Московский Авиационный Институт

(Национальный Исследовательский Университет)

Институт №8 “Компьютерные науки и прикладная математика”

Кафедра №806 “Вычислительная математика и программирование”

Лабораторная работа №3 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 file mapping, который связан с стандартным входным потоком дочернего процесса. 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:

- CreateFileMapping; – создает file mapping.
- WriteFile; – записывает данные в канал.
- ReadFile; – читает данные из канала.
- CloseHandle; – закрывает хендлеры, в том числе и каналы.
- MapViewOfFile; – позволяет посмотреть данные в file mapping.
- 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() {
    char fileName[BUFFER_SIZE];
    char buffer[BUFFER_SIZE];
    DWORD bytesWritten;

    HANDLE hMapFile = CreateFileMapping(INVALID_HANDLE_VALUE, NULL,
PAGE_READWRITE, 0, BUFFER_SIZE, "SharedMemory");
    if (hMapFile == NULL) {
        demidov_printf("Failed to create file mapping\n");
        return ERROR_CREATE_FILE_MAPPING;
    }

    HANDLE hSemParent = CreateSemaphore(NULL, 1, 1, "SemaphoreParent");
    HANDLE hSemChild = CreateSemaphore(NULL, 0, 1, "SemaphoreChild");
    if (hSemParent == NULL || hSemChild == NULL) {
        CloseHandle(hMapFile);
        demidov_printf("Failed to create semaphore\n");
        return ERROR_CREATE_SEMAPHORE;
    }

    char* pBuf = (char*) MapViewOfFile(hMapFile, FILE_MAP_ALL_ACCESS, 0, 0, BUFFER_SIZE);
    if (pBuf == NULL) {
        CloseHandle(hMapFile);
        CloseHandle(hSemParent);
        CloseHandle(hSemChild);
        demidov_printf("Failed to map view of file\n");
        return ERROR_MAP_VIEW_OF_FILE;
    }

    WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), "Enter file name: ", strlen("Enter file name: "), &bytesWritten, NULL);
    ReadFile(GetStdHandle(STD_INPUT_HANDLE), fileName, BUFFER_SIZE, &bytesWritten, NULL);
    fileName[bytesWritten - 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)) {
        UnmapViewOfFile(pBuf);
        CloseHandle(hMapFile);
        CloseHandle(hSemParent);
        CloseHandle(hSemChild);
        demidov_printf("Failed to create process\n");
        return ERROR_CREATE_CHILD_PROCESS;
    }

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

    WaitForSingleObject(hSemParent, INFINITE);
    strcpy(pBuf, buffer);
    ReleaseSemaphore(hSemChild, 1, NULL);

    WaitForSingleObject(hSemParent, INFINITE);
    if (strcmp(pBuf, "DIVIDE_BY_ZERO") == 0) {
        WriteFile(GetStdHandle(STD_OUTPUT_HANDLE), "Division by zero detected. Exiting...\n", strlen("Division by zero detected. Exiting...\n"), &bytesWritten, NULL);
    }

    UnmapViewOfFile(pBuf);
    CloseHandle(hMapFile);
    CloseHandle(hSemParent);
    CloseHandle(hSemChild);
    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[]) {
    if (argc < 2) {
        demidov_printf("Wrong args count");
        return ERROR_ARGS_COUNT;
    }

    char* fileName = argv[1];
    HANDLE hFile;

    HANDLE hMapFile = OpenFileMapping(FILE_MAP_ALL_ACCESS, FALSE, "SharedMemory");
    HANDLE hSemParent = OpenSemaphore(SEMAPHORE_ALL_ACCESS, FALSE,
"SemaphoreParent");
    HANDLE hSemChild = OpenSemaphore(SEMAPHORE_ALL_ACCESS, FALSE,
"SemaphoreChild");
    if (hMapFile == NULL || hSemParent == NULL || hSemChild == NULL) {
        demidov_printf("Failed to open shared memory or semaphore\n");
        return ERROR_OPEN_FILE_MAPPING;
    }

    char* pBuf = (char*) MapViewOfFile(hMapFile, FILE_MAP_ALL_ACCESS, 0, 0, BUFFER_SIZE);
    if (pBuf == NULL) {
        CloseHandle(hMapFile);
        CloseHandle(hSemParent);
        CloseHandle(hSemChild);
        demidov_printf("Failed to map view of file\n");
        return ERROR_MAP_VIEW_OF_FILE;
    }

    WaitForSingleObject(hSemChild, INFINITE);
    char buffer[BUFFER_SIZE];
    strcpy(buffer, pBuf);

    hFile = CreateFile(fileName, GENERIC_WRITE, 0, NULL, CREATE_ALWAYS,
FILE_ATTRIBUTE_NORMAL, NULL);
    if (hFile == INVALID_HANDLE_VALUE) {
        UnmapViewOfFile(pBuf);
        CloseHandle(hMapFile);
        CloseHandle(hSemParent);
        CloseHandle(hSemChild);
        demidov_printf("Failed to open file");
        return ERROR_OPEN_FILE;
    }

    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 writeBuffer[BUFFER_SIZE];

    for (int i = 1; i < count; i++) {
        if (numbers[i] == 0) {
            strcpy(pBuf, "DIVIDE_BY_ZERO");
            ReleaseSemaphore(hSemParent, 1, NULL);
            UnmapViewOfFile(pBuf);
            CloseHandle(hMapFile);
            CloseHandle(hSemParent);
            CloseHandle(hSemChild);
            CloseHandle(hFile);
            return ERROR_DEV_ZERO;
        }
        snprintf(writeBuffer, BUFFER_SIZE, "%d ", result / numbers[i]);
        DWORD bytesWritten;
        WriteFile(hFile, writeBuffer, strlen(writeBuffer), &bytesWritten, NULL);
    }

    strcpy(pBuf, "COMPLETED");
    ReleaseSemaphore(hSemParent, 1, NULL);

    UnmapViewOfFile(pBuf);
    CloseHandle(hMapFile);
    CloseHandle(hSemParent);
    CloseHandle(hSemChild);
    CloseHandle(hFile);

    return SUCCESS;
}
```

Протокол работы программы

```
Process 67588 starting at 00007FF6F62313E0 with command line: ".\parent.exe"
D:\Users\lenovo\Desktop\osi\OSmai\Lab3\parent.exe
Loaded DLL at 00007FFBBB230000 ntdll.dll
NtQueryPerformanceCounter(Counter=0x5c5b7ff290 [2.5757e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7ff2d8 [0x00007ffbbb3ce000],
Size=0x5c5b7ff2d0 [0x1000], NewProtect=4, OldProtect=0x5c5b7ff310 [8]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7ff2d8 [0x00007ffbbb3ce000],
Size=0x5c5b7ff2d0 [0x1000], NewProtect=8, OldProtect=0x5c5b7ff310 [4]) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbbb2d4240, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x5c5b7ff260, Length=0x18, ReturnLength=null) =>
0
NtCreateEvent(EventHandle=0x7ffbbb3b6398 [8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0
NtManageHotPatch(Unknown=9, Unknown=0x5c5b7ff0f8 [1], Unknown=8, Unknown=0x5c5b7ff0f0) =>
0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']
NtSetEvent(EventHandle=8, PrevState=null) => 0
NtCreateEvent(EventHandle=0x7ffbbb3b63e8 [0xc],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x5c5b7ff010, Length=0x40, ReturnLength=null) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x5c5b7fed08, Length=4, ReturnLength=null) => 0
NtOpenKey(KeyHandle=0x5c5b7febb8 [0x10], DesiredAccess=GENERIC_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\CodePage") => 0
NtQueryValueKey(KeyHandle=0x10, ValueName="ACP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec20, Length=0x24,
ResultLength=0x5c5b7febb0 [0x16]) => 0
NtQueryValueKey(KeyHandle=0x10, ValueName="OEMCP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec20, Length=0x24,
ResultLength=0x5c5b7febb0 [0x14]) => 0
NtClose(Handle=0x10) => 0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x7ffbbb3b37e0 [0x000001714dc60000], SectionSize=null) => 0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x7ffbbb3b37e8 [0x000001714dc80000], SectionSize=null) => 0
NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x5c5b7feca8 [0x000001714dca0000], SectionSize=null) => 0
NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0x5c5b7fec60, Length=0x20, ReturnLength=null) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbbb230000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x5c5b7febf0, Length=0x18, ReturnLength=null) =>
0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0x5c5b7fec30, Length=0x50,
ReturnLength=null) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fec80 [0x00007ffbbb3cb000],
Size=0x5c5b7fec78 [0x4000], NewProtect=2, OldProtect=0x5c5b7fec70 [4]) => 0
NtOpenKey(KeyHandle=0x5c5b7fe930 [0x14], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0
NtQueryValueKey(KeyHandle=0x14, ValueName="RaiseExceptionOnPossibleDeadlock",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5c5b7fe940,
Length=0x50, ResultLength=0x5c5b7fe938) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x14) => 0
NtOpenKey(KeyHandle=0x5c5b7fe8c8 [0x18], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File
Execution Options") => 0
NtOpenKey(KeyHandle=0x5c5b7fe9b0, DesiredAccess=0x9, ObjectAttributes=0x18:"parent.exe") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5c5b7fe910, 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=0x7ffbbb3b7268, Length=4, ReturnLength=null) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x5c5b7fec18, Length=4, ReturnLength=null) => 0
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x5c5b7fe5b0, Length=0x330, ReturnLength=0x5c5b7fe568) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x5c5b7fe5b0, Length=0x330, ReturnLength=0x5c5b7fe568) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
NtOpenKey(KeyHandle=0x5c5b7feb60 [0x1c], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0
NtQueryValueKey(KeyHandle=0x1c, ValueName="ResourcePolicies", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7feba0, Length=0x18,
ResultLength=0x5c5b7feb68) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x1c) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x5c5b7fec70, Length=4, ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x5c5b7fec10, Length=0x40, ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation],
SystemInformation=0x5c5b7fec40, Length=0x40, ReturnLength=null) => 0
NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffbbb3b7a88 [0x00007ff52d620000],
ZeroBits=0x0000005c5b7febc0, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x5c5b7feb08, DataCount=1) => 0
NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffbbb3b7a80 [0x00007ff52f620000],
ZeroBits=0x0000005c5b7febc8, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null,
DataCount=0) => 0
NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffbbb3b7af0 [0x00007ff42d600000],
ZeroBits=0x0000005c5b7feb70, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x5c5b7feab8, DataCount=1) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x5c5b7feab0, Length=0x40, ReturnLength=null) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe690 [0x000001714dcb0000],
ZeroBits=0, pSize=0x5c5b7fe698 [0x001f0000], flAllocationType=0x2000, flProtect=4) => 0
NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe690 [0x000001714dcb0000],
pSize=0x5c5b7fe688 [0x000f0000], flFreeType=0x8000) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe678 [0x000001714dda0000],
ZeroBits=0, pSize=0x5c5b7fe670 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtQuerySystemInformation(SystemInformationClass=0xc5
[SystemHypervisorSharedPageInformation], SystemInformation=0x5c5b7fee10, Length=8,
ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap],
SystemInformation=0x5c5b7fe880, Length=0x408, ReturnLength=0x5c5b7feca0 [0x18]) => 0
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5c5b7fe868 [4], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x5c5b7fe860) => 0xc0000004 [24 '¬ышэр
т√фрээющ яЁюуЁрьью ъюьрэф√ ёыш°ъюь тхышър.']
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5c5b7fe868 [4], Alignment=4,
SystemInformation=0x1714dda0880, Length=0x50, ReturnLength=0x5c5b7fe860 [0x50]) => 0
NtCreateEvent(EventHandle=0x5c5b7fea58 [0x20],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
```

```
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1714dda0c40 [0x24],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5c5b7fe7d0 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x5c5b7fe7c8) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5c5b7fe7d0 [6], Alignment=4,
SystemInformation=0x1714dda0ff0, Length=0x30, ReturnLength=0x5c5b7fe7c8 [0x30]) => 0
NtCreateIoCompletion(IoHandle=0x1714dda0d20 [0x28],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0
NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1714dda0d18 [0x14],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x28, WorkerProcessHandle=-1, StartRoutine=0x7ffbbb265580,
StartParameter=0x1714dda0ce0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0
NtCreateTimer2(TimerHandle=0x1714dda0d70 [0x10], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1714dda0d78 [0x1c],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x1c, IoCompletionHandle=0x28,
TargetObjectHandle=0x10, KeyContext=0x1714dda0d80, ApcContext=0x1714dda0d50, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x5c5b7fe790 [0]) => 0
NtCreateTimer2(TimerHandle=0x1714dda0de8 [0x2c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x17100000002) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1714dda0df0 [0x30],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x30, IoCompletionHandle=0x28,
TargetObjectHandle=0x2c, KeyContext=0x1714dda0df8, ApcContext=0x1714dda0d50, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5c5b7fe790 [0]) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x14, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x5c5b7fe878, BufferLength=4) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x14, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0x5c5b7fe878, BufferLength=4) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x14, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x5c5b7fe998, BufferLength=4) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x24, IoCompletionHandle=0x28,
TargetObjectHandle=0x20, KeyContext=0x1714dda0c58, ApcContext=0x1714dda0ad0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5c5b7fe9e0 [0x4dda0c00]) => 0
NtTraceControl(CtrlCode=0x1b, InputBuffer=0x5c5b7fea98, InputBufferLength=4,
OutputBuffer=null, OutputBufferLength=0, ReturnLength=0x5c5b7fea50 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7feaf8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7feaf8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7feaf0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7feb48, InputBufferLength=0x18,
OutputBuffer=0x5c5b7feb60, OutputBufferLength=0x78, ReturnLength=0x5c5b7feb40 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7feb48, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7feb48, OutputBufferLength=0xa0, ReturnLength=0x5c5b7feb40 [0xa0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7feb48, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7feb48, OutputBufferLength=0xa0, ReturnLength=0x5c5b7feb40 [0xa0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7feaf8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7feaf8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7feaf0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7feb48, InputBufferLength=0x18,
OutputBuffer=0x5c5b7feb60, OutputBufferLength=0x78, ReturnLength=0x5c5b7feb40 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7feb48, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7feb48, OutputBufferLength=0xa0, ReturnLength=0x5c5b7feb40 [0xa0]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe480 [0x000001714dda2000],
ZeroBits=0, pSize=0x5c5b7fe528 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe0a0 [0x000001714dda4000],
ZeroBits=0, pSize=0x5c5b7fe148 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7feca0 [0x000001714dbf0000],
pSize=0x5c5b7feca8 [0x00020000], flFreeType=0x8000) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fec80 [0x00007ffbbb3cb000],
Size=0x5c5b7fec78 [0x4000], NewProtect=4, OldProtect=0x5c5b7fec70 [2]) => 0
NtOpenDirectoryObject(DirectoryHandle=0x7ffbbb3cb2b0 [0x48], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fec80 [0x00007ffbbb3cb000],
Size=0x5c5b7fec78 [0x4000], NewProtect=2, OldProtect=0x5c5b7fec70 [4]) => 0
NtOpenSymbolicLinkObject(LinkHandle=0x5c5b7fedf8 [0x4c], DesiredAccess=0x1,
ObjectAttributes=0x48:"KnownDllPath") => 0
```

```
NtQuerySymbolicLinkObject(LinkHandle=0x4c, LinkTarget="C:\WINDOWS\System32",
ReturnedLength=0x5c5b7fed90 [0x28]) => 0
NtClose(Handle=0x4c) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fec50 [0x00007ffbbb3cb000],
Size=0x5c5b7fec48 [0x4000], NewProtect=4, OldProtect=0x5c5b7fec40 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fec80 [0x00007ffbbb3cb000],
Size=0x5c5b7fec78 [0x4000], NewProtect=2, OldProtect=0x5c5b7fec70 [4]) => 0
NtCreateEvent(EventHandle=0x7ffbbb3b62d8 [0x50],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
NtCreateEvent(EventHandle=0x7ffbbb3b6310 [0x58],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe480 [0x000001714dda5000],
ZeroBits=0, pSize=0x5c5b7fe528 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7febe0 [0x00007ffbbb3cb000],
Size=0x5c5b7febd8 [0x4000], NewProtect=4, OldProtect=0x5c5b7febd0 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7febe0 [0x00007ffbbb3cb000],
Size=0x5c5b7febd8 [0x4000], NewProtect=2, OldProtect=0x5c5b7febd0 [4]) => 0
NtOpenFile(FileHandle=0x5c5b7fec88 [0x64], DesiredAccess=SYNCHRONIZE|0x20,
ObjectAttributes="\??\D:\Users\lenovo\Desktop\osi\OSmai\Lab3\", IoStatusBlock=0x5c5b7febf8
[0/1], ShareAccess=3, OpenOptions=0x21) => 0
NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0x5c5b7febf8 [0/8],
FsInformation=0x5c5b7febe0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtSetEvent(EventHandle=0x50, PrevState=null) => 0
NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x5c5b7fe950) => 0xc000007c [1008 '╧юя√Єър ёё√ыьш эр эхёє·хёЄтє■·шщ Єюъхэ.']
NtOpenSection(SectionHandle=0x5c5b7fe8e8 [0x68], DesiredAccess=0xd,
ObjectAttributes=0x48:"KERNEL32.DLL") => 0
Loaded DLL at 00007FFBBA400000 C:\WINDOWS\System32\KERNEL32.DLL
NtMapViewOfSection(SectionHandle=0x68, ProcessHandle=-1, BaseAddress=0x1714dda56b0
[0x00007ffbba400000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1714dda5608
[0x000c4000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5c5b7fe740 [2.5757e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe6d0 [0x00007ffbba4c1000],
Size=0x5c5b7fe6c8 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe6c0 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe750 [0x00007ffbbb3cb000],
Size=0x5c5b7fe748 [0x4000], NewProtect=4, OldProtect=0x5c5b7fe740 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe750 [0x00007ffbbb3cb000],
Size=0x5c5b7fe748 [0x4000], NewProtect=2, OldProtect=0x5c5b7fe740 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe790 [0x00007ffbba483000],
Size=0x5c5b7fe798 [0x4000], NewProtect=4, OldProtect=0x1714dda55f0 [2]) => 0
NtOpenSection(SectionHandle=0x5c5b7fe188 [0x6c], DesiredAccess=0xd,
ObjectAttributes=0x48:"KERNELBASE.dll") => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fd890 [0x000001714dda6000],
ZeroBits=0, pSize=0x5c5b7fd938 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
Loaded DLL at 00007FFBB8500000 C:\WINDOWS\System32\KERNELBASE.dll
NtMapViewOfSection(SectionHandle=0x6c, ProcessHandle=-1, BaseAddress=0x1714dda5df0
[0x00007ffbb8500000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1714dda5d48
[0x003b9000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5c5b7fdfe0 [2.5757e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fdf70 [0x00007ffbb8887000],
Size=0x5c5b7fdf68 [0x1000], NewProtect=2, OldProtect=0x5c5b7fdf60 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fdff0 [0x00007ffbbb3cb000],
Size=0x5c5b7fdfe8 [0x4000], NewProtect=4, OldProtect=0x5c5b7fdfe0 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fdff0 [0x00007ffbbb3cb000],
Size=0x5c5b7fdfe8 [0x4000], NewProtect=2, OldProtect=0x5c5b7fdfe0 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe030 [0x00007ffbb876f000],
Size=0x5c5b7fe038 [0x2000], NewProtect=4, OldProtect=0x1714dda5d30 [2]) => 0
NtClose(Handle=0x6c) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1714dda55d0 [0x00007ffbba483000],
Size=0x1714dda55d8 [0x4000], NewProtect=2, OldProtect=0x5c5b7fe590 [4]) => 0
NtClose(Handle=0x68) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1714dda5d10 [0x00007ffbb876f000],
Size=0x1714dda5d18 [0x2000], NewProtect=2, OldProtect=0x5c5b7fe6d0 [4]) => 0
NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x5c5b7fe630, Length=0x28) => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0x5c5b7fe410, Length=8, ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffbb8868ec0, Length=0x40, ReturnLength=null) => 0
NtOpenSection(SectionHandle=0x5c5b7fe1d0 [0x68], DesiredAccess=0x4,
ObjectAttributes="\Sessions\9\Windows\SharedSection") => 0
NtCreateSection(SectionHandle=0x5c5b7fe1f0 [0x6c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0x5c5b7fe1e0 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0
NtConnectPort(PortHandle=0x7ffbbb3b6c08 [0x70], PortName="\Sessions\9\Windows\ApiPort",
SecurityQos=0x5c5b7fe310, ClientView=0x5c5b7fe208, ServerView=0x5c5b7fe238,
MaxMsgLength=0x5c5b7fe200 [0x3b8], ConnectionInfo=0x5c5b7fe280,
ConnectionInfoLength=0x5c5b7fe1d8 [0x30]) => 0
NtClose(Handle=0x6c) => 0
NtMapViewOfSection(SectionHandle=0x68, ProcessHandle=-1, BaseAddress=0x5c5b7fe1e8
[0x00007ff42d500000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5c5b7fe1f8
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0
NtClose(Handle=0x68) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x1714dbf0000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x5c5b7fded0, Length=0x30, ReturnLength=null) =>
0
NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x5c5b7fe3b8 [0x000001714dc00000], SectionSize=null) => 0
NtInitializeNlsFiles(BaseAddress=0x5c5b7fe3b0 [0x000001714dcb0000],
DefaultLocaleId=0x7ffbb886abb8 [0x419], DefaultCasingTableSize=null) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fdb00 [0x000001714dda7000],
ZeroBits=0, pSize=0x5c5b7fdba8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x5c5b7fe390 [0x000001714dd80000], SectionSize=0x5c5b7fe358 [0x00011000]) =>
0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x5c5b7fe390 [0x000001714dea0000], SectionSize=0x5c5b7fe358 [0x00011000]) =>
0
NtCreateFile(FileHandle=0x5c5b7fe418 [0x68], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f,
ObjectAttributes=4:"\Connect", IoStatusBlock=0x5c5b7fddd0 [0/0x18], AllocationSize=null,
FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20,
EaBuffer=0x1714dda7270, EaLength=0x54b) => 0
NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5c5b7fe360 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0x5c5b7fe380, OutputBufferLength=8) => 0
NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0x5c5b7fe388, Length=8) => 0
NtDeviceIoControlFile(FileHandle=0x68, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5c5b7fe150, IoControlCode=0x00500016, InputBuffer=0x5c5b7fe160,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fe268, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fe268, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fe260 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fe2b8, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fe2d0, OutputBufferLength=0x78, ReturnLength=0x5c5b7fe2b0 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fe4c8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fe4c8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fe4c0 [0xa0]) => 0
NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x5c5b7fe270 [0x78]) =>
0
NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0xc [TokenSessionId],
TokenInformation=0x5c5b7fdb90, Length=4, ReturnLength=0x5c5b7fdb70 [4]) => 0
NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0x5c5b7fdbd8, Length=4, ReturnLength=0x5c5b7fdb70 [4]) => 0
NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x2a
[TokenPrivateNameSpace], TokenInformation=0x5c5b7fdb74, Length=4, ReturnLength=0x5c5b7fdb70
[4]) => 0
NtOpenDirectoryObject(DirectoryHandle=0x5c5b7fdb98 [0x7c], DesiredAccess=0xf,
ObjectAttributes="\Sessions\9\BaseNamedObjects") => 0
NtQueryInformationToken(TokenHandle=0x78, TokenInformationClass=0x2c [TokenBnoIsolation],
TokenInformation=0x5c5b7fde90, Length=0x120, ReturnLength=0x5c5b7fdb70 [0x10]) => 0
NtClose(Handle=0x78) => 0
NtCreateMutant(MutantHandle=0x5c5b7fe2c8 [0x80],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x7c:"Local\SM0:67588:304:WilStaging_02", InitialOwner=false) => 0
NtWaitForSingleObject(Handle=0x80, Alertable=false, Timeout=null) => 0
```

```
NtOpenSemaphore(SemaphoreHandle=0x5c5b7fe088,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"Local\SM0:67588:304:WilStaging_02_p0") => 0xc0000034 [2 '=x
єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtCreateSemaphore(SemaphoreHandle=0x5c5b7fdfe8 [0x4c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"Local\SM0:67588:304:WilStaging_02_p0", InitialCount=0x53769d34,
MaxCount=0x53769d34) => 0
NtCreateSemaphore(SemaphoreHandle=0x5c5b7fdfe8 [0x78],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"Local\SM0:67588:304:WilStaging_02_p0h", InitialCount=0xb8,
MaxCount=0xb8) => 0
NtReleaseMutant(MutantHandle=0x80, PreviousCount=null) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fe4a8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fe4a8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fe4a0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fe4f8, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fe510, OutputBufferLength=0x78, ReturnLength=0x5c5b7fe4f0 [0]) => 0
NtQueryWnfStateData(StateName=0x5c5b7fe390 [0xa3bc0875], TypeId=0x5c5b7fe438,
ExplicitScope=null, ChangeStamp=0x5c5b7fe384 [0x21], Buffer=0x5c5b7fd380,
BufferSize=0x5c5b7fe380 [8]) => 0
NtCreateEvent(EventHandle=0x5c5b7fe300 [0x88],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1714dda7ca0 [0x8c],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtSetWnfProcessNotificationEvent(NotificationEvent=0x88) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x8c, IoCompletionHandle=0x28,
TargetObjectHandle=0x88, KeyContext=0x1714dda7cb8, ApcContext=0x1714dda7b30, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5c5b7fe280 [0x4dda0c00]) => 0
NtSubscribeWnfStateChange(StateName=0x1714dda7e30 [0xa3bc0875], ChangeStamp=0x21,
EventMask=0x11, SubscriptionId=0x5c5b7fe370 [0x00012346]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fdc00 [0x000001714dda8000],
ZeroBits=0, pSize=0x5c5b7fdca8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0x5c5b7fe1f0 [0], Alignment=0x18,
SystemInformation=0x5c5b7fe210, Length=0x50, ReturnLength=null) => 0
NtMapViewOfSection(SectionHandle=0x90, ProcessHandle=-1, BaseAddress=0x5c5b7fe180
[0x000001714dec0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5c5b7fe190
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0
NtMapViewOfSection(SectionHandle=0x94, ProcessHandle=-1, BaseAddress=0x5c5b7fe180
[0x000001714ded0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5c5b7fe190
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0
NtMapViewOfSection(SectionHandle=0x98, ProcessHandle=-1, BaseAddress=0x5c5b7fe180
[0x000001714dee0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5c5b7fe190
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0
NtClose(Handle=0x90) => 0
NtClose(Handle=0x94) => 0
NtClose(Handle=0x98) => 0
NtSetTimer2(TimerHandle=0x2c, DueTime=0x5c5b7fe300 [-3e+09], Period=null,
Parameters=0x5c5b7fe308) => 0
NtOpenKey(KeyHandle=0x5c5b7fe4a0, 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=0x5c5b7fe4a8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fe4a8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fe4a0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fe4f8, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fe510, OutputBufferLength=0x78, ReturnLength=0x5c5b7fe4f0 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fe4d8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fe4d8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fe4d0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fe528, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fe540, OutputBufferLength=0x78, ReturnLength=0x5c5b7fe520 [0]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe3f0 [0x00007ffbbb3cb000],
Size=0x5c5b7fe3e8 [0x4000], NewProtect=4, OldProtect=0x5c5b7fe3e0 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe3f0 [0x00007ffbbb3cb000],
Size=0x5c5b7fe3e8 [0x4000], NewProtect=2, OldProtect=0x5c5b7fe3e0 [4]) => 0
NtOpenKey(KeyHandle=0x5c5b7fe3c0, DesiredAccess=0x9, ObjectAttributes=0x18:"parent.exe") =>
0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5c5b7fe478 [0x94], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0
```

```
NtQueryValueKey(KeyHandle=0x94, ValueName="TSAppCompat", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x1714dda89e0, Length=0x224,
ResultLength=0x5c5b7fe468) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0x94, ValueName="TSUserEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x1714dda89e0, Length=0x224,
ResultLength=0x5c5b7fe468 [0x10]) => 0
NtClose(Handle=0x94) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffbba4b9a80, Length=0x40, ReturnLength=null) => 0
NtSetEvent(EventHandle=0x50, PrevState=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=4, OldProtect=0x5c5b7fe588 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe578 [0x00007ffbb8887000],
Size=0x5c5b7fe570 [0x1000], NewProtect=2, OldProtect=0x5c5b7fe588 [4]) => 0
NtOpenKey(KeyHandle=0x5c5b7feb40, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5c5b7feb20 [0xa0], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0
NtQueryKey(KeyHandle=0xa0, KeyInformationClass=2 [KeyFullInformation],
KeyInformation=0x5c5b7feb98, Length=0x30, ResultLength=0x5c5b7feb10 [0x2c]) => 0
NtClose(Handle=0xa0) => 0
NtOpenKey(KeyHandle=0x5c5b7feb18 [0xa4], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0
NtQueryValueKey(KeyHandle=0xa4, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7febd0, Length=0x50,
ResultLength=0x5c5b7feb10) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0xa4) => 0
```

```
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5c5b7fea40, Length=0x58, ReturnLength=0x5c5b7fea38 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7feb18, 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=0x5c5b7febf0 [0xa8], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0
NtQueryValueKey(KeyHandle=0xa8, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec30, Length=0x14,
ResultLength=0x5c5b7febf8 [0x10]) => 0
NtClose(Handle=0xa8) => 0
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5c5b7feb80 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x5c5b7feb78) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5c5b7feb80 [6], Alignment=4,
SystemInformation=0x1714dda5d60, Length=0x30, ReturnLength=0x5c5b7feb78 [0x30]) => 0
NtCreateIoCompletion(IoHandle=0x1714dda5930 [0xac],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0
NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x1714dda5928 [0xa8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0xac, WorkerProcessHandle=-1, StartRoutine=0x7ffbbb265580,
StartParameter=0x1714dda58f0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa8, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0x5c5b7fec28, BufferLength=4) => 0
NtCreateTimer2(TimerHandle=0x1714dda5980 [0xa4], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1714dda5988 [0xa0],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xa0, IoCompletionHandle=0xac,
TargetObjectHandle=0xa4, KeyContext=0x1714dda5990, ApcContext=0x1714dda5960, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x5c5b7feb40 [0]) => 0
NtCreateTimer2(TimerHandle=0x1714dda59f8 [0x90], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x17100000002) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x1714dda5a00 [0x94],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x94, IoCompletionHandle=0xac,
TargetObjectHandle=0x90, KeyContext=0x1714dda5a08, ApcContext=0x1714dda5960, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5c5b7feb40 [0]) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa8, InformationClass=2
[WorkerFactoryIdleTimeout], Buffer=0x5c5b7fec28, BufferLength=8) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa8, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x5c5b7fec28, BufferLength=4) => 0
NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x5c5b7feca0) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fec20 [0x00007ff6f623f000],
Size=0x5c5b7fec28 [0x1000], NewProtect=4, OldProtect=0x5c5b7fef70 [8]) => 0
NtOpenSection(SectionHandle=0x5c5b7fe618 [0xb0], DesiredAccess=0xd,
ObjectAttributes=0x48:"msvcrt.dll") => 0
Loaded DLL at 00007FFBBA550000 C:\WINDOWS\System32\msvcrt.dll
NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x1714dda8a10
[0x00007ffbba550000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1714dda5ba8
[0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5c5b7fe470 [2.5757e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe480 [0x00007ffbbb3cb000],
Size=0x5c5b7fe478 [0x4000], NewProtect=4, OldProtect=0x5c5b7fe470 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe480 [0x00007ffbbb3cb000],
Size=0x5c5b7fe478 [0x4000], NewProtect=2, OldProtect=0x5c5b7fe470 [4]) => 0
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x5c5b7fdf30, Length=0x330, ReturnLength=0x5c5b7fdee8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x5c5b7fdf30, Length=0x330, ReturnLength=0x5c5b7fdee8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
```

```
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbba550000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x5c5b7fe1a8, Length=0x30, ReturnLength=null)
=> 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fe4c0 [0x00007ffbba5ce000],
Size=0x5c5b7fe4c8 [0x1000], NewProtect=4, OldProtect=0x1714dda5b90 [2]) => 0
NtClose(Handle=0xb0) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fef50 [0x00007ff6f623f000],
Size=0x5c5b7fef58 [0x1000], NewProtect=8, OldProtect=0x5c5b7fea20 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1714dda5b70 [0x00007ffbba5ce000],
Size=0x1714dda5b78 [0x1000], NewProtect=2, OldProtect=0x5c5b7fea20 [4]) => 0
NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x5c5b7fe980, Length=0x28) => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11
[ThreadHideFromDebugger], ThreadInformation=0x5c5b7feca0, Length=1, ReturnLength=null) => 0
Initial breakpoint
NtSetEvent(EventHandle=0x50, PrevState=null) => 0
NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x5c5b7fec10 [0xb4]) =>
0
NtQueryInformationToken(TokenHandle=0xb4, TokenInformationClass=0xa [TokenStatistics],
TokenInformation=0x5c5b7fec20, Length=0x38, ReturnLength=0x5c5b7fec18 [0x38]) => 0
NtClose(Handle=0xb4) => 0
NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode",
Type=0x5c5b7fe81c [4], Buffer=0x5c5b7fe810, Length=4, ReturnedLength=0x5c5b7fe814 [4]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe3b0 [0x000001714def0000],
ZeroBits=0, pSize=0x5c5b7fe3b8 [0x00150000], flAllocationType=0x2000, flProtect=4) => 0
NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe3b0 [0x000001714def0000],
pSize=0x5c5b7fe3a8 [0x00140000], flFreeType=0x8000) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe398 [0x000001714e030000],
ZeroBits=0, pSize=0x5c5b7fe390 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe020 [0x000001714dda9000],
ZeroBits=0, pSize=0x5c5b7fe0c8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtQueryVolumeInformationFile(FileHandle=0x54, IoStatusBlock=0x5c5b7fe960 [0/8],
FsInformation=0x5c5b7fe980, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtQueryVolumeInformationFile(FileHandle=0xc5c, IoStatusBlock=0x5c5b7fe960 [0/8],
FsInformation=0x5c5b7fe980, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtQueryVolumeInformationFile(FileHandle=0x60, IoStatusBlock=0x5c5b7fe960 [0/8],
FsInformation=0x5c5b7fe980, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe1c0 [0x000001714ddaa000],
ZeroBits=0, pSize=0x5c5b7fe268 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe170 [0x000001714e032000],
ZeroBits=0, pSize=0x5c5b7fe218 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtOpenKey(KeyHandle=0x5c5b7fd6a0 [0xb4], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions")
=> 0
NtQueryValueKey(KeyHandle=0xb4, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x5c5b7fdb80, Length=0x214,
ResultLength=0x5c5b7fdb28 [0x2a]) => 0
NtQueryValueKey(KeyHandle=0xb4, ValueName="000604xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x5c5b7fdb60, Length=0x214,
ResultLength=0x5c5b7fd908 [0x42]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe190 [0x000001714e033000],
ZeroBits=0, pSize=0x5c5b7fe238 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fe170 [0x000001714e034000],
ZeroBits=0, pSize=0x5c5b7fe218 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbba5ded28, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x5c5b7fe790, Length=0x18, ReturnLength=null) =>
0
NtSetEvent(EventHandle=0x50, PrevState=null) => 0
NtOpenKey(KeyHandle=0x5c5b7feca0 [0xb0], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelaySleepLoopWindowSize",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec00,
Length=0x50, ResultLength=0x5c5b7febf0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelaySpinCountThreshold",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec00,
Length=0x50, ResultLength=0x5c5b7febf0) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
```

```
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelayBaseYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec00, Length=0x50,
ResultLength=0x5c5b7febf0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtFactorYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec00, Length=0x50,
ResultLength=0x5c5b7febf0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelayMaxYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fec00, Length=0x50,
ResultLength=0x5c5b7febf0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0xb0) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0xa8, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x5c5b7fef78, BufferLength=4) => 0
NtSetEvent(EventHandle=0xc, PrevState=null) => 0
NtTestAlert() => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6f62327f0, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x5c5b7ff4c0, Length=0x30,
ReturnLength=0x5c5b7ff470 [0x30]) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6f62327f0, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x5c5b7ff4f0, Length=0x30, ReturnLength=null)
=> 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff6f62327f0, MemoryInformationClass=2
[MemoryMappedFilenameInformation], MemoryInformation=0x5c5b7ff568, Length=0x21a,
ReturnLength=null) => 0
NtCreateSection(SectionHandle=0x5c5b7fe9c0 [0xb0],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x7,
ObjectAttributes=0x7c:"SharedMemory", SectionSize=0x5c5b7fe9b0 [1024], Protect=4,
Attributes=0x08000000, FileHandle=0) => 0
NtCreateSemaphore(SemaphoreHandle=0x5c5b7fe9a8 [0xb8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"SemaphoreParent", InitialCount=1, MaxCount=1) => 0
NtCreateSemaphore(SemaphoreHandle=0x5c5b7fe9a8 [0xbc],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x7c:"SemaphoreChild", InitialCount=0, MaxCount=1) => 0
NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x5c5b7fea18
[0x000001714def0000], ZeroBits=0, CommitSize=0, SectionOffset=0x5c5b7fea10 [0],
ViewSize=0x5c5b7fea20 [0x1000], InheritDisposition=1 [ViewShare], AllocationType=0,
Protect=4) => 0
Enter file name: NtWriteFile(FileHandle=0xc5c, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5c5b7fea70 [0/0x11], Buffer=0x7ff6f623a086, Length=0x11, ByteOffset=null,
Key=null) => 0
NtReadFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5c5b7fea70 [0/7], Buffer=0x5c5b7ff370, Length=0x400, ByteOffset=null,
Key=null) => 0
NtQueryAttributesFile(ObjectAttributes="\??\D:\Users\lenovo\Desktop\osi\OSmai\Lab3\child.exe
", Attributes=0x5c5b7fca70 [ARCHIVE]) => 0
NtQueryAttributesFile(ObjectAttributes="\??\D:\Users\lenovo\Desktop\osi\OSmai\Lab3\child.exe
", AttributesЫ=0x5c5b7fce48 [ARCHIVE]) => 0
NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x5c5b7fc2d0) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']
NtOpenSection(SectionHandle=0x5c5b7fc268 [0xc0], DesiredAccess=0xd,
ObjectAttributes=0x48:"sechost.dll") => 0
Loaded DLL at 00007FFBB9BD0000 C:\WINDOWS\System32\sechost.dll
NtMapViewOfSection(SectionHandle=0xc0, ProcessHandle=-1, BaseAddress=0x1714dda9ae0
[0x00007ffbb9bd0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1714dda5ba8
[0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5c5b7fc0c0 [2.57577e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fc050 [0x00007ffbb9c72000],
Size=0x5c5b7fc048 [0x1000], NewProtect=2, OldProtect=0x5c5b7fc040 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fc0d0 [0x00007ffbbb3cb000],
Size=0x5c5b7fc0c8 [0x4000], NewProtect=4, OldProtect=0x5c5b7fc0c0 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fc0d0 [0x00007ffbbb3cb000],
Size=0x5c5b7fc0c8 [0x4000], NewProtect=2, OldProtect=0x5c5b7fc0c0 [4]) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbb9bd0000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x5c5b7fbdf8, Length=0x30, ReturnLength=null)
=> 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fc110 [0x00007ffbb9c4c000],
Size=0x5c5b7fc118 [0x2000], NewProtect=4, OldProtect=0x1714dda5b90 [2]) => 0
NtOpenSection(SectionHandle=0x5c5b7fbb08 [0xc4], DesiredAccess=0xd,
ObjectAttributes=0x48:"bcrypt.dll") => 0
Loaded DLL at 00007FFBB8EC0000 C:\WINDOWS\System32\bcrypt.dll
```

```
NtMapViewOfSection(SectionHandle=0xc4, ProcessHandle=-1, BaseAddress=0x1714dda9f70
[0x00007ffbb8ec0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x1714dda9ed8
[0x00028000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5c5b7fb960 [2.57577e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fb8f0 [0x00007ffbb8ee5000],
Size=0x5c5b7fb8e8 [0x1000], NewProtect=2, OldProtect=0x5c5b7fb8e0 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fb970 [0x00007ffbbb3cb000],
Size=0x5c5b7fb968 [0x4000], NewProtect=4, OldProtect=0x5c5b7fb960 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fb970 [0x00007ffbbb3cb000],
Size=0x5c5b7fb968 [0x4000], NewProtect=2, OldProtect=0x5c5b7fb960 [4]) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbb8ec0000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x5c5b7fb698, Length=0x30, ReturnLength=null)
=> 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fb9b0 [0x00007ffbb8edc000],
Size=0x5c5b7fb9b8 [0x1000], NewProtect=4, OldProtect=0x1714dda9ec0 [2]) => 0
NtClose(Handle=0xc4) => 0
NtClose(Handle=0xc0) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1714dda9ea0 [0x00007ffbb8edc000],
Size=0x1714dda9ea8 [0x1000], NewProtect=2, OldProtect=0x5c5b7fc050 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x1714dda5b70 [0x00007ffbb9c4c000],
Size=0x1714dda5b78 [0x2000], NewProtect=2, OldProtect=0x5c5b7fc050 [4]) => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fbe28, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fbe28, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fbe20 [0xa0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fbe88, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fbe88, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fbe80 [0xa0]) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x56
[ProcessEnclaveInformation], ProcessInformation=0x5c5b7fbf10, Length=0xb0,
ReturnLength=null) => 0xc0000003 [87 '╧рЁрьхЄЁ чрфрэ эхтхЁэю.']
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0
[ProcessBasicInformation], ProcessInformation=0x5c5b7fbe90, Length=0x40, ReturnLength=null)
=> 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fbe38, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fbe38, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fbe30 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fbe88, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fbea0, OutputBufferLength=0x78, ReturnLength=0x5c5b7fbe80 [0]) => 0
NtCreateSemaphore(SemaphoreHandle=0x5c5b7fbe48 [0xc0], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0
NtCreateSemaphore(SemaphoreHandle=0x5c5b7fbe58 [0xd0], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes=null, InitialCount=0, MaxCount=0x7fffffff) => 0
NtCreateEvent(EventHandle=0x5c5b7fbe48 [0xd4],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
NtOpenFile(FileHandle=0x7ffbb8ee27a0 [0xd8], DesiredAccess=SYNCHRONIZE|0x3,
ObjectAttributes="\Device\KsecDD", IoStatusBlock=0x5c5b7fbd90 [0/0], ShareAccess=7,
OpenOptions=0x20) => 0
NtDeviceIoControlFile(FileHandle=0xd8, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5c5b7fbe30 [0/0], IoControlCode=0x00390400, InputBuffer=0x5c5b7fbf10,
InputBufferLength=0x68, OutputBuffer=0x5c5b7fbe40, OutputBufferLength=8) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fbde8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fbde8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fbde0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fbe38, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fbe50, OutputBufferLength=0x78, ReturnLength=0x5c5b7fbe30 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fbde8, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fbde8, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fbde0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fbe38, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fbe50, OutputBufferLength=0x78, ReturnLength=0x5c5b7fbe30 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fbe18, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fbe18, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fbe10 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5c5b7fbe68, InputBufferLength=0x18,
OutputBuffer=0x5c5b7fbe80, OutputBufferLength=0x78, ReturnLength=0x5c5b7fbe60 [0]) => 0
NtSetEvent(EventHandle=0x50, PrevState=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fc7a8 [0x00007ffbb8887000],
Size=0x5c5b7fc7a0 [0x1000], NewProtect=4, OldProtect=0x5c5b7fc7b8 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5c5b7fc7a8 [0x00007ffbb8887000],
Size=0x5c5b7fc7a0 [0x1000], NewProtect=2, OldProtect=0x5c5b7fc7b8 [4]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5c5b7fc0b0 [0x000001714ddac000],
ZeroBits=0, pSize=0x5c5b7fc158 [0x3000], flAllocationType=0x1000, flProtect=4) => 0
```

```
NtOpenKey(KeyHandle=0x5c5b7fce00, DesiredAccess=0x9, ObjectAttributes=0x18:"child.exe") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5c5b7fcde0, DesiredAccess=0x101,
ObjectAttributes="\Registry\Machine\Software\Microsoft\Wow64\x86\xtajit") => 0xc0000034 [2
'=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtCreateUserProcess(ProcessHandle=0x5c5b7fcf90 [0xec], ThreadHandle=0x5c5b7fd010 [0xe8],
ProcessDesiredAccess=MAXIMUM_ALLOWED, ThreadDesiredAccess=MAXIMUM_ALLOWED,
ProcessObjectAttributes=null, ThreadObjectAttributes=null, ProcessFlags=0x200,
ThreadFlags=1, ProcessParameters=0x1714ddaba40
["D:\Users\lenovo\Desktop\osi\OSmai\Lab3\child.exe"], CreateInfo=0x5c5b7fd2e0,
AttributeList=0x5c5b7fd780) => 0
NtOpenKey(KeyHandle=0x5c5b7fcea8, DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session
Manager\AppCertDlls") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0xa, TokenHandle=0x5c5b7fcb60 [0xf8]) =>
0
NtQueryInformationToken(TokenHandle=0xf8, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5c5b7fcdb0, Length=0x90, ReturnLength=0x5c5b7fcb88 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fcb80, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5c5b7fcb48 [0xfc], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0
NtQueryValueKey(KeyHandle=0xfc, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fcc90, Length=0x50,
ResultLength=0x5c5b7fcb40) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xfc, ValueName="AuthenticodeEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fcc90, Length=0x50,
ResultLength=0x5c5b7fcb40 [0x10]) => 0
NtClose(Handle=0xfc) => 0
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5c5b7fca70, Length=0x58, ReturnLength=0x5c5b7fca68 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fcb48, 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.']
NtClose(Handle=0xf8) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5c5b7fcc08, InputBufferLength=0xa0,
OutputBuffer=0x5c5b7fcc08, OutputBufferLength=0xa0, ReturnLength=0x5c5b7fcc00 [0xa0]) => 0
NtQueryInformationProcess(ProcessHandle=0xec, ProcessInformationClass=0x3c
[ProcessCommandLineInformation], ProcessInformation=0x1714ddad3a0, Length=0x400,
ReturnLength=0x5c5b7fcb30 [0x30]) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap],
ProcessInformation=0x5c5b7fc610, Length=0x24, ReturnLength=null) => 0
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5c5b7fc7b0, Length=0x54, ReturnLength=0x5c5b7fc790 [0x2c]) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x17 [ProcessDeviceMap],
ProcessInformation=0x5c5b7fc5a0, Length=0x24, ReturnLength=null) => 0
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5c5b7fc950, Length=0x58, ReturnLength=0x5c5b7fc948 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fcac8 [0xf8], DesiredAccess=0x1,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-
1001\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders") => 0
NtQueryValueKey(KeyHandle=0xf8, ValueName="Cache", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x1714ddada10, Length=0x208,
ResultLength=0x5c5b7fcac0 [0x94]) => 0
NtClose(Handle=0xf8) => 0
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5c5b7fc950, Length=0x58, ReturnLength=0x5c5b7fc948 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fca70 [0xf8], DesiredAccess=0x8,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-
1001\Software\Microsoft\Windows NT\CurrentVersion") => 0
NtOpenKey(KeyHandle=0x5c5b7fca78 [0xfc], DesiredAccess=0x101,
ObjectAttributes=0xf8:"AppCompatFlags\Layers") => 0
NtQueryValueKey(KeyHandle=0xfc,
ValueName="D:\Users\lenovo\Desktop\osi\OSmai\Lab3\child.exe", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5c5b7fcad8, Length=0x10,
ResultLength=0x5c5b7fca80) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0xfc) => 0
NtApphelpCacheControl(ServiceClass=0xb, ServiceData="") => 0
```

```
NtQueryInformationProcess(ProcessHandle=0xec, ProcessInformationClass=0
[ProcessBasicInformation], ProcessInformation=0x5c5b7fcdd0, Length=0x40, ReturnLength=null)
=> 0
NtOpenKey(KeyHandle=0x5c5b7fcb80 [0x104], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide")
=> 0
NtQueryValueKey(KeyHandle=0x104, ValueName="PreferExternalManifest",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5c5b7fcbd0,
Length=0x14, ResultLength=0x5c5b7fcb88) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x104) => 0
NtQueryVolumeInformationFile(FileHandle=0xf0, IoStatusBlock=0x5c5b7fcbe0 [0/8],
FsInformation=0x5c5b7fcc10, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtGetMUIRegistryInfo(Flags=0, BufferLength=0x5c5b7fca00 [0x4d0], Buffer=null) => 0
NtGetMUIRegistryInfo(Flags=0, BufferLength=0x5c5b7fca00 [0x4d0], Buffer=0x1714ddaba40) => 0
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5c5b7fc830, Length=0x58, ReturnLength=0x5c5b7fc828 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fca18 [0x104], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0
NtOpenKey(KeyHandle=0x5c5b7fca10, DesiredAccess=KEY_READ, ObjectAttributes=0x104:"Control
Panel\Desktop\MuiCached\MachineLanguageConfiguration") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш
єърчрээ√щ Їрщы.']
NtClose(Handle=0x104) => 0
NtOpenKey(KeyHandle=0x5c5b7fc8a8, 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=0x5c5b7fc740, Length=0x58, ReturnLength=0x5c5b7fc738 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fc8b0 [0x108], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0
NtOpenKey(KeyHandle=0x5c5b7fc8b8, DesiredAccess=KEY_READ,
ObjectAttributes=0x108:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2
'=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5c5b7fc8a8, DesiredAccess=KEY_READ, ObjectAttributes=0x108:"Control
Panel\Desktop\LanguageConfiguration") => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x108) => 0
NtOpenKey(KeyHandle=0x5c5b7fc848, 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=0x5c5b7fc6b0, Length=0x58, ReturnLength=0x5c5b7fc6a8 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fc840 [0x108], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0
NtOpenKey(KeyHandle=0x5c5b7fc770, DesiredAccess=KEY_READ,
ObjectAttributes=0x108:"Software\Policies\Microsoft\Control Panel\Desktop") => 0xc0000034 [2
'=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5c5b7fc838 [0x10c], DesiredAccess=KEY_READ,
ObjectAttributes=0x108:"Control Panel\Desktop") => 0
NtQueryValueKey(KeyHandle=0x10c, ValueName="PreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1714dda8290,
Length=0xc, ResultLength=0x5c5b7fc808) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x10c) => 0
NtClose(Handle=0x108) => 0
NtOpenKey(KeyHandle=0x5c5b7fc848, 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=0x5c5b7fc6b0, Length=0x58, ReturnLength=0x5c5b7fc6a8 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5c5b7fc840 [0x108], DesiredAccess=MAXIMUM_ALLOWED,
ObjectAttributes="\REGISTRY\USER\S-1-5-21-3512441621-816733789-498939024-1001") => 0
NtOpenKey(KeyHandle=0x5c5b7fc838 [0x10c], DesiredAccess=KEY_READ,
ObjectAttributes=0x108:"Control Panel\Desktop\MuiCached") => 0
NtQueryValueKey(KeyHandle=0x10c, ValueName="MachinePreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1714dda8310,
Length=0xc, ResultLength=0x5c5b7fc808) => 0x80000005 [234 '╚ьх■Єё  фюяюыэшЄхы№э√х фрээ√х.']
NtQueryValueKey(KeyHandle=0x10c, ValueName="MachinePreferredUILanguages",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x1714dda8350,
Length=0x18, ResultLength=0x5c5b7fc808 [0x18]) => 0
NtClose(Handle=0x10c) => 0
NtClose(Handle=0x108) => 0
```

```
NtAlpcSendWaitReceivePort(PortHandle=0x70, SendFlags=0x00020000, SendMessage=0x5c5b7fdb70 [2
[LPC_REPLY] (560b)], InMessageBuffer=null, ReceiveBuffer=0x5c5b7fdb70,
ReceiveBufferSize=0x5c5b7fce80 [0x258], OutMessageBuffer=null, Timeout=null) => 0
NtQueryLicenseValue(Name="Kernel-OneCore-DeviceFamilyID", Type=0x5c5b7fca98 [4],
Buffer=0x5c5b7fca90, Length=4, ReturnedLength=0x5c5b7fcae0 [4]) => 0
NtAllocateVirtualMemory(ProcessHandle=0xec, lpAddress=0x5c5b7fd238 [0x00000184c7e30000],
ZeroBits=0, pSize=0x5c5b7fd3f0 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtWriteVirtualMemory(ProcessHandle=0xec, BaseAddress=0x184c7e30000, Buffer=0x1714ddabf40,
BufferLength=0x11c0, ReturnedLength=null) => 0
NtWriteVirtualMemory(ProcessHandle=0xec, BaseAddress=0x5b9e6972d8, Buffer=0x5c5b7fd238,
BufferLength=8, ReturnedLength=null) => 0
NtResumeThread(ThreadHandle=0xe8, SuspendCount=null) => 0
NtClose(Handle=0xf0) => 0
Process 74212 starting at 00007FF620FA13E0 with command line: "child.exe whore"
D:\Users\lenovo\Desktop\osi\OSmai\Lab3\child.exe
Loaded DLL at 00007FFBBB230000 ntdll.dll
NtClose(Handle=0xf4) => 0
Enter command: NtQueryPerformanceCounter(Counter=0x5b9e9ff960 [2.57577e+12], Freq=null) => 0
NtWriteFile(FileHandle=0xc5c, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5c5b7fea70 [0/0xf], Buffer=0x7ff6f623a0bf, Length=0xf, ByteOffset=null,
Key=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff9a8 [0x00007ffbbb3ce000],
Size=0x5b9e9ff9a0 [0x1000], NewProtect=4, OldProtect=0x5b9e9ff9e0 [8]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff9a8 [0x00007ffbbb3ce000],
Size=0x5b9e9ff9a0 [0x1000], NewProtect=8, OldProtect=0x5b9e9ff9e0 [4]) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbbb2d4240, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x5b9e9ff930, Length=0x18, ReturnLength=null) =>
0
NtCreateEvent(EventHandle=0x7ffbbb3b6398 [0x14],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0
NtManageHotPatch(Unknown=9, Unknown=0x5b9e9ff7c8 [1], Unknown=8, Unknown=0x5b9e9ff7c0) =>
0xc00000bb [50 '╥ръющ чряЁюё эх яюффхЁцштрхЄё .']
NtSetEvent(EventHandle=0x14, PrevState=null) => 0
NtCreateEvent(EventHandle=0x7ffbbb3b63e8 [0x18],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=0 [NotificationEvent], InitialState=false) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x5b9e9ff6e0, Length=0x40, ReturnLength=null) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x5b9e9ff3d8, Length=4, ReturnLength=null) => 0
NtOpenKey(KeyHandle=0x5b9e9ff288 [0x1c], DesiredAccess=GENERIC_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\CodePage") => 0
NtQueryValueKey(KeyHandle=0x1c, ValueName="ACP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2f0, Length=0x24,
ResultLength=0x5b9e9ff280 [0x16]) => 0
NtQueryValueKey(KeyHandle=0x1c, ValueName="OEMCP", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2f0, Length=0x24,
ResultLength=0x5b9e9ff280 [0x14]) => 0
NtClose(Handle=0x1c) => 0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x7ffbbb3b37e0 [0x00000184c7e40000], SectionSize=null) => 0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x7ffbbb3b37e8 [0x00000184c7e60000], SectionSize=null) => 0
NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x5b9e9ff378 [0x00000184c7e80000], SectionSize=null) => 0
NtQuerySystemInformation(SystemInformationClass=0xc0 [SystemFlushInformation],
SystemInformation=0x5b9e9ff330, Length=0x20, ReturnLength=null) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbbb230000, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x5b9e9ff2c0, Length=0x18, ReturnLength=null) =>
0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=null, MemoryInformationClass=4
[MemoryWorkingSetExInformation], MemoryInformation=0x5b9e9ff300, Length=0x50,
ReturnLength=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff350 [0x00007ffbbb3cb000],
Size=0x5b9e9ff348 [0x4000], NewProtect=2, OldProtect=0x5b9e9ff340 [4]) => 0
NtOpenKey(KeyHandle=0x5b9e9ff000 [0x20], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0
```

```
NtQueryValueKey(KeyHandle=0x20, ValueName="RaiseExceptionOnPossibleDeadlock",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff010,
Length=0x50, ResultLength=0x5b9e9ff008) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x20) => 0
NtOpenKey(KeyHandle=0x5b9e9fefe0, 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=0x7ffbbb3b7268, Length=4, ReturnLength=null) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x5b9e9ff2e8, Length=4, ReturnLength=null) => 0
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x5b9e9fec80, Length=0x330, ReturnLength=0x5b9e9fec38) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x5b9e9fec80, Length=0x330, ReturnLength=0x5b9e9fec38) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
NtOpenKey(KeyHandle=0x5b9e9ff230 [0x24], DesiredAccess=0x9,
ObjectAttributes="\Registry\Machine\SYSTEM\CurrentControlSet\Control\Session Manager") => 0
NtQueryValueKey(KeyHandle=0x24, ValueName="ResourcePolicies", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff270, Length=0x18,
ResultLength=0x5b9e9ff238) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x24) => 0
NtQueryInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x24 [ProcessCookie],
ProcessInformation=0x5b9e9ff340, Length=4, ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x5b9e9ff2e0, Length=0x40, ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0x3e [SystemEmulationBasicInformation],
SystemInformation=0x5b9e9ff310, Length=0x40, ReturnLength=null) => 0
NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffbbb3b7a88 [0x00007ff534460000],
ZeroBits=0x0000005b9e9ff290, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x5b9e9ff1d8, DataCount=1) => 0
NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffbbb3b7a80 [0x00007ff536460000],
ZeroBits=0x0000005b9e9ff298, pSize=0x1000 [0], flAllocationType=4, DataBuffer=null,
DataCount=0) => 0
NtAllocateVirtualMemoryEx(ProcessHandle=-1, lpAddress=0x7ffbbb3b7af0 [0x00007ff434440000],
ZeroBits=0x0000005b9e9ff240, pSize=0x102000 [0], flAllocationType=4,
DataBuffer=0x5b9e9ff188, DataCount=1) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x5b9e9ff180, Length=0x40, ReturnLength=null) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fed60 [0x00000184c7e90000],
ZeroBits=0, pSize=0x5b9e9fed68 [0x00250000], flAllocationType=0x2000, flProtect=4) => 0
NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fed60 [0x00000184c7e90000],
pSize=0x5b9e9fed58 [0x00150000], flFreeType=0x8000) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fed48 [0x00000184c7fe0000],
ZeroBits=0, pSize=0x5b9e9fed40 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtQuerySystemInformation(SystemInformationClass=0xc5
[SystemHypervisorSharedPageInformation], SystemInformation=0x5b9e9ff4e0, Length=8,
ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0x37 [SystemNumaProcessorMap],
SystemInformation=0x5b9e9fef50, Length=0x408, ReturnLength=0x5b9e9ff370 [0x18]) => 0
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9e9fef38 [4], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x5b9e9fef30) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9e9fef38 [4], Alignment=4,
SystemInformation=0x184c7fe0880, Length=0x50, ReturnLength=0x5b9e9fef30 [0x50]) => 0
NtCreateEvent(EventHandle=0x5b9e9ff128 [0x24],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x184c7fe0c40 [0x28],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9e9feea0 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x5b9e9fee98) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9e9feea0 [6], Alignment=4,
SystemInformation=0x184c7fe0ff0, Length=0x30, ReturnLength=0x5b9e9fee98 [0x30]) => 0
```

```
NtCreateIoCompletion(IoHandle=0x184c7fe0d20 [0x2c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0
NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x184c7fe0d18 [0x30],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x2c, WorkerProcessHandle=-1, StartRoutine=0x7ffbbb265580,
StartParameter=0x184c7fe0ce0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0
NtCreateTimer2(TimerHandle=0x184c7fe0d70 [0x34], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x184c7fe0d78 [0x38],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x38, IoCompletionHandle=0x2c,
TargetObjectHandle=0x34, KeyContext=0x184c7fe0d80, ApcContext=0x184c7fe0d50, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x5b9e9fee60 [0]) => 0
NtCreateTimer2(TimerHandle=0x184c7fe0de8 [0x3c], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x18400000002) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x184c7fe0df0 [0x40],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x40, IoCompletionHandle=0x2c,
TargetObjectHandle=0x3c, KeyContext=0x184c7fe0df8, ApcContext=0x184c7fe0d50, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5b9e9fee60 [0]) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x30, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x5b9e9fef48, BufferLength=4) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x30, InformationClass=0xe
[WorkerFactoryThreadSoftMaximum], Buffer=0x5b9e9fef48, BufferLength=4) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x30, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x5b9e9ff068, BufferLength=4) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x28, IoCompletionHandle=0x2c,
TargetObjectHandle=0x24, KeyContext=0x184c7fe0c58, ApcContext=0x184c7fe0ad0, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5b9e9ff0b0 [0xc7fe0c00]) => 0
NtTraceControl(CtrlCode=0x1b, InputBuffer=0x5b9e9ff168, InputBufferLength=4,
OutputBuffer=null, OutputBufferLength=0, ReturnLength=0x5b9e9ff120 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9ff1c8, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9ff1c8, OutputBufferLength=0xa0, ReturnLength=0x5b9e9ff1c0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9e9ff218, InputBufferLength=0x18,
OutputBuffer=0x5b9e9ff230, OutputBufferLength=0x78, ReturnLength=0x5b9e9ff210 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9ff218, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9ff218, OutputBufferLength=0xa0, ReturnLength=0x5b9e9ff210 [0xa0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9ff218, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9ff218, OutputBufferLength=0xa0, ReturnLength=0x5b9e9ff210 [0xa0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9ff1c8, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9ff1c8, OutputBufferLength=0xa0, ReturnLength=0x5b9e9ff1c0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9e9ff218, InputBufferLength=0x18,
OutputBuffer=0x5b9e9ff230, OutputBufferLength=0x78, ReturnLength=0x5b9e9ff210 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9ff218, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9ff218, OutputBufferLength=0xa0, ReturnLength=0x5b9e9ff210 [0xa0]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9feb50 [0x00000184c7fe2000],
ZeroBits=0, pSize=0x5b9e9febf8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe770 [0x00000184c7fe4000],
ZeroBits=0, pSize=0x5b9e9fe818 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9ff370 [0x00000184c7dd0000],
pSize=0x5b9e9ff378 [0x00020000], flFreeType=0x8000) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff350 [0x00007ffbbb3cb000],
Size=0x5b9e9ff348 [0x4000], NewProtect=4, OldProtect=0x5b9e9ff340 [2]) => 0
NtOpenDirectoryObject(DirectoryHandle=0x7ffbbb3cb2b0 [0x58], DesiredAccess=0x3,
ObjectAttributes="\KnownDlls") => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff350 [0x00007ffbbb3cb000],
Size=0x5b9e9ff348 [0x4000], NewProtect=2, OldProtect=0x5b9e9ff340 [4]) => 0
NtOpenSymbolicLinkObject(LinkHandle=0x5b9e9ff4c8 [0x5c], DesiredAccess=0x1,
ObjectAttributes=0x58:"KnownDllPath") => 0
NtQuerySymbolicLinkObject(LinkHandle=0x5c, LinkTarget="C:\WINDOWS\System32",
ReturnedLength=0x5b9e9ff460 [0x28]) => 0
NtClose(Handle=0x5c) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff320 [0x00007ffbbb3cb000],
Size=0x5b9e9ff318 [0x4000], NewProtect=4, OldProtect=0x5b9e9ff310 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff350 [0x00007ffbbb3cb000],
Size=0x5b9e9ff348 [0x4000], NewProtect=2, OldProtect=0x5b9e9ff340 [4]) => 0
NtCreateEvent(EventHandle=0x7ffbbb3b62d8 [0x60],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
```

```
NtCreateEvent(EventHandle=0x7ffbbb3b6310 [0x5c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9feb50 [0x00000184c7fe5000],
ZeroBits=0, pSize=0x5b9e9febf8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff2b0 [0x00007ffbbb3cb000],
Size=0x5b9e9ff2a8 [0x4000], NewProtect=4, OldProtect=0x5b9e9ff2a0 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff2b0 [0x00007ffbbb3cb000],
Size=0x5b9e9ff2a8 [0x4000], NewProtect=2, OldProtect=0x5b9e9ff2a0 [4]) => 0
NtOpenFile(FileHandle=0x5b9e9ff358 [0x64], DesiredAccess=SYNCHRONIZE|0x20,
ObjectAttributes="\??\D:\Users\lenovo\Desktop\osi\OSmai\Lab3\", IoStatusBlock=0x5b9e9ff2c8
[0/1], ShareAccess=3, OpenOptions=0x21) => 0
NtQueryVolumeInformationFile(FileHandle=0x64, IoStatusBlock=0x5b9e9ff2c8 [0/8],
FsInformation=0x5b9e9ff2b0, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtSetEvent(EventHandle=0x60, PrevState=null) => 0
NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x5b9e9ff020) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']
NtOpenSection(SectionHandle=0x5b9e9fefb8 [0x1c], DesiredAccess=0xd,
ObjectAttributes=0x58:"KERNEL32.DLL") => 0
Loaded DLL at 00007FFBBA400000 C:\WINDOWS\System32\KERNEL32.DLL
NtMapViewOfSection(SectionHandle=0x1c, ProcessHandle=-1, BaseAddress=0x184c7fe56b0
[0x00007ffbba400000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x184c7fe5608
[0x000c4000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5b9e9fee10 [2.57577e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9feda0 [0x00007ffbba4c1000],
Size=0x5b9e9fed98 [0x1000], NewProtect=2, OldProtect=0x5b9e9fed90 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fee20 [0x00007ffbbb3cb000],
Size=0x5b9e9fee18 [0x4000], NewProtect=4, OldProtect=0x5b9e9fee10 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fee20 [0x00007ffbbb3cb000],
Size=0x5b9e9fee18 [0x4000], NewProtect=2, OldProtect=0x5b9e9fee10 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fee60 [0x00007ffbba483000],
Size=0x5b9e9fee68 [0x4000], NewProtect=4, OldProtect=0x184c7fe55f0 [2]) => 0
NtOpenSection(SectionHandle=0x5b9e9fe858 [0x68], DesiredAccess=0xd,
ObjectAttributes=0x58:"KERNELBASE.dll") => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fdf60 [0x00000184c7fe6000],
ZeroBits=0, pSize=0x5b9e9fe008 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
Loaded DLL at 00007FFBB8500000 C:\WINDOWS\System32\KERNELBASE.dll
NtMapViewOfSection(SectionHandle=0x68, ProcessHandle=-1, BaseAddress=0x184c7fe5df0
[0x00007ffbb8500000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x184c7fe5d48
[0x003b9000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5b9e9fe6b0 [2.57577e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fe640 [0x00007ffbb8887000],
Size=0x5b9e9fe638 [0x1000], NewProtect=2, OldProtect=0x5b9e9fe630 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fe6c0 [0x00007ffbbb3cb000],
Size=0x5b9e9fe6b8 [0x4000], NewProtect=4, OldProtect=0x5b9e9fe6b0 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fe6c0 [0x00007ffbbb3cb000],
Size=0x5b9e9fe6b8 [0x4000], NewProtect=2, OldProtect=0x5b9e9fe6b0 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fe700 [0x00007ffbb876f000],
Size=0x5b9e9fe708 [0x2000], NewProtect=4, OldProtect=0x184c7fe5d30 [2]) => 0
NtClose(Handle=0x68) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x184c7fe55d0 [0x00007ffbba483000],
Size=0x184c7fe55d8 [0x4000], NewProtect=2, OldProtect=0x5b9e9fec60 [4]) => 0
NtClose(Handle=0x1c) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x184c7fe5d10 [0x00007ffbb876f000],
Size=0x184c7fe5d18 [0x2000], NewProtect=2, OldProtect=0x5b9e9feda0 [4]) => 0
NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x5b9e9fed00, Length=0x28) => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtQuerySystemInformation(SystemInformationClass=0x32 [SystemRangeStartInformation],
SystemInformation=0x5b9e9feae0, Length=8, ReturnLength=null) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffbb8868ec0, Length=0x40, ReturnLength=null) => 0
NtOpenSection(SectionHandle=0x5b9e9fe8a0 [0x6c], DesiredAccess=0x4,
ObjectAttributes="\Sessions\9\Windows\SharedSection") => 0
NtCreateSection(SectionHandle=0x5b9e9fe8c0 [0x20],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f, ObjectAttributes=null,
SectionSize=0x5b9e9fe8b0 [65536], Protect=4, Attributes=0x08000000, FileHandle=0) => 0
```

```
NtConnectPort(PortHandle=0x7ffbbb3b6c08 [0x1c], PortName="\Sessions\9\Windows\ApiPort",
SecurityQos=0x5b9e9fe9e0, ClientView=0x5b9e9fe8d8, ServerView=0x5b9e9fe908,
MaxMsgLength=0x5b9e9fe8d0 [0x3b8], ConnectionInfo=0x5b9e9fe950,
ConnectionInfoLength=0x5b9e9fe8a8 [0x30]) => 0
NtClose(Handle=0x20) => 0
NtMapViewOfSection(SectionHandle=0x6c, ProcessHandle=-1, BaseAddress=0x5b9e9fe8b8
[0x00007ff434340000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9e9fe8c8
[0x00100000], InheritDisposition=2 [ViewUnmap], AllocationType=0x00500000, Protect=2) => 0
NtClose(Handle=0x6c) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x184c7dd0000, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x5b9e9fe5a0, Length=0x30, ReturnLength=null) =>
0
NtGetNlsSectionPtr(SectionType=0xe, SectionData=0, ContextData=null,
SectionPointer=0x5b9e9fea88 [0x00000184c7de0000], SectionSize=null) => 0
NtInitializeNlsFiles(BaseAddress=0x5b9e9fea80 [0x00000184c7e90000],
DefaultLocaleId=0x7ffbb886abb8 [0x419], DefaultCasingTableSize=null) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe1d0 [0x00000184c7fe7000],
ZeroBits=0, pSize=0x5b9e9fe278 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x4e3, ContextData=null,
SectionPointer=0x5b9e9fea60 [0x00000184c7f60000], SectionSize=0x5b9e9fea28 [0x00011000]) =>
0
NtGetNlsSectionPtr(SectionType=0xb, SectionData=0x362, ContextData=null,
SectionPointer=0x5b9e9fea60 [0x00000184c7f80000], SectionSize=0x5b9e9fea28 [0x00011000]) =>
0
NtCreateFile(FileHandle=0x5b9e9feae8 [0x70], DesiredAccess=READ_CONTROL|SYNCHRONIZE|0x19f,
ObjectAttributes=4:"\Connect", IoStatusBlock=0x5b9e9fe4a0 [0/0x18], AllocationSize=null,
FileAttributes=0, ShareAccess=7, CreateDisposition=2, CreateOptions=0x20,
EaBuffer=0x184c7fe7270, EaLength=0x54b) => 0
NtDeviceIoControlFile(FileHandle=0x70, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5b9e9fea30 [0/0], IoControlCode=0x00500023, InputBuffer=null,
InputBufferLength=0, OutputBuffer=0x5b9e9fea50, OutputBufferLength=8) => 0
NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x31
[ProcessOwnerInformation], ProcessInformation=0x5b9e9fea58, Length=8) => 0
NtDeviceIoControlFile(FileHandle=0x70, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5b9e9fe820, IoControlCode=0x00500016, InputBuffer=0x5b9e9fe830,
InputBufferLength=0x30, OutputBuffer=null, OutputBufferLength=0) => 0xc00700bb [187 '=x
эрщфхэю єърчрээюх шь  ёшёЄхьэюую ёхьрЇюЁр.']
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9fe938, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9fe938, OutputBufferLength=0xa0, ReturnLength=0x5b9e9fe930 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9e9fe988, InputBufferLength=0x18,
OutputBuffer=0x5b9e9fe9a0, OutputBufferLength=0x78, ReturnLength=0x5b9e9fe980 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9feb98, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9feb98, OutputBufferLength=0xa0, ReturnLength=0x5b9e9feb90 [0xa0]) => 0
NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x5b9e9fe940 [0x68]) =>
0
NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0xc [TokenSessionId],
TokenInformation=0x5b9e9fe260, Length=4, ReturnLength=0x5b9e9fe240 [4]) => 0
NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0x1d [TokenIsAppContainer],
TokenInformation=0x5b9e9fe2a8, Length=4, ReturnLength=0x5b9e9fe240 [4]) => 0
NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0x2a
[TokenPrivateNameSpace], TokenInformation=0x5b9e9fe244, Length=4, ReturnLength=0x5b9e9fe240
[4]) => 0
NtOpenDirectoryObject(DirectoryHandle=0x5b9e9fe268 [0x74], DesiredAccess=0xf,
ObjectAttributes="\Sessions\9\BaseNamedObjects") => 0
NtQueryInformationToken(TokenHandle=0x68, TokenInformationClass=0x2c [TokenBnoIsolation],
TokenInformation=0x5b9e9fe560, Length=0x120, ReturnLength=0x5b9e9fe240 [0x10]) => 0
NtClose(Handle=0x68) => 0
NtCreateMutant(MutantHandle=0x5b9e9fe998 [0x78],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x1,
ObjectAttributes=0x74:"Local\SM0:74212:304:WilStaging_02", InitialOwner=false) => 0
NtWaitForSingleObject(Handle=0x78, Alertable=false, Timeout=null) => 0
NtOpenSemaphore(SemaphoreHandle=0x5b9e9fe758,
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x74:"Local\SM0:74212:304:WilStaging_02_p0") => 0xc0000034 [2 '=x
єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtCreateSemaphore(SemaphoreHandle=0x5b9e9fe6b8 [0x7c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x74:"Local\SM0:74212:304:WilStaging_02_p0", InitialCount=0x31ff9d34,
MaxCount=0x31ff9d34) => 0
NtCreateSemaphore(SemaphoreHandle=0x5b9e9fe6b8 [0x80],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x74:"Local\SM0:74212:304:WilStaging_02_p0h", InitialCount=0xc2,
MaxCount=0xc2) => 0
NtReleaseMutant(MutantHandle=0x78, PreviousCount=null) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9feb78, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9feb78, OutputBufferLength=0xa0, ReturnLength=0x5b9e9feb70 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9e9febc8, InputBufferLength=0x18,
OutputBuffer=0x5b9e9febe0, OutputBufferLength=0x78, ReturnLength=0x5b9e9febc0 [0]) => 0
NtQueryWnfStateData(StateName=0x5b9e9fea60 [0xa3bc0875], TypeId=0x5b9e9feb08,
ExplicitScope=null, ChangeStamp=0x5b9e9fea54 [0x21], Buffer=0x5b9e9fda50,
BufferSize=0x5b9e9fea50 [8]) => 0
NtCreateEvent(EventHandle=0x5b9e9fe9d0 [0x88],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, EventType=1 [SynchronizationEvent], InitialState=false) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x184c7fe7ca0 [0x68],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtSetWnfProcessNotificationEvent(NotificationEvent=0x88) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0x68, IoCompletionHandle=0x2c,
TargetObjectHandle=0x88, KeyContext=0x184c7fe7cb8, ApcContext=0x184c7fe7b30, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5b9e9fe950 [0xc7fe0c00]) => 0
NtSubscribeWnfStateChange(StateName=0x184c7fe7e30 [0xa3bc0875], ChangeStamp=0x21,
EventMask=0x11, SubscriptionId=0x5b9e9fea40 [0x00012359]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe2d0 [0x00000184c7fe8000],
ZeroBits=0, pSize=0x5b9e9fe378 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtQuerySystemInformationEx(SystemInformationClass=0xd3
[SystemFeatureConfigurationSectionInformation], QueryType=0x5b9e9fe8c0 [0], Alignment=0x18,
SystemInformation=0x5b9e9fe8e0, Length=0x50, ReturnLength=null) => 0
NtMapViewOfSection(SectionHandle=0x8c, ProcessHandle=-1, BaseAddress=0x5b9e9fe850
[0x00000184c7fa0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9e9fe860
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0
NtMapViewOfSection(SectionHandle=0x90, ProcessHandle=-1, BaseAddress=0x5b9e9fe850
[0x00000184c7fb0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9e9fe860
[0x3000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0
NtMapViewOfSection(SectionHandle=0x94, ProcessHandle=-1, BaseAddress=0x5b9e9fe850
[0x00000184c7fc0000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x5b9e9fe860
[0x1000], InheritDisposition=2 [ViewUnmap], AllocationType=0, Protect=2) => 0
NtClose(Handle=0x8c) => 0
NtClose(Handle=0x90) => 0
NtClose(Handle=0x94) => 0
NtSetTimer2(TimerHandle=0x3c, DueTime=0x5b9e9fe9d0 [-3e+09], Period=null,
Parameters=0x5b9e9fe9d8) => 0
NtOpenKey(KeyHandle=0x5b9e9feb70, 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=0x5b9e9feb78, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9feb78, OutputBufferLength=0xa0, ReturnLength=0x5b9e9feb70 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9e9febc8, InputBufferLength=0x18,
OutputBuffer=0x5b9e9febe0, OutputBufferLength=0x78, ReturnLength=0x5b9e9febc0 [0]) => 0
NtTraceControl(CtrlCode=0xf, InputBuffer=0x5b9e9feba8, InputBufferLength=0xa0,
OutputBuffer=0x5b9e9feba8, OutputBufferLength=0xa0, ReturnLength=0x5b9e9feba0 [0xa0]) => 0
NtTraceControl(CtrlCode=0x1e, InputBuffer=0x5b9e9febf8, InputBufferLength=0x18,
OutputBuffer=0x5b9e9fec10, OutputBufferLength=0x78, ReturnLength=0x5b9e9febf0 [0]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9feac0 [0x00007ffbbb3cb000],
Size=0x5b9e9feab8 [0x4000], NewProtect=4, OldProtect=0x5b9e9feab0 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9feac0 [0x00007ffbbb3cb000],
Size=0x5b9e9feab8 [0x4000], NewProtect=2, OldProtect=0x5b9e9feab0 [4]) => 0
NtOpenKey(KeyHandle=0x5b9e9feb48 [0x90], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Terminal Server") => 0
NtQueryValueKey(KeyHandle=0x90, ValueName="TSAppCompat", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x184c7fe89e0, Length=0x224,
ResultLength=0x5b9e9feb38) => 0xc0000034 [2 '=x єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0x90, ValueName="TSUserEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x184c7fe89e0, Length=0x224,
ResultLength=0x5b9e9feb38 [0x10]) => 0
NtClose(Handle=0x90) => 0
NtQuerySystemInformation(SystemInformationClass=0 [SystemBasicInformation],
SystemInformation=0x7ffbba4b9a80, Length=0x40, ReturnLength=null) => 0
NtSetEvent(EventHandle=0x60, PrevState=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
```

```
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=4, OldProtect=0x5b9e9fec58 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9fec48 [0x00007ffbb8887000],
Size=0x5b9e9fec40 [0x1000], NewProtect=2, OldProtect=0x5b9e9fec58 [4]) => 0
NtOpenKey(KeyHandle=0x5b9e9ff210, DesiredAccess=0x3,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option") =>
0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtOpenKey(KeyHandle=0x5b9e9ff1f0 [0x90], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL") => 0
NtQueryKey(KeyHandle=0x90, KeyInformationClass=2 [KeyFullInformation],
KeyInformation=0x5b9e9ff268, Length=0x30, ResultLength=0x5b9e9ff1e0 [0x2c]) => 0
NtClose(Handle=0x90) => 0
NtOpenKey(KeyHandle=0x5b9e9ff1e8 [0x90], DesiredAccess=0x1,
ObjectAttributes="\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifier
s") => 0
NtQueryValueKey(KeyHandle=0x90, ValueName="TransparentEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2a0, Length=0x50,
ResultLength=0x5b9e9ff1e0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0x90) => 0
NtQueryInformationToken(TokenHandle=-6, TokenInformationClass=1 [TokenUser],
TokenInformation=0x5b9e9ff110, Length=0x58, ReturnLength=0x5b9e9ff108 [0x2c]) => 0
NtOpenKey(KeyHandle=0x5b9e9ff1e8, 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=0x5b9e9ff2c0 [0x90], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\FileSystem\") => 0
NtQueryValueKey(KeyHandle=0x90, ValueName="LongPathsEnabled", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff300, Length=0x14,
ResultLength=0x5b9e9ff2c8 [0x10]) => 0
NtClose(Handle=0x90) => 0
```

```
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9e9ff250 [6], Alignment=4,
SystemInformation=null, Length=0, ReturnLength=0x5b9e9ff248) => 0xc0000004 [24 '─ышэр
т√фрээющ яЁюуЁрььющ ъюьрэф√ ёыш°ъюь тхышър.']
NtQuerySystemInformationEx(SystemInformationClass=0x6b
[SystemLogicalProcessorAndGroupInformation], QueryType=0x5b9e9ff250 [6], Alignment=4,
SystemInformation=0x184c7fe5d60, Length=0x30, ReturnLength=0x5b9e9ff248 [0x30]) => 0
NtCreateIoCompletion(IoHandle=0x184c7fe5930 [0x98],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=null, NumberOfConcurrentThreads=0x11) => 0
NtCreateWorkerFactory(WorkerFactoryHandleReturn=0x184c7fe5928 [0x9c],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0xff, ObjectAttributes=null,
CompletionPortHandle=0x98, WorkerProcessHandle=-1, StartRoutine=0x7ffbbb265580,
StartParameter=0x184c7fe58f0, MaxThreadCount=0x200, StackReserve=0x00200000,
StackCommit=0x1000) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=0xd
[WorkerFactoryFlags], Buffer=0x5b9e9ff2f8, BufferLength=4) => 0
NtCreateTimer2(TimerHandle=0x184c7fe5980 [0xa0], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x2) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x184c7fe5988 [0xa4],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xa4, IoCompletionHandle=0x98,
TargetObjectHandle=0xa0, KeyContext=0x184c7fe5990, ApcContext=0x184c7fe5960, IoStatus=0,
IoStatusInformation=1, AlreadySignaled=0x5b9e9ff210 [0]) => 0
NtCreateTimer2(TimerHandle=0x184c7fe59f8 [0xa8], Unknown1=null, ObjectAttributes=null,
Attributes=8, DesiredAccess=SYNCHRONIZE|0x18400000002) => 0
NtCreateWaitCompletionPacket(WaitCompletionPacketHandle=0x184c7fe5a00 [0xac],
DesiredAccess=0x1, ObjectAttributes=null) => 0
NtAssociateWaitCompletionPacket(WaitCompletionPacketHandle=0xac, IoCompletionHandle=0x98,
TargetObjectHandle=0xa8, KeyContext=0x184c7fe5a08, ApcContext=0x184c7fe5960, IoStatus=0,
IoStatusInformation=0, AlreadySignaled=0x5b9e9ff210 [0]) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=2
[WorkerFactoryIdleTimeout], Buffer=0x5b9e9ff2f8, BufferLength=8) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=5
[WorkerFactoryThreadMaximum], Buffer=0x5b9e9ff2f8, BufferLength=4) => 0
NtOpenThreadToken(ThreadHandle=-2, DesiredAccess=READ_CONTROL|0x1c, OpenAsSelf=false,
TokenHandle=0x5b9e9ff370) => 0xc000007c [1008 '╧юя√Єър ёё√ыъш эр эхёє·хёЄтє■·шщ Єюъхэ.']
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff2f0 [0x00007ff620faf000],
Size=0x5b9e9ff2f8 [0x1000], NewProtect=4, OldProtect=0x5b9e9ff640 [8]) => 0
NtOpenSection(SectionHandle=0x5b9e9fece8 [0xb0], DesiredAccess=0xd,
ObjectAttributes=0x58:"msvcrt.dll") => 0
Loaded DLL at 00007FFBBA550000 C:\WINDOWS\System32\msvcrt.dll
NtMapViewOfSection(SectionHandle=0xb0, ProcessHandle=-1, BaseAddress=0x184c7fe8a10
[0x00007ffbba550000], ZeroBits=0, CommitSize=0, SectionOffset=null, ViewSize=0x184c7fe5ba8
[0x000a7000], InheritDisposition=1 [ViewShare], AllocationType=0x00800000, Protect=0x80) =>
0
NtQueryPerformanceCounter(Counter=0x5b9e9feb40 [2.57577e+12], Freq=null) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9feb50 [0x00007ffbbb3cb000],
Size=0x5b9e9feb48 [0x4000], NewProtect=4, OldProtect=0x5b9e9feb40 [2]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9feb50 [0x00007ffbbb3cb000],
Size=0x5b9e9feb48 [0x4000], NewProtect=2, OldProtect=0x5b9e9feb40 [4]) => 0
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=2, Buffer=0x5b9e9fe600, Length=0x330, ReturnLength=0x5b9e9fe5b8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
NtQuerySecurityAttributesToken(TokenHandle=-4, Attributes="WIN://SYSAPPID",
NumberOfAttributes=1, Buffer=0x5b9e9fe600, Length=0x330, ReturnLength=0x5b9e9fe5b8) =>
0xc0000225 [1168 '▌ыхьхэЄ эх эрщфхэ.']
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbba550000, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x5b9e9fe878, Length=0x30, ReturnLength=null)
=> 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9feb90 [0x00007ffbba5ce000],
Size=0x5b9e9feb98 [0x1000], NewProtect=4, OldProtect=0x184c7fe5b90 [2]) => 0
NtClose(Handle=0xb0) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x5b9e9ff620 [0x00007ff620faf000],
Size=0x5b9e9ff628 [0x1000], NewProtect=8, OldProtect=0x5b9e9ff0f0 [4]) => 0
NtProtectVirtualMemory(ProcessHandle=-1, BaseAddress=0x184c7fe5b70 [0x00007ffbba5ce000],
Size=0x184c7fe5b78 [0x1000], NewProtect=2, OldProtect=0x5b9e9ff0f0 [4]) => 0
NtSetInformationProcess(ProcessHandle=-1, ProcessInformationClass=0x23
[ProcessTlsInformation], ProcessInformation=0x5b9e9ff050, Length=0x28) => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
NtApphelpCacheControl(ServiceClass=6, ServiceData="") => 0
```

```
NtQueryInformationThread(ThreadHandle=-2, ThreadInformationClass=0x11
[ThreadHideFromDebugger], ThreadInformation=0x5b9e9ff370, Length=1, ReturnLength=null) => 0
Initial breakpoint
NtSetEvent(EventHandle=0x60, PrevState=null) => 0
NtOpenProcessToken(ProcessHandle=-1, DesiredAccess=0x8, TokenHandle=0x5b9e9ff2e0 [0xb4]) =>
0
NtQueryInformationToken(TokenHandle=0xb4, TokenInformationClass=0xa [TokenStatistics],
TokenInformation=0x5b9e9ff2f0, Length=0x38, ReturnLength=0x5b9e9ff2e8 [0x38]) => 0
NtClose(Handle=0xb4) => 0
NtQueryLicenseValue(Name="TerminalServices-RemoteConnectionManager-AllowAppServerMode",
Type=0x5b9e9feeec [4], Buffer=0x5b9e9feee0, Length=4, ReturnedLength=0x5b9e9feee4 [4]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fea80 [0x00000184c80e0000],
ZeroBits=0, pSize=0x5b9e9fea88 [0x00160000], flAllocationType=0x2000, flProtect=4) => 0
NtFreeVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fea80 [0x00000184c80e0000],
pSize=0x5b9e9fea78 [0x00150000], flFreeType=0x8000) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fea68 [0x00000184c8230000],
ZeroBits=0, pSize=0x5b9e9fea60 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe6f0 [0x00000184c7fe9000],
ZeroBits=0, pSize=0x5b9e9fe798 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtQueryVolumeInformationFile(FileHandle=8, IoStatusBlock=0x5b9e9ff030 [0/8],
FsInformation=0x5b9e9ff050, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtQueryVolumeInformationFile(FileHandle=0xc, IoStatusBlock=0x5b9e9ff030 [0/8],
FsInformation=0x5b9e9ff050, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtQueryVolumeInformationFile(FileHandle=0x10, IoStatusBlock=0x5b9e9ff030 [0/8],
FsInformation=0x5b9e9ff050, Length=8, FsInformationClass=4 [FsDeviceInformation]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe890 [0x00000184c7fea000],
ZeroBits=0, pSize=0x5b9e9fe938 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe840 [0x00000184c8232000],
ZeroBits=0, pSize=0x5b9e9fe8e8 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtOpenKey(KeyHandle=0x5b9e9fdd70 [0xb4], DesiredAccess=KEY_READ,
ObjectAttributes="\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions")
=> 0
NtQueryValueKey(KeyHandle=0xb4, ValueName="", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x5b9e9fe240, Length=0x214,
ResultLength=0x5b9e9fe1f8 [0x2a]) => 0
NtQueryValueKey(KeyHandle=0xb4, ValueName="000604xx", KeyValueInformationClass=1
[KeyValueFullInformation], KeyValueInformation=0x5b9e9fe220, Length=0x214,
ResultLength=0x5b9e9fdfd8 [0x42]) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe860 [0x00000184c8233000],
ZeroBits=0, pSize=0x5b9e9fe908 [0x1000], flAllocationType=0x1000, flProtect=4) => 0
NtAllocateVirtualMemory(ProcessHandle=-1, lpAddress=0x5b9e9fe840 [0x00000184c8234000],
ZeroBits=0, pSize=0x5b9e9fe8e8 [0x2000], flAllocationType=0x1000, flProtect=4) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ffbba5ded28, MemoryInformationClass=6
[MemoryImageInformation], MemoryInformation=0x5b9e9fee60, Length=0x18, ReturnLength=null) =>
0
NtSetEvent(EventHandle=0x60, PrevState=null) => 0
NtOpenKey(KeyHandle=0x5b9e9ff370 [0xb0], DesiredAccess=0x1,
ObjectAttributes="\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager") => 0
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelaySleepLoopWindowSize",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2d0,
Length=0x50, ResultLength=0x5b9e9ff2c0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelaySpinCountThreshold",
KeyValueInformationClass=2 [KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2d0,
Length=0x50, ResultLength=0x5b9e9ff2c0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelayBaseYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2d0, Length=0x50,
ResultLength=0x5b9e9ff2c0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtFactorYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2d0, Length=0x50,
ResultLength=0x5b9e9ff2c0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtQueryValueKey(KeyHandle=0xb0, ValueName="SmtDelayMaxYield", KeyValueInformationClass=2
[KeyValuePartialInformation], KeyValueInformation=0x5b9e9ff2d0, Length=0x50,
ResultLength=0x5b9e9ff2c0) => 0xc0000034 [2 '=х єфрхЄё  эрщЄш єърчрээ√щ Їрщы.']
NtClose(Handle=0xb0) => 0
NtSetInformationWorkerFactory(WorkerFactoryHandle=0x9c, InformationClass=3
[WorkerFactoryBindingCount], Buffer=0x5b9e9ff648, BufferLength=4) => 0
NtSetEvent(EventHandle=0x18, PrevState=null) => 0
NtTestAlert() => 0
```

```
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff620fa27e0, MemoryInformationClass=0
[MemoryBasicInformation], MemoryInformation=0x5b9e9ffb90, Length=0x30,
ReturnLength=0x5b9e9ffb40 [0x30]) => 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff620fa27e0, MemoryInformationClass=3
[MemoryRegionInformation], MemoryInformation=0x5b9e9ffbc0, Length=0x30, ReturnLength=null)
=> 0
NtQueryVirtualMemory(ProcessHandle=-1, BaseAddress=0x7ff620fa27e0, MemoryInformationClass=2
[MemoryMappedFilenameInformation], MemoryInformation=0x5b9e9ffc38, Length=0x21a,
ReturnLength=null) => 0
NtOpenSection(SectionHandle=0x5b9e9fe588 [0xb8],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|0x1f,
ObjectAttributes=0x74:"SharedMemory") => 0
NtOpenSemaphore(SemaphoreHandle=0x5b9e9fe588 [0xb0],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x74:"SemaphoreParent") => 0
NtOpenSemaphore(SemaphoreHandle=0x5b9e9fe588 [0xbc],
DesiredAccess=DELETE|READ_CONTROL|WRITE_DAC|WRITE_OWNER|SYNCHRONIZE|0x3,
ObjectAttributes=0x74:"SemaphoreChild") => 0
NtMapViewOfSection(SectionHandle=0xb8, ProcessHandle=-1, BaseAddress=0x5b9e9fe538
[0x00000184c7fd0000], ZeroBits=0, CommitSize=0, SectionOffset=0x5b9e9fe530 [0],
ViewSize=0x5b9e9fe540 [0x1000], InheritDisposition=1 [ViewShare], AllocationType=0,
Protect=4) => 0
NtReadFile(FileHandle=0x54, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5c5b7fea70 [0/0xa], Buffer=0x5c5b7fef70, Length=0x400, ByteOffset=null,
Key=null) => 0
NtWaitForSingleObject(Handle=0xb8, Alertable=false, Timeout=null) => 0
NtReleaseSemaphore(SemaphoreHandle=0xbc, Count=1, PreviousCount=null) => 0
NtWaitForSingleObject(Handle=0xbc, Alertable=false, Timeout=null) => 0
NtCreateFile(FileHandle=0x5b9e9fe430 [0xc0], DesiredAccess=SYNCHRONIZE|GENERIC_WRITE|0x80,
ObjectAttributes=0x64:"whore", IoStatusBlock=0x5b9e9fe438 [0/2], AllocationSize=null,
FileAttributes=0x80, ShareAccess=0, CreateDisposition=5, CreateOptions=0x00020060,
EaBuffer=null, EaLength=0) => 0
NtWriteFile(FileHandle=0xc0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5b9e9fe590 [0/2], Buffer=0x5b9e9fe600, Length=2, ByteOffset=null, Key=null)
=> 0
NtWriteFile(FileHandle=0xc0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5b9e9fe590 [0/2], Buffer=0x5b9e9fe600, Length=2, ByteOffset=null, Key=null)
=> 0
NtWriteFile(FileHandle=0xc0, Event=0, ApcRoutine=null, ApcContext=null,
IoStatusBlock=0x5b9e9fe590 [0/2], Buffer=0x5b9e9fe600, Length=2, ByteOffset=null, Key=null)
=> 0
NtReleaseSemaphore(SemaphoreHandle=0xb0, Count=1, PreviousCount=null) => 0
NtWaitForSingleObject(Handle=0xb8, Alertable=false, Timeout=null) => 0
NtUnmapViewOfSectionEx(ProcessHandle=-1, BaseAddress=0x184c7fd0000, Flags=0) => 0
NtUnmapViewOfSectionEx(ProcessHandle=-1, BaseAddress=0x1714def0000, Flags=0) => 0
NtClose(Handle=0xb8) => 0
NtClose(Handle=0xb0) => 0
NtClose(Handle=0xb0) => 0
NtClose(Handle=0xb8) => 0
NtClose(Handle=0xbc) => 0
NtClose(Handle=0xbc) => 0
NtClose(Handle=0xec) => 0
NtClose(Handle=0xc0) => 0
NtClose(Handle=0xe8) => 0
NtTerminateProcess(ProcessHandle=0, ExitStatus=0) => 0
NtTerminateProcess(ProcessHandle=0, ExitStatus=0) => 0
NtClose(Handle=0x6c) => 0
NtClose(Handle=0xe4) => 0
NtClose(Handle=0x8c) => 0
NtClose(Handle=0xdc) => 0
NtClose(Handle=0x94) => 0
NtClose(Handle=0xe0) => 0
NtQueryWnfStateData(StateName=0x5b9e9ff920 [0xa3bc1c75], TypeId=null, ExplicitScope=null,
ChangeStamp=0x5b9e9fe86c [0x0001cd06], Buffer=0x5b9e9fe8c0, BufferSize=0x5b9e9fe868 [0x678])
=> 0
NtClose(Handle=0xc8) => 0
NtClose(Handle=0x84) => 0
NtClose(Handle=0xcc) => 0
NtClose(Handle=0x20) => 0
NtClose(Handle=0x6c) => 0
```

```
Process 74212 exit code: 0
NtClose(Handle=0x98) => 0
NtClose(Handle=0x9c) => 0
NtQueryWnfStateData(StateName=0x5c5b7ff250 [0xa3bc1c75], TypeId=null, ExplicitScope=null, ChangeStamp=0x5c5b7fe19c [0x0001cd06], Buffer=0x5c5b7fe1f0, BufferSize=0x5c5b7fe198 [0x678]) => 0
NtClose(Handle=0x84) => 0
NtClose(Handle=0x74) => 0
Process 67588 exit code: 0
```

Вывод

Просто переделал первое задание с file mapping. Все супер.