20.12.2023

Курс:

Практическая работа к уроку № Lesson_3

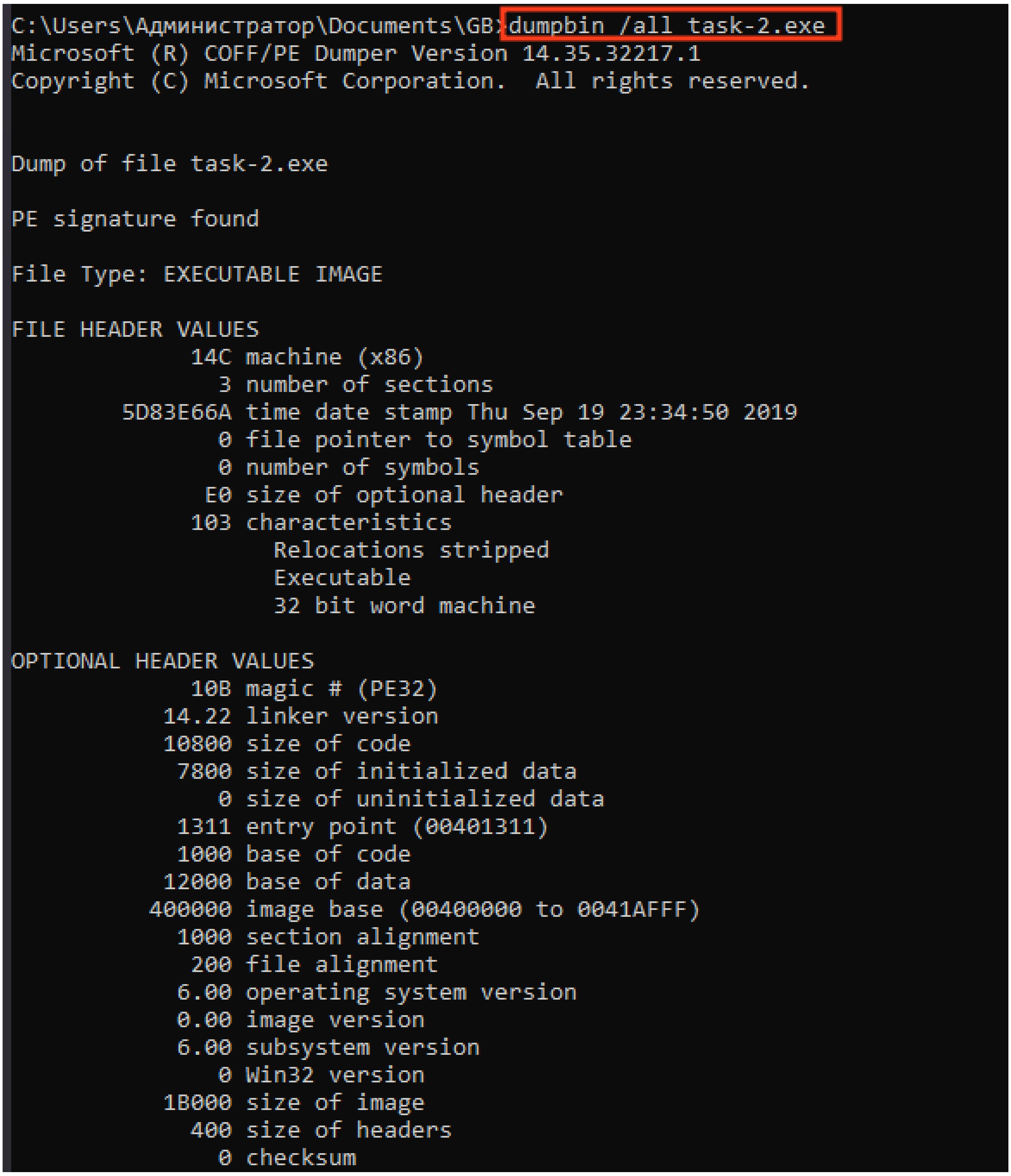
--
Анализ PE-файлов

Задание:

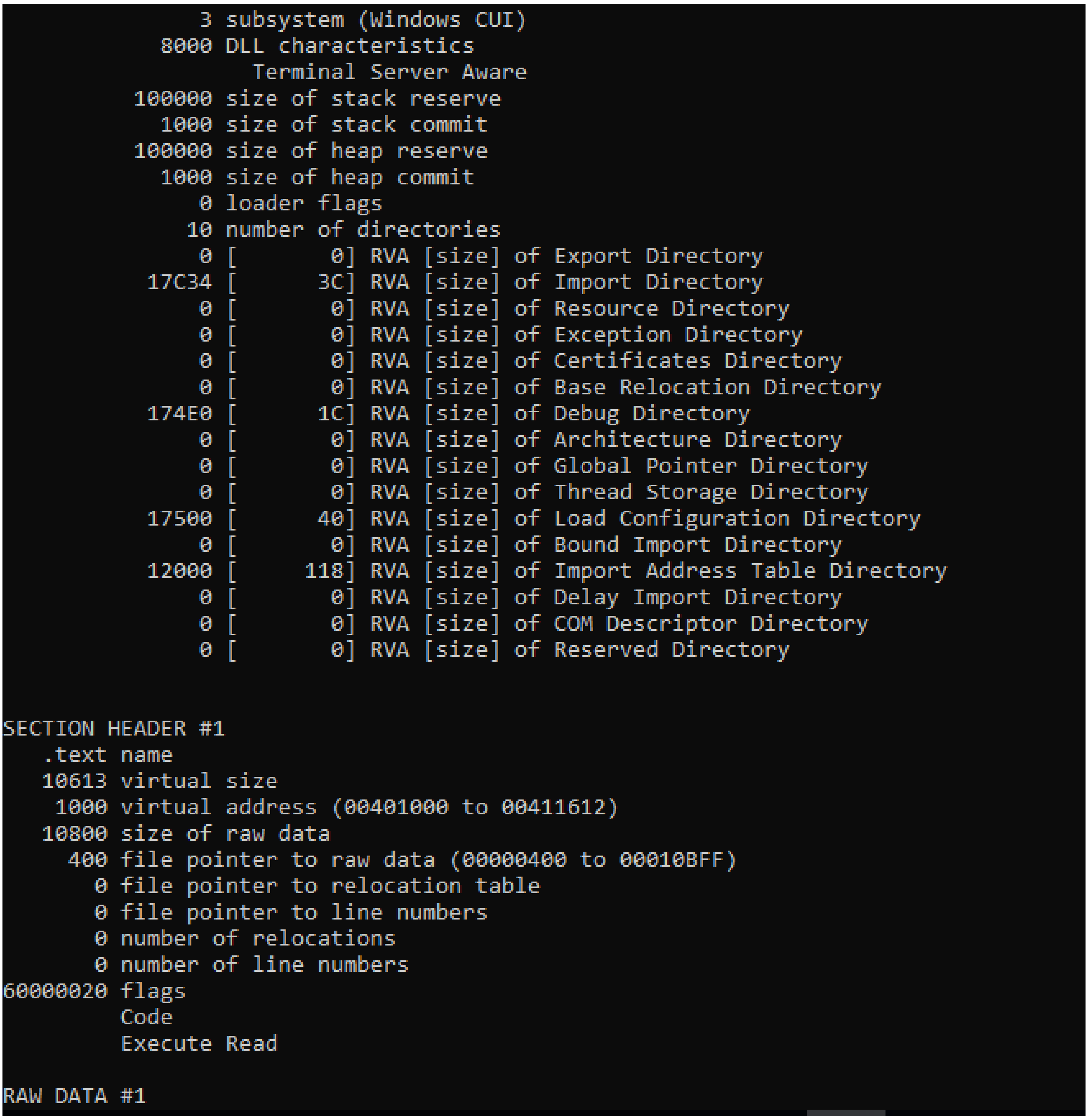
Предоставлен файл *task-2.exe*
Необходимо получить о нем следующую информацию:

1. Тип файла:
   .exe
   Executable image
2. Архитектура:
   intel 386 (x86)
3. Количество секций в файле (number of sections):
   3
4. RVA для секции кода (base of code):
   1000
5. RVA для секции данных (base of data):
   12000
6. Базовый адрес (image bese):
   400000
7. RVA точки входа (address of entry point):
   1311
8. Планируемый адрес точки входа (address of entry point (...)):
   00401311
9. Импортируемые библиотеки (Directory Entry Import):
   USER32.DLL
   KERNEL32.DLL
10. Импортируемые функции (name):
    USER32.DLL
    MessageBoxA
    KERNEL32.DLL
    HeapAlloc, ..., CloseHandle

```
task-2.exe
```

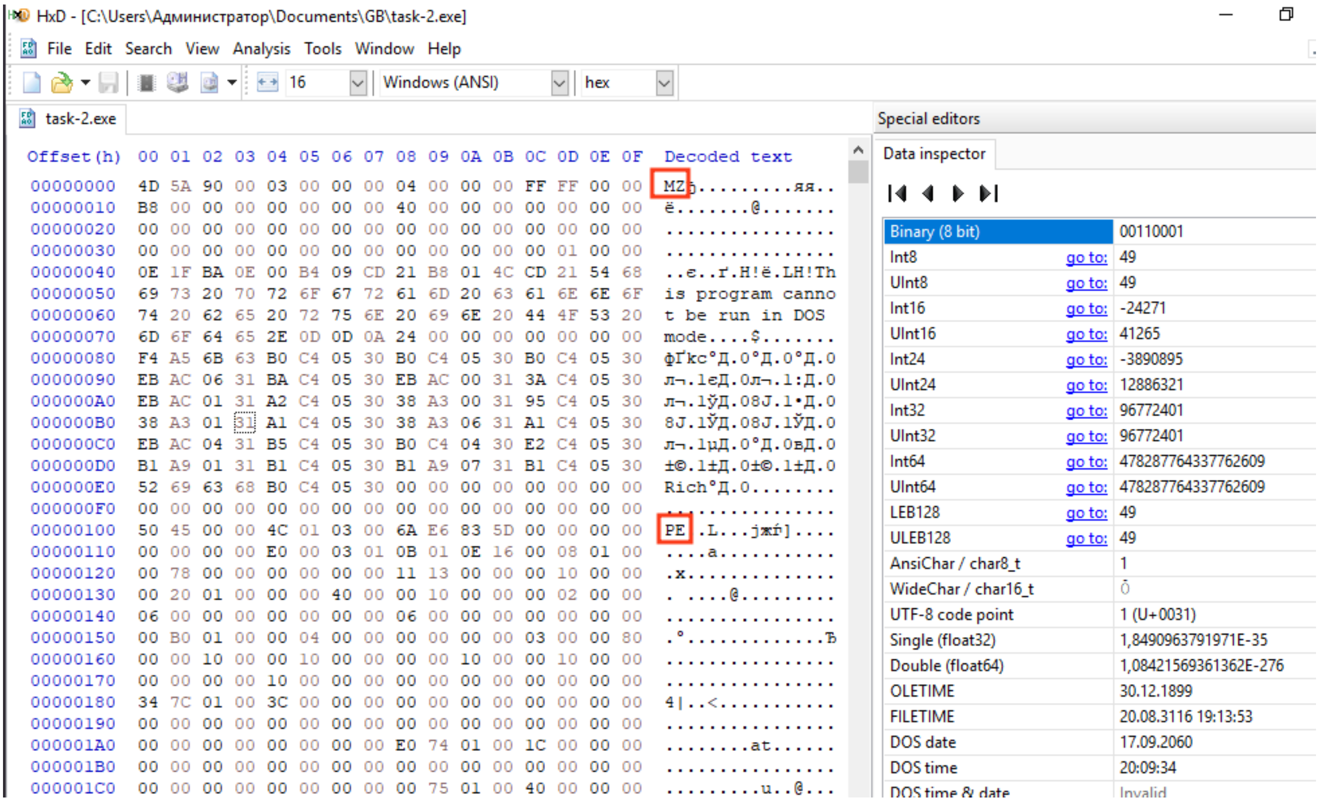


```
C:\Users\Администратор\Documents\GB>dumpbin /all task-2.exe
Microsoft (R) COFF/PE Dumper Version 14.35.32217.1
Copyright (C) Microsoft Corporation.  All rights reserved.


Dump of file task-2.exe

PE signature found

File Type: EXECUTABLE IMAGE

FILE HEADER VALUES
             14C machine (x86)
               3 number of sections
        5D83E66A time date stamp Thu Sep 19 23:34:50 2019
               0 file pointer to symbol table
               0 number of symbols
              E0 size of optional header
             103 characteristics
                   Relocations stripped
                   Executable
                   32 bit word machine

OPTIONAL HEADER VALUES
             10B magic # (PE32)
           14.22 linker version
           10800 size of code
            7800 size of initialized data
               0 size of uninitialized data
            1311 entry point (00401311)
            1000 base of code
           12000 base of data
          400000 image base (00400000 to 0041AFFF)
            1000 section alignment
             200 file alignment
            6.00 operating system version
            0.00 image version
            6.00 subsystem version
               0 Win32 version
           1B000 size of image
             400 size of headers
               0 checksum
```



```
               3 subsystem (Windows CUI)
            8000 DLL characteristics
                   Terminal Server Aware
          100000 size of stack reserve
            1000 size of stack commit
          100000 size of heap reserve
            1000 size of heap commit
               0 loader flags
              10 number of directories
               0 [       0] RVA [size] of Export Directory
           17C34 [      3C] RVA [size] of Import Directory
               0 [       0] RVA [size] of Resource Directory
               0 [       0] RVA [size] of Exception Directory
               0 [       0] RVA [size] of Certificates Directory
               0 [       0] RVA [size] of Base Relocation Directory
           174E0 [      1C] RVA [size] of Debug Directory
               0 [       0] RVA [size] of Architecture Directory
               0 [       0] RVA [size] of Global Pointer Directory
               0 [       0] RVA [size] of Thread Storage Directory
           17500 [      40] RVA [size] of Load Configuration Directory
               0 [       0] RVA [size] of Bound Import Directory
           12000 [     118] RVA [size] of Import Address Table Directory
               0 [       0] RVA [size] of Delay Import Directory
               0 [       0] RVA [size] of COM Descriptor Directory
               0 [       0] RVA [size] of Reserved Directory


SECTION HEADER #1
   .text name
   10613 virtual size
    1000 virtual address (00401000 to 00411612)
   10800 size of raw data
     400 file pointer to raw data (00000400 to 00010BFF)
       0 file pointer to relocation table
       0 file pointer to line numbers
       0 number of relocations
       0 number of line numbers
60000020 flags
         Code
         Execute Read

RAW DATA #1
```

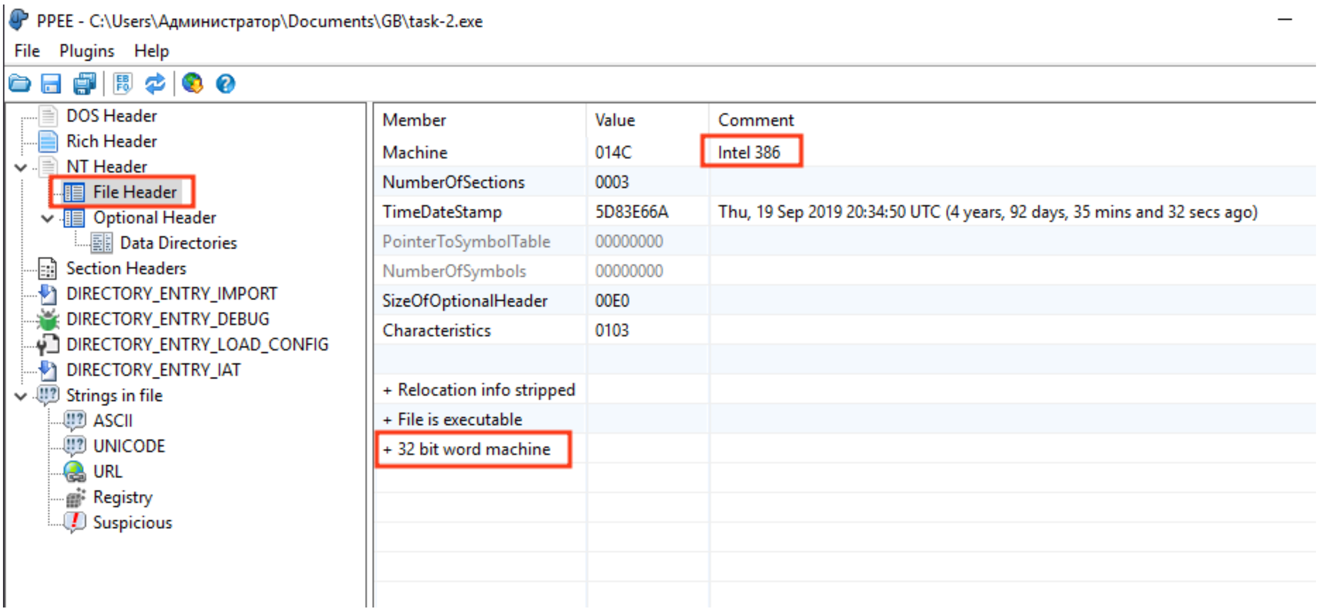
PE файл. Считываем из HxD или дампа (MZ + PE)


HxD - [C:\Users\Администратор\Documents\GB\task-2.exe]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
task-2.exe
Special editors
Data inspector

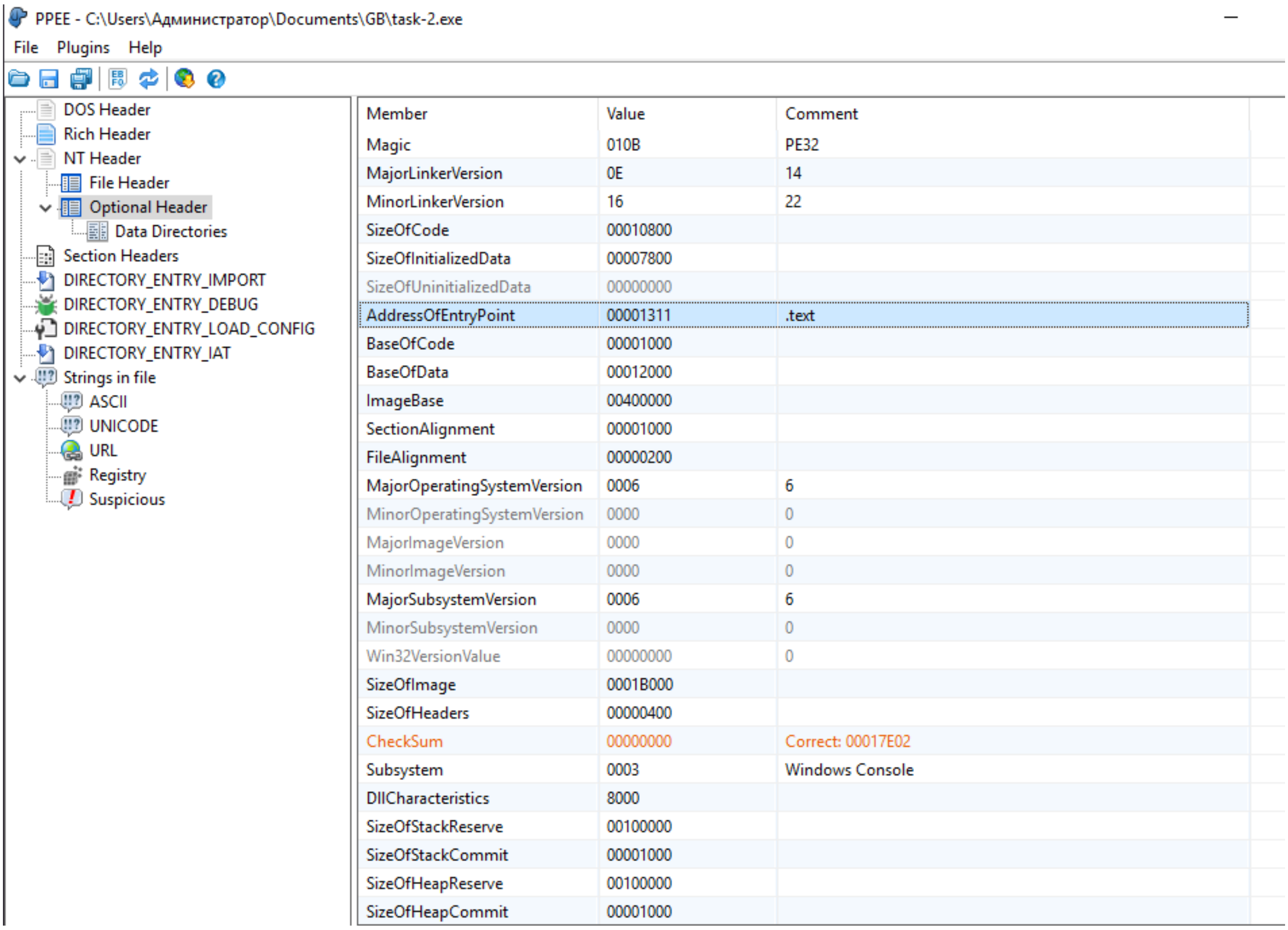
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZђ.........яя..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ё.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  ................
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..є..ґ.Н!ё.LН!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  F4 A5 6B 63 B0 C4 05 30 B0 C4 05 30 B0 C4 05 30  фҐkc°Д.0°Д.0°Д.0
00000090  EB AC 06 31 BA C4 05 30 EB AC 00 31 3A C4 05 30  л¬.1єД.0л¬.1:Д.0
000000A0  EB AC 01 31 A2 C4 05 30 38 A3 00 31 95 C4 05 30  л¬.1ўД.08Ј.1•Д.0
000000B0  38 A3 01 31 A1 C4 05 30 38 A3 06 31 A1 C4 05 30  8Ј.1ЎД.08Ј.1ЎД.0
000000C0  EB AC 04 31 B5 C4 05 30 B0 C4 04 30 E2 C4 05 30  л¬.1µД.0°Д.0вД.0
000000D0  B1 A9 01 31 B1 C4 05 30 B1 A9 07 31 B1 C4 05 30  ±©.1±Д.0±©.1±Д.0
000000E0  52 69 63 68 B0 C4 05 30 00 00 00 00 00 00 00 00  Rich°Д.0........
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  50 45 00 00 4C 01 03 00 6A E6 83 5D 00 00 00 00  PE..L...jжѓ]....
00000110  00 00 00 00 E0 00 03 01 0B 01 0E 16 00 08 01 00  ....a...........
00000120  00 78 00 00 00 00 00 00 11 13 00 00 00 10 00 00  .x..............
00000130  00 20 01 00 00 00 40 00 00 10 00 00 00 02 00 00  . ....@.........
00000140  06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00  ................
00000150  00 B0 01 00 00 04 00 00 00 00 00 00 03 00 00 80  .°.............Ђ
00000160  00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
00000170  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  34 7C 01 00 3C 00 00 00 00 00 00 00 00 00 00 00  4|..<...........
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 E0 74 01 00 1C 00 00 00  ........at......
000001B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001C0  00 00 00 00 00 00 00 00 00 75 01 00 40 00 00 00  .........u..@...
```

Binary (8 bit)		00110001
Int8	go to:	49
UInt8	go to:	49
Int16	go to:	-24271
UInt16	go to:	41265
Int24	go to:	-3890895
UInt24	go to:	12886321
Int32	go to:	96772401
UInt32	go to:	96772401
Int64	go to:	478287764337762609
UInt64	go to:	478287764337762609
LEB128	go to:	49
ULEB128	go to:	49
AnsiChar / char8_t		1
WideChar / char16_t		옱
UTF-8 code point		1 (U+0031)
Single (float32)		1,8490963791971E-35
Double (float64)		1,08421569361362E-276
OLETIME		30.12.1899
FILETIME		20.08.3116 19:13:53
DOS date		17.09.2060
DOS time		20:09:34
DOS time & date		Invalid

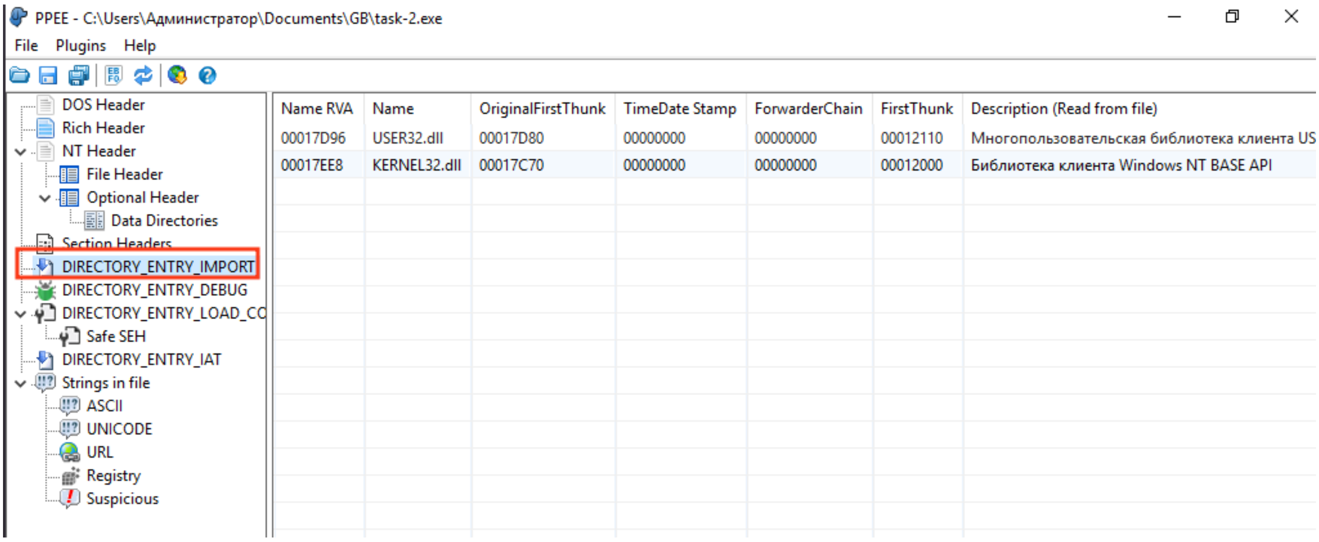
Открываем в PPEE



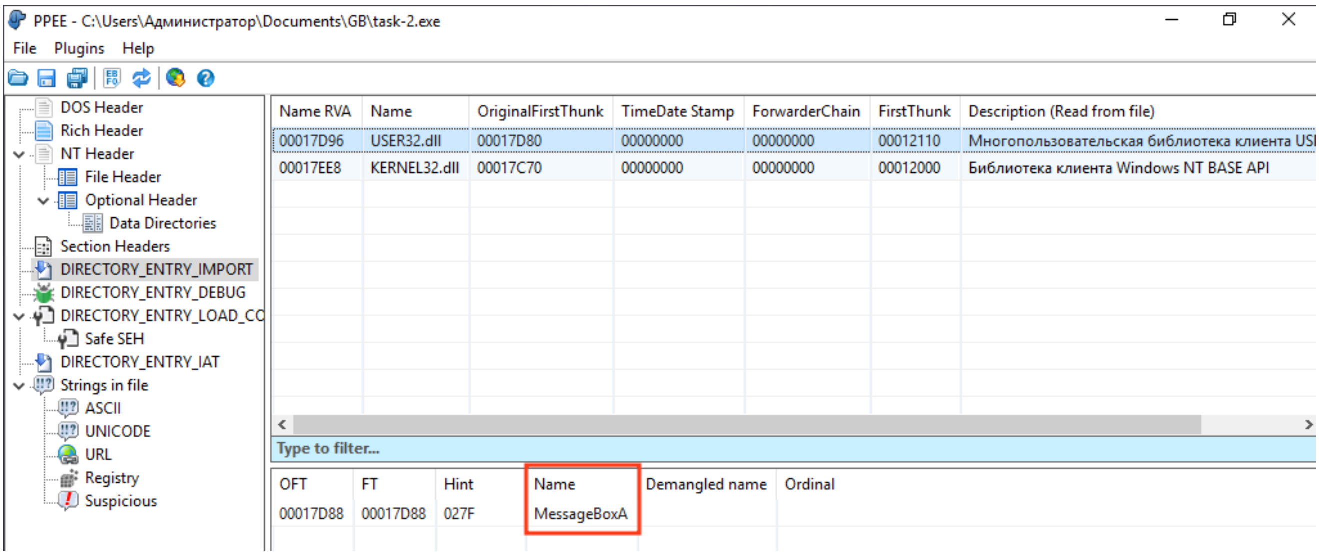
Member	Value	Comment
Machine	014C	Intel 386
NumberOfSections	0003	
TimeDateStamp	5D83E66A	Thu, 19 Sep 2019 20:34:50 UTC (4 years, 92 days, 35 mins and 32 secs ago)
PointerToSymbolTable	00000000	
NumberOfSymbols	00000000	
SizeOfOptionalHeader	00E0	
Characteristics	0103	
+ Relocation info stripped		
+ File is executable		
+ 32 bit word machine		



Member	Value	Comment
Magic	010B	PE32
MajorLinkerVersion	0E	14
MinorLinkerVersion	16	22
SizeOfCode	00010800	
SizeOfInitializedData	00007800	
SizeOfUninitializedData	00000000	
AddressOfEntryPoint	00001311	.text
BaseOfCode	00001000	
BaseOfData	00012000	
ImageBase	00400000	
SectionAlignment	00001000	
FileAlignment	00000200	
MajorOperatingSystemVersion	0006	6
MinorOperatingSystemVersion	0000	0
MajorImageVersion	0000	0
MinorImageVersion	0000	0
MajorSubsystemVersion	0006	6
MinorSubsystemVersion	0000	0
Win32VersionValue	00000000	0
SizeOfImage	0001B000	
SizeOfHeaders	00000400	
CheckSum	00000000	Correct: 00017E02
Subsystem	0003	Windows Console
DllCharacteristics	8000	
SizeOfStackReserve	00100000	
SizeOfStackCommit	00001000	
SizeOfHeapReserve	00100000	
SizeOfHeapCommit	00001000	

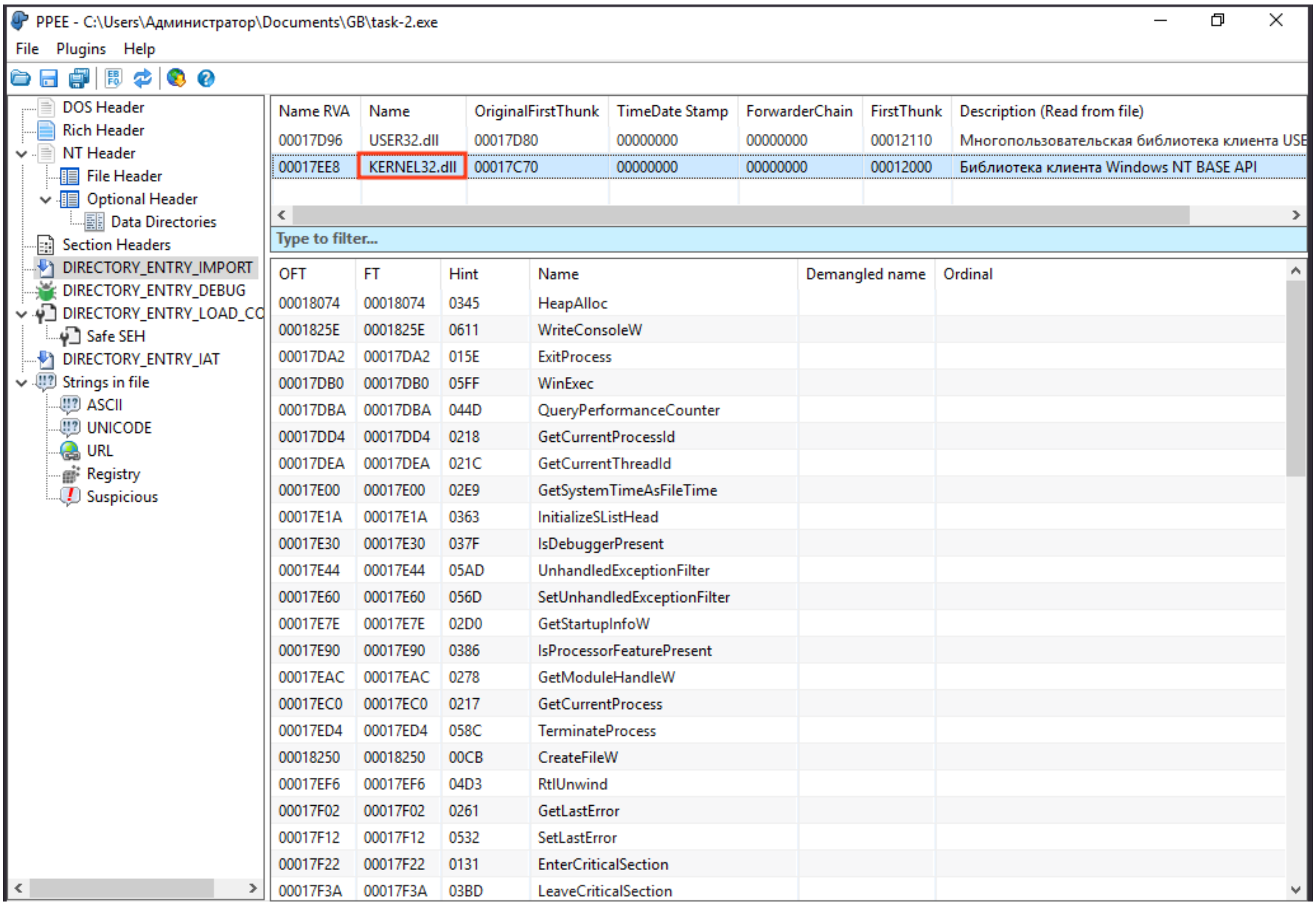


Name RVA	Name	OriginalFirstThunk	TimeDate Stamp	ForwarderChain	FirstThunk	Description (Read from file)
00017D96	USER32.dll	00017D80	00000000	00000000	00012110	Многопользовательская библиотека клиента US
00017EE8	KERNEL32.dll	00017C70	00000000	00000000	00012000	Библиотека клиента Windows NT BASE API



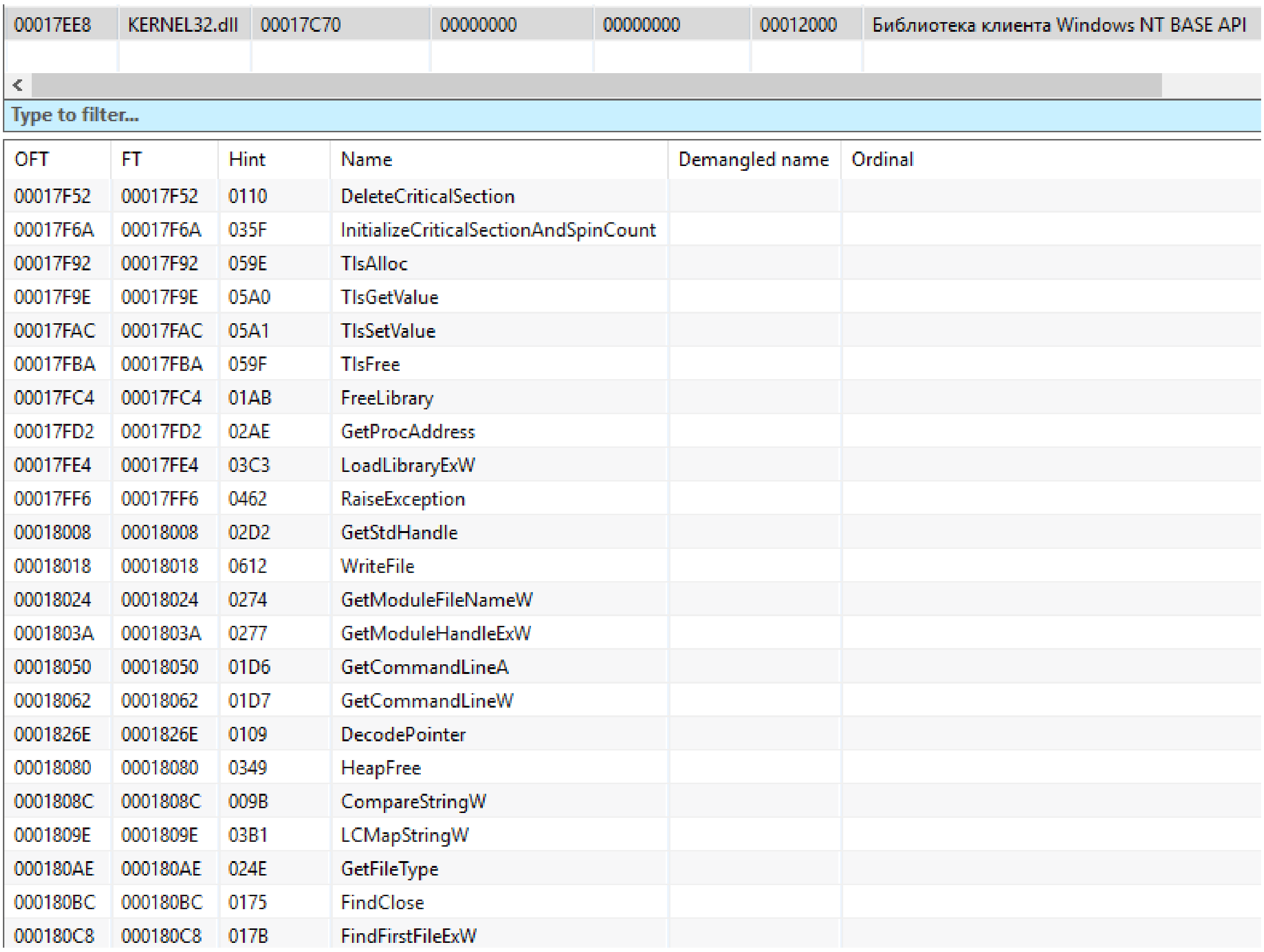
Name RVA	Name	OriginalFirstThunk	TimeDate Stamp	ForwarderChain	FirstThunk	Description (Read from file)
00017D96	USER32.dll	00017D80	00000000	00000000	00012110	Многопользовательская библиотека клиента USI
00017EE8	KERNEL32.dll	00017C70	00000000	00000000	00012000	Библиотека клиента Windows NT BASE API

OFT	FT	Hint	Name	Demangled name	Ordinal
00017D88	00017D88	027F	MessageBoxA		



Name RVA	Name	OriginalFirstThunk	TimeDate Stamp	ForwarderChain	FirstThunk	Description (Read from file)
00017D96	USER32.dll	00017D80	00000000	00000000	00012110	Многопользовательская библиотека клиента USE
00017EE8	KERNEL32.dll	00017C70	00000000	00000000	00012000	Библиотека клиента Windows NT BASE API

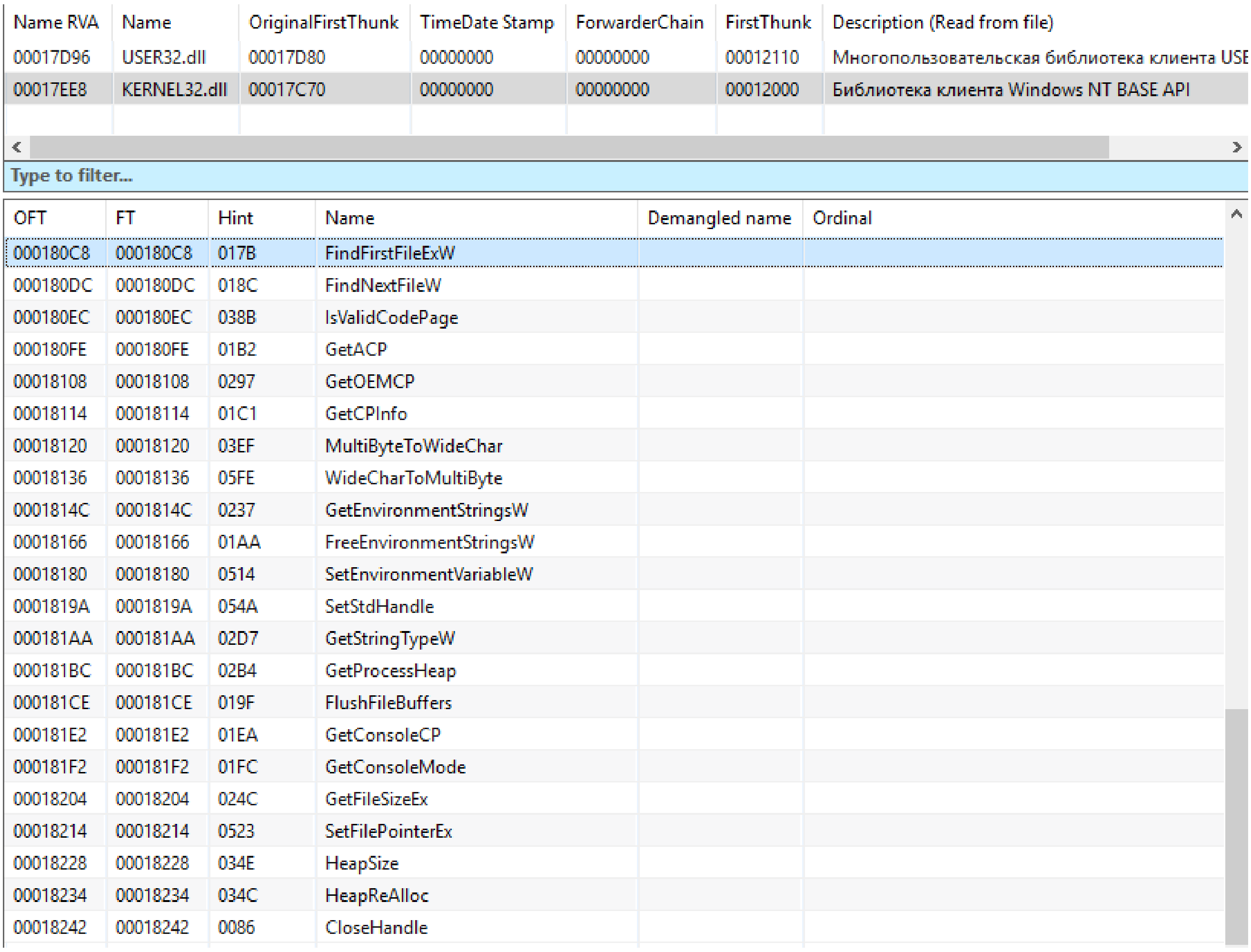
OFT	FT	Hint	Name	Demangled name	Ordinal
00018074	00018074	0345	HeapAlloc		
0001825E	0001825E	0611	WriteConsoleW		
00017DA2	00017DA2	015E	ExitProcess		
00017DB0	00017DB0	05FF	WinExec		
00017DBA	00017DBA	044D	QueryPerformanceCounter		
00017DD4	00017DD4	0218	GetCurrentProcessId		
00017DEA	00017DEA	021C	GetCurrentThreadId		
00017E00	00017E00	02E9	GetSystemTimeAsFileTime		
00017E1A	00017E1A	0363	InitializeSListHead		
00017E30	00017E30	037F	IsDebuggerPresent		
00017E44	00017E44	05AD	UnhandledExceptionFilter		
00017E60	00017E60	056D	SetUnhandledExceptionFilter		
00017E7E	00017E7E	02D0	GetStartupInfoW		
00017E90	00017E90	0386	IsProcessorFeaturePresent		
00017EAC	00017EAC	0278	GetModuleHandleW		
00017EC0	00017EC0	0217	GetCurrentProcess		
00017ED4	00017ED4	058C	TerminateProcess		
00018250	00018250	00CB	CreateFileW		
00017EF6	00017EF6	04D3	RtlUnwind		
00017F02	00017F02	0261	GetLastError		
00017F12	00017F12	0532	SetLastError		
00017F22	00017F22	0131	EnterCriticalSection		
00017F3A	00017F3A	03BD	LeaveCriticalSection		



00017EE8	KERNEL32.dll	00017C70	00000000	00000000	00012000	Библиотека клиента Windows NT BASE API

Type to filter...

OFT	FT	Hint	Name	Demangled name	Ordinal
00017F52	00017F52	0110	DeleteCriticalSection		
00017F6A	00017F6A	035F	InitializeCriticalSectionAndSpinCount		
00017F92	00017F92	059E	TlsAlloc		
00017F9E	00017F9E	05A0	TlsGetValue		
00017FAC	00017FAC	05A1	TlsSetValue		
00017FBA	00017FBA	059F	TlsFree		
00017FC4	00017FC4	01AB	FreeLibrary		
00017FD2	00017FD2	02AE	GetProcAddress		
00017FE4	00017FE4	03C3	LoadLibraryExW		
00017FF6	00017FF6	0462	RaiseException		
00018008	00018008	02D2	GetStdHandle		
00018018	00018018	0612	WriteFile		
00018024	00018024	0274	GetModuleFileNameW		
0001803A	0001803A	0277	GetModuleHandleExW		
00018050	00018050	01D6	GetCommandLineA		
00018062	00018062	01D7	GetCommandLineW		
0001826E	0001826E	0109	DecodePointer		
00018080	00018080	0349	HeapFree		
0001808C	0001808C	009B	CompareStringW		
0001809E	0001809E	03B1	LCMapStringW		
000180AE	000180AE	024E	GetFileType		
000180BC	000180BC	0175	FindClose		
000180C8	000180C8	017B	FindFirstFileExW		



Name RVA	Name	OriginalFirstThunk	TimeDate Stamp	ForwarderChain	FirstThunk	Description (Read from file)
00017D96	USER32.dll	00017D80	00000000	00000000	00012110	Многопользовательская библиотека клиента USE
00017EE8	KERNEL32.dll	00017C70	00000000	00000000	00012000	Библиотека клиента Windows NT BASE API

Type to filter...

OFT	FT	Hint	Name	Demangled name	Ordinal
000180C8	000180C8	017B	FindFirstFileExW		
000180DC	000180DC	018C	FindNextFileW		
000180EC	000180EC	038B	IsValidCodePage		
000180FE	000180FE	01B2	GetACP		
00018108	00018108	0297	GetOEMCP		
00018114	00018114	01C1	GetCPInfo		
00018120	00018120	03EF	MultiByteToWideChar		
00018136	00018136	05FE	WideCharToMultiByte		
0001814C	0001814C	0237	GetEnvironmentStringsW		
00018166	00018166	01AA	FreeEnvironmentStringsW		
00018180	00018180	0514	SetEnvironmentVariableW		
0001819A	0001819A	054A	SetStdHandle		
000181AA	000181AA	02D7	GetStringTypeW		
000181BC	000181BC	02B4	GetProcessHeap		
000181CE	000181CE	019F	FlushFileBuffers		
000181E2	000181E2	01EA	GetConsoleCP		
000181F2	000181F2	01FC	GetConsoleMode		
00018204	00018204	024C	GetFileSizeEx		
00018214	00018214	0523	SetFilePointerEx		
00018228	00018228	034E	HeapSize		
00018234	00018234	034C	HeapReAlloc		
00018242	00018242	0086	CloseHandle		

*Выполнил: AndreiM