformation=0x11a09ff2b0, Length=1, ReturnLength=null) => 0

Initial breakpoint

NtSetEvent(EventHandle=0x54, PrevState=null) => 0

NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x11a09ff220 [0xac]) =>
0

NtQueryInformationToken(TokenHandle=0xac, TokenInformationClass=0xa [TokenStatistics],
TokenInformation=0x11a09ff230, Length=0x38, ReturnLength=0x11a09ff228 [0x38]) => 0

NtClose(Handle=0xac) => 0

NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode",
Type=0x11a09fee2c [4], Buffer=0x11a09fee20, Length=4, ReturnedLength=0x11a09fee24 [4]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe9c0 [0x000001d5a8b00000],
ZeroBits=0, pSize=0x11a09fe9c8 [0x00040000], flAllocationType=0x2000, flProtect=4) => 0

NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe9c0 [0x000001d5a8b00000],
pSize=0x11a09fe9b8 [0x00030000], flFreeType=0x8000) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe9a8 [0x000001d5a8b30000],
ZeroBits=0, pSize=0x11a09fe9a0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVolumeInformationFile(FileHandle=8, IoStatusBlock=0x11a09fef70 [0/8],
FsInformation=0x11a09fef90, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtQueryVolumeInformationFile(FileHandle=0xc, IoStatusBlock=0x11a09fef70 [0/8],
FsInformation=0x11a09fef90, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
```

```
NtQueryVolumeInformationFile(FileHandle=0x10, IoStatusBlock=0x11a09fef70 [0/8],
FsInformation=0x11a09fef90, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe7d0 [0x000001d5a88c9000],
ZeroBits=0, pSize=0x11a09fe878 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe780 [0x000001d5a8b32000],
ZeroBits=0, pSize=0x11a09fe828 [0x1000], flAllocationType=0x1000, flProtect=4) => 0

NtOpenKey(KeyHandle=0x11a09fdcb0 [0xb0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions")
=> 0

NtQueryValueKey(KeyHandle=0xb0, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x11a09fe180, Length=0x214,
ResultLength=0x11a09fe138 [0x2a]) => 0

NtQueryValueKey(KeyHandle=0xb0, ValueName="000604xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x11a09fe160, Length=0x214,
ResultLength=0x11a09fdf18 [0x42]) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe780 [0x000001d5a8b33000],
ZeroBits=0, pSize=0x11a09fe828 [0x2000], flAllocationType=0x1000, flProtect=4) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff81912ed28, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x11a09feda0, Length=0x18, ReturnLength=null) =>
0

NtSetEvent(EventHandle=0x54, PrevState=null) => 0

NtOpenKey(KeyHandle=0x11a09ff2b0 [0xb4], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelaySleepLoopWindowSize",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x11a09ff210,
Length=0x50, ResultLength=0x11a09ff200) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelaySpinCountThreshold",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x11a09ff210,
Length=0x50, ResultLength=0x11a09ff200) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelayBaseYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff210, Length=0x50,
ResultLength=0x11a09ff200) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtFactorYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff210, Length=0x50,
ResultLength=0x11a09ff200) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtQueryValueKey(KeyHandle=0xb4, ValueName="SmtDelayMaxYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x11a09ff210, Length=0x50,
ResultLength=0x11a09ff200) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']

NtClose(Handle=0xb4) => 0

NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x11a09ff588, BufferLength=4) => 0

NtSetEvent(EventHandle=0x18, PrevState=null) => 0

NtTestAlert() => 0
```

```
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6d0db2740, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x11a09ffad0, Length=0x30,
ReturnLength=0x11a09ffa80 [0x30]) => 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6d0db2740, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x11a09ffb00, Length=0x30, ReturnLength=null)
=> 0

NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6d0db2740, MemoryInformationClass=2
[MemoryMappedFilenameInformation], MemoryInformation=0x11a09ffb78, Length=0x21a,
ReturnLength=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe0b0 [0x000001d5a8b35000],
ZeroBits=0, pSize=0x11a09fe158 [0x3000], flAllocationType=0x1000, flProtect=4) => 0

NtFsControlFile(FileHandle=0xb8, Event=0, UserApcRoutine=null, UserApcContext=null,
UserIoStatus=0x248fdfecc0 [0/0], FsControlCode=0x00110008, InputBuffer=null,
InputBufferLength=0, OutputBuffer=null, OutputBufferLength=0) => 0

NtCreateFile(FileHandle=0x11a09fe750 [0xb4], DesiredAccess=SYNCHRONIZE|GENERIC_READ|0x80,
ObjectAttributes="\??\pipe\Pipe1", IoStatusBlock=0x11a09fe758 [0/1], AllocationSize=null,
FileAttributes=0, ShareAccess=0, CreateDisposition=1, CreateOptions=0x00020060,
EaBuffer=null, EaLength=0) => 0

NtFsControlFile(FileHandle=0xb4, Event=0, UserApcRoutine=null, UserApcContext=null,
UserIoStatus=0x248fdfecc0 [0/0], FsControlCode=0x00110008, InputBuffer=null,
InputBufferLength=0, OutputBuffer=null, OutputBufferLength=0) => 0

NtCreateFile(FileHandle=0x11a09fe750 [0xb8], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80,
ObjectAttributes="\??\pipe\Pipe2", IoStatusBlock=0x11a09fe758 [0/1], AllocationSize=null,
FileAttributes=0, ShareAccess=0, CreateDisposition=1, CreateOptions=0x00020060,
EaBuffer=null, EaLength=0) => 0

Enter command: NtWriteFile(FileHandle=0xbe0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfecc0 [0/0xf], Buffer=0x7ff62ec2a054, Length=0xf, ByteOffset=null,
Key=null) => 0

NtCreateFile(FileHandle=0x11a09fe750 [0xbc], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80,
ObjectAttributes=0x5c:"smth.txt", IoStatusBlock=0x11a09fe758 [0/2], AllocationSize=null,
FileAttributes=0x80, ShareAccess=0, CreateDisposition=5, CreateOptions=0x00020060,
EaBuffer=null, EaLength=0) => 0

NtReadFile(FileHandle=0x64, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfecc0 [0/0xc], Buffer=0x248fdff5c0, Length=0x400, ByteOffset=null,
Key=null) => 0

NtWriteFile(FileHandle=0xb8, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfecc0 [0/0xc], Buffer=0x248fdff5c0, Length=0xc, ByteOffset=null,
Key=null) => 0

NtReadFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x11a09fe8b0 [0/0xc], Buffer=0x11a09ff920, Length=0x400, ByteOffset=null,
Key=null) => 0

NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x11a09fe0b0 [0x000001d5a8b38000],
ZeroBits=0, pSize=0x11a09fe158 [0x3000], flAllocationType=0x1000, flProtect=4) => 0

NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x11a09fe410 [0/2], Buffer=0x11a09fe480, Length=2, ByteOffset=null, Key=null)
=> 0
```

```
NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x11a09fe410 [0/2], Buffer=0x11a09fe480, Length=2, ByteOffset=null, Key=null)
=> 0

NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x11a09fe410 [0/2], Buffer=0x11a09fe480, Length=2, ByteOffset=null, Key=null)
=> 0

NtWriteFile(FileHandle=0xbc, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x11a09fe410 [0/2], Buffer=0x11a09fe480, Length=2, ByteOffset=null, Key=null)
=> 0

NtClose(Handle=0xb4) => 0

NtClose(Handle=0xb8) => 0

NtReadFile(FileHandle=0xb4, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x248fdfecc0, Buffer=0x248fdfed30, Length=0x400, ByteOffset=null, Key=null) =>
0xc000014b [109 '╨рэры c√ы чръЁ√Є.']

NtClose(Handle=0xb8) => 0

NtClose(Handle=0xbc) => 0

NtClose(Handle=0xb4) => 0

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

NtClose(Handle=0xe8) => 0

NtClose(Handle=0x74) => 0

NtClose(Handle=0xe4) => 0

NtClose(Handle=0x94) => 0

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

NtClose(Handle=0x90) => 0

NtClose(Handle=0xe0) => 0

NtQueryWnfStateData(StateName=0x11a09ff860 [0xa3bc1c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0x11a09fe7ac [0x0001b1cd], Buffer=0x11a09fe800, BufferSize=0x11a09fe7a8 [0x66c])
=> 0

NtClose(Handle=0xd8) => 0

NtClose(Handle=0x60) => 0

NtClose(Handle=0xdc) => 0

NtClose(Handle=0x68) => 0

NtClose(Handle=0xc4) => 0

NtClose(Handle=0xc0) => 0

Process 116932 exit code: 0

NtClose(Handle=0x58) => 0

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

NtQueryWnfStateData(StateName=0x248fdff8b0 [0xa3bc1c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0x248fdfe7fc [0x0001b1cd], Buffer=0x248fdfe850, BufferSize=0x248fdfe7f8 [0x66c])
=> 0

NtClose(Handle=0x84) => 0

NtClose(Handle=0x60) => 0

Process 118680 exit code: 0
```

Вывод

Задание интересное, возникло много вопросов при выполнении, потому что выполнял на ОС Windows без WSL и тд. <windows.h>, конечно, вещь хорошая, но то, что занимает у нормальных людей одну строчку, у меня заняло десяток. К тому же столкнулся с некоторыми особенностями, которые у меня заняли много времени. Например, я не знал, что на винде в конце помимо \n еще и \r внезапно появляется. Хотелось бы, чтобы на курсе были хотя бы полезные ссылки для работы с winapi, а то пришлось немало времени потратить на поиски). Очевидно, большая часть людей предпочла пойти по пути наименьшего сопротивления, но хотя бы для общего развития было бы хорошо.