**Міністерство освіти і науки України**

**Національний технічний університет України**

**«Київський політехнічний інститут імені Ігоря Сікорського»**

**Факультет інформатики та обчислювальної техніки**

**Кафедра обчислювальної техніки**

**Лабораторна робота №3**

з дисципліни

«Системне програмування»

на тему

«Дослідження структури програм формату EXE»

Виконав:

Перевірив:

студент групи ІП-93

Павлов Валерій Георгійович

Домінський Валентин Олексійович

номер залікової книжки: 9311

номер у списку: 9

Київ 2021

**Мета:**

Ознайомлення із специфікацією COFF (Common Object File Format). Вивчення прийомів

дослідження структури файлів PE-формату

**Порядок виконання роботи:**

1. Вивчити структуру програм формату EXE
2. Розробити програму на мові Асемблер, за допомогою якої у віконному інтерфейсі по введеному паролю виводяться персональні дані студента – ПІБ, дата народження, номер залікової книжки тощо

; Processors

.386

.model **flat,** **stdcall**

option **CaseMap:None**

WinMainProto proto **:dword,:dword,:dword**

; Libraries And Macroses

include \masm32\include\windows.inc

include \masm32\include\user32.inc

include \masm32\include\kernel32.inc

includelib \masm32\lib\user32.lib

includelib \masm32\lib\kernel32.lib

.data?

hInstance HINSTANCE **?** ; Handle of our program

hWndOfMainWindow HWND **?** ; Handle of our editbox

hWndOfEditbox HWND **?** ; Handle of our editbox

StringFromUser DB 128 dup**(?)**

; Data Segment

.data

StartingText DB "Введiть пароль у наступому вікні, щоб отримати дані"**,** 0

FailureText DB "Пароль невiрний. Спробуйте ще раз"**,** 0

; Name Of Message Box

MsgBoxName DB "3-9-IP93-Dominskyi"**,** 0

; We can write password in two ways:

Password DB "Dominskyi"

; And another one is:

; Password DB 31h 32h 33h

PasswordCount **=** **$-**Password

; Text To Show

InformationText DB "ПIБ = Домiнський Валентин Олексiйович"**,** 13**,**

"Дата Народження = 22.02.2002"**,** 13**,**

"Номер Залiковки книжки = 9311"**,** 0

NameOfTheStartingWindows DB "Window with starting text"**,** 0 ; the name of our window class

NameOfTheEditBox DB "Edit"**,** 0 ; the name of our editbox class

NameOfTheButton DB "Button"**,** 0 ; the name of our button class

TextForButton DB "Перевірити пароль"**,** 0

; Code Segment

.code

start**:** ; Generates program start-up code

invoke MessageBox**,** 0**,** offset StartingText**,** offset MsgBoxName**,** MB\_OK

invoke GetModuleHandle**,** NULL

**mov** hInstance**,** **eax**

invoke WinMainProto**,** hInstance**,**NULL**,** SW\_SHOWDEFAULT ;invoke function

invoke ExitProcess**,** **eax** ; quit program. code returns in EAX register from Main Function.

; function declaration of WinMain

WinMainProto proc hInst**:**HINSTANCE**,**hPrevInst**:**HINSTANCE**,**CmdShow**:dword**

; there we need local variables

local wc**:**WNDCLASSEX

local msg**:**MSG

local hwnd**:**HWND

; assign variables of WNDCLASSEX

; window class is a specification of a window

**mov** wc.cbSize**,** sizeof WNDCLASSEX

**mov** wc.style**,** CS\_HREDRAW **or** CS\_VREDRAW

**mov** wc.lpfnWndProc**,** offset WndProc

**mov** wc.cbClsExtra**,** NULL

**mov** wc.cbWndExtra**,** NULL

**push** hInstance

**pop** wc.hInstance

**mov** wc.hbrBackground**,** COLOR\_WINDOW**+**2

**mov** wc.lpszMenuName**,** NULL

**mov** wc.lpszClassName**,** offset NameOfTheStartingWindows

invoke LoadIcon**,** NULL**,** IDI\_APPLICATION

**mov** wc.hIcon**,** **eax**

**mov** wc.hIconSm**,** **eax**

invoke LoadCursor**,** NULL**,** IDC\_ARROW

**mov** wc.hCursor**,** **eax**

; create class of the window

invoke RegisterClassEx**,** **addr** wc

invoke CreateWindowEx**,** NULL**,**

offset NameOfTheStartingWindows**,**

offset MsgBoxName**,**

WS\_OVERLAPPEDWINDOW **or** DS\_CENTER**,**

470**,** 280**,** 300**,** 200**,**

NULL**,** NULL**,** hInst**,** NULL

**mov** hWndOfMainWindow**,** **eax**

; write window handle in eax

**mov** hwnd**,eax**

; Show window

invoke ShowWindow**,** hwnd**,**CmdShow

; update screen

invoke UpdateWindow**,** hwnd

; waits for message

.while TRUE

;returns FALSE if WM\_QUIT message is received and will kill the loop

invoke GetMessage**,** **addr** msg**,**NULL**,**0**,**0

.break .if **(**!**eax)**

;takes raw keyboard input and generates a new message

invoke TranslateMessage**,** **addr** msg

;sends the message data to the window procedure responsible for the specific window the message is for

invoke DispatchMessage**,** **addr** msg

; end while

.endw

; code returns in EAX register from Main Function.

**mov** **eax,** msg.wParam

; return

**ret**

;The ENDP directive defines the end of the procedure

;and has the same name as in the PROC directive

WinMainProto endp

WndProc proc hWnd**:**HWND**,** ourMSG**:**UINT**,** wParam**:**WPARAM**,** lParam**:**LPARAM

; on window close

.if ourMSG**==**WM\_CLOSE

; exit program

invoke PostQuitMessage**,**NULL

.elseif ourMSG**==**WM\_CREATE

invoke CreateWindowEx**,**NULL**,**

offset NameOfTheEditBox**,** NULL**,**

WS\_VISIBLE **or** WS\_CHILD **or** ES\_LEFT **or** ES\_AUTOHSCROLL **or** ES\_AUTOVSCROLL **,**

65**,**20**,**150**,** 30**,**

hWnd**,** 7000**,** hInstance**,** NULL

**mov** hWndOfEditbox**,** **eax**

invoke CreateWindowEx**,**NULL**,**

offset NameOfTheButton**,** offset TextForButton**,**

WS\_VISIBLE **or** WS\_CHILD **or** BS\_CENTER **or** BS\_TEXT **or** BS\_VCENTER**,**

60**,** 90**,** 170**,** 30**,**

hWnd**,** 7001**,** hInstance**,** NULL

.elseif ourMSG**==**WM\_COMMAND

**mov** **bx,** 03h ; counter for tries

**cmp** wParam**,** 7001

**jne** ExitCode

invoke SendMessage**,** hWndOfEditbox**,** WM\_GETTEXT**,** PasswordCount**+**2**,** offset StringFromUser

**mov** **edi,** 0

**cmp** **ax,** PasswordCount

**jne** WrongPasswordByUser

LoopItself**:**

**inc** **edi** ; incrementing

**loop** IsPasswordCorrect

IsPasswordCorrect**:**

**cmp** **edi,** PasswordCount

**je** CorrectPasswordByUser

**mov** **ah,** StringFromUser**[edi]**

**cmp** **ah,** Password**[edi]** ; Compare

**je** LoopItself ; Jump Equal

**jmp** WrongPasswordByUser ; Unconditional jump

WrongPasswordByUser**:**

; counting tries

**add** **bx,** **-**01h ; decrementing

**cmp** **bx,** **-**01h ; negative possible tries

**je** TotalExitCode

invoke MessageBox**,** hWnd**,** offset FailureText**,** offset MsgBoxName**,** MB\_OK

**jmp** ExitCode

CorrectPasswordByUser**:**

invoke MessageBox**,** hWnd**,** offset InformationText**,** offset MsgBoxName**,** MB\_OK

**jmp** ExitCode

TotalExitCode**:**

invoke DestroyWindow**,**hWndOfMainWindow

.else

; process the message

invoke DefWindowProc**,**hWnd**,**ourMSG**,**wParam**,**lParam

**ret**

.ENDIF

ExitCode**:**

**xor** **eax,eax**

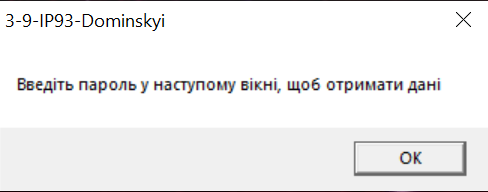
**ret**

WndProc endp

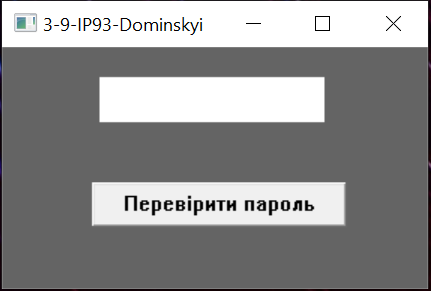
end start

1. Виконати компіляцію розробленого файлу у формат EXE
2. Перевірити роботу програми шляхом введення як правильного, так і невірного паролів:

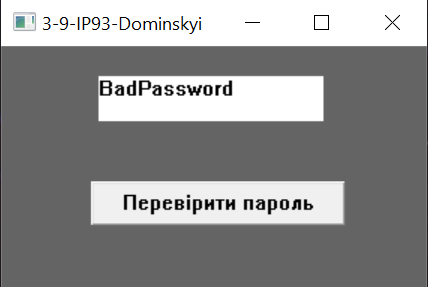
Початкове вікно:



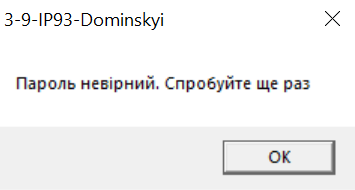
Вікно введення паролю:



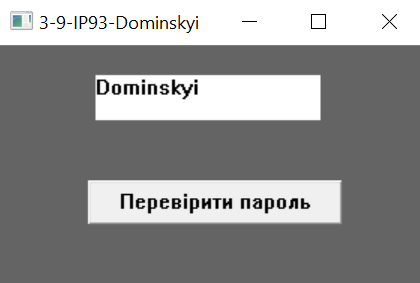
Введення неправильного паролю:



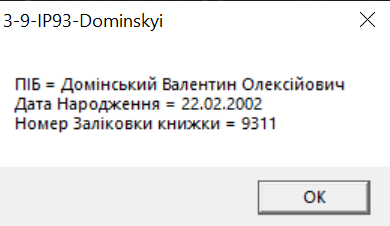
Вивід при такому паролі:



Введення правильно паролю:

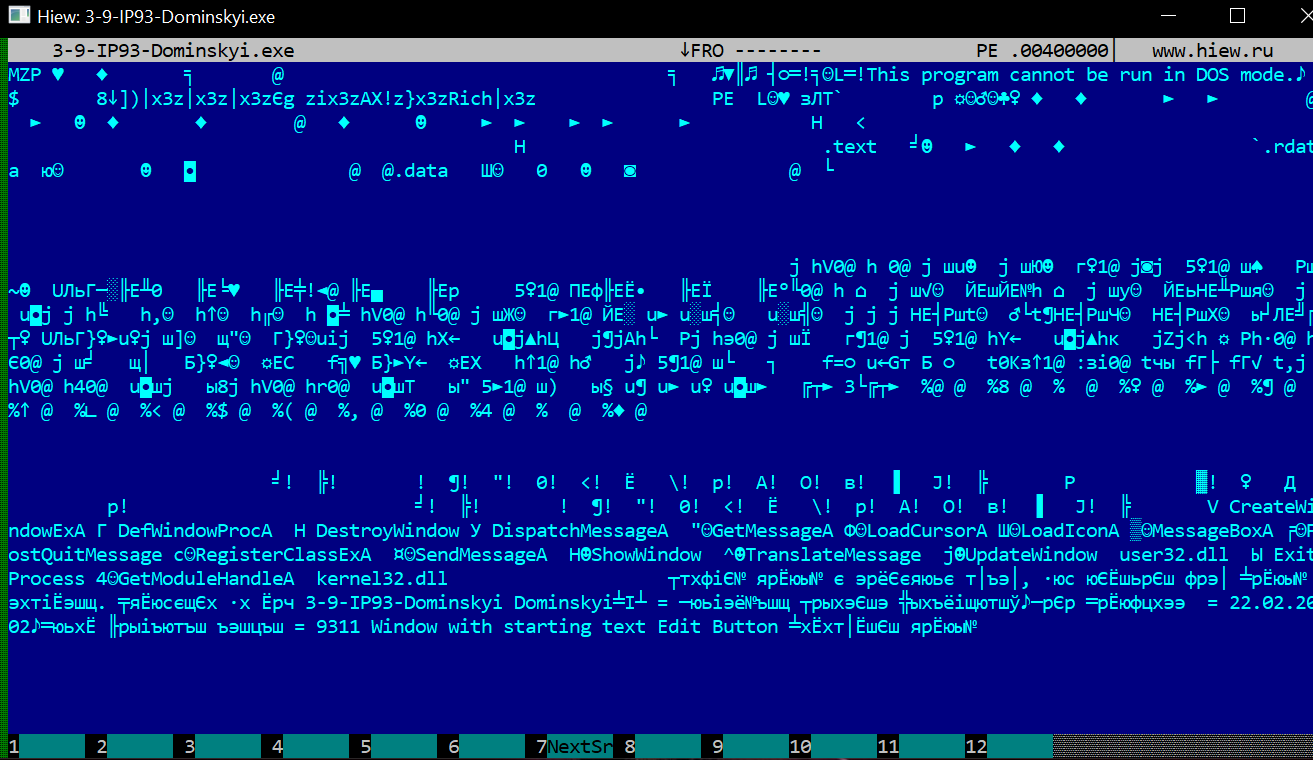


Вивід:

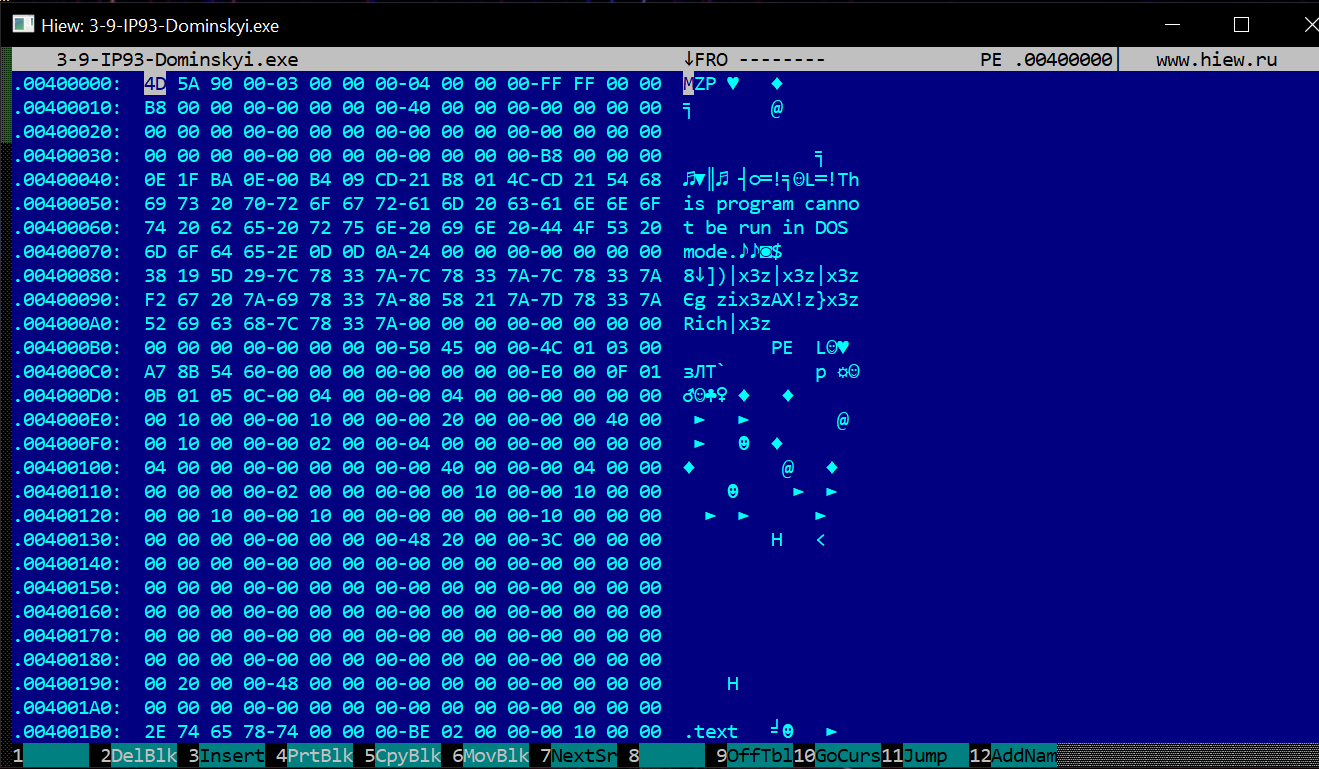


1. Отриманий виконавчий файл дослідити за допомогою програми HEX-редактора HIEW32 або WinHex:

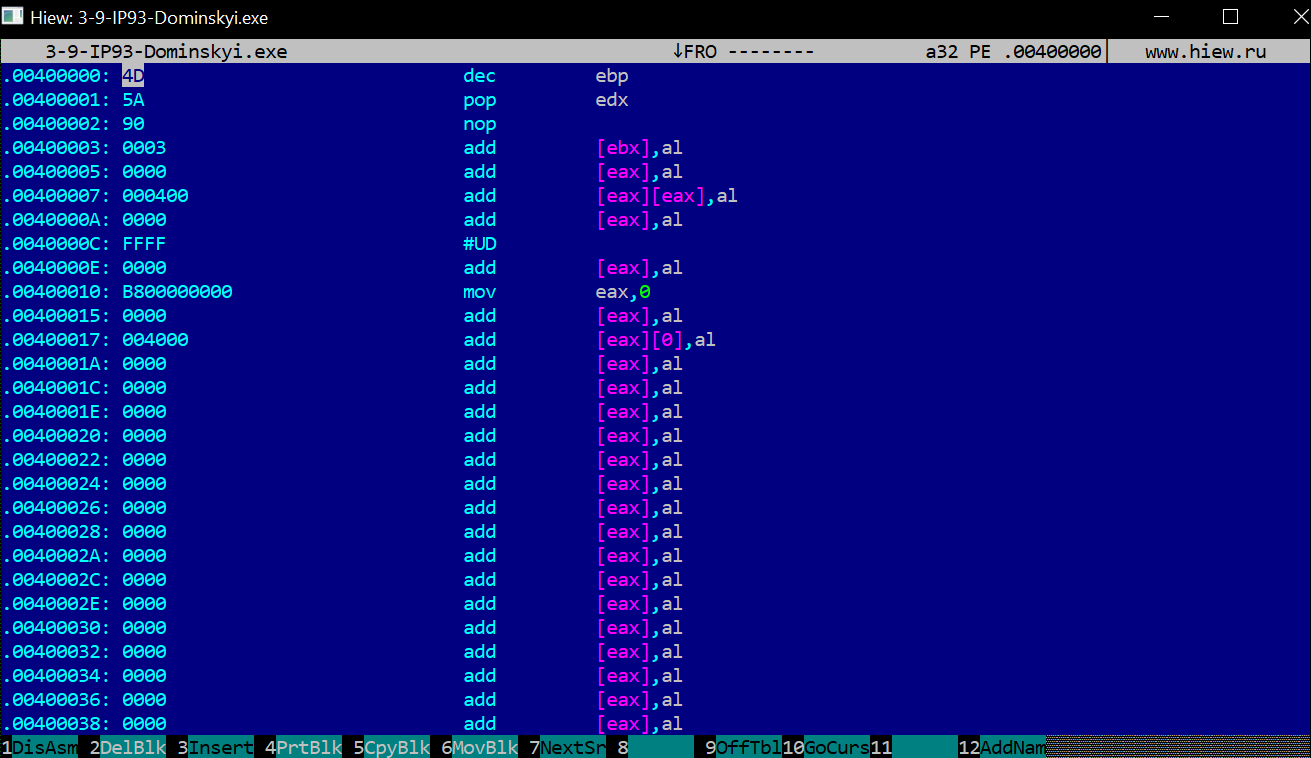
Text:



Hex:

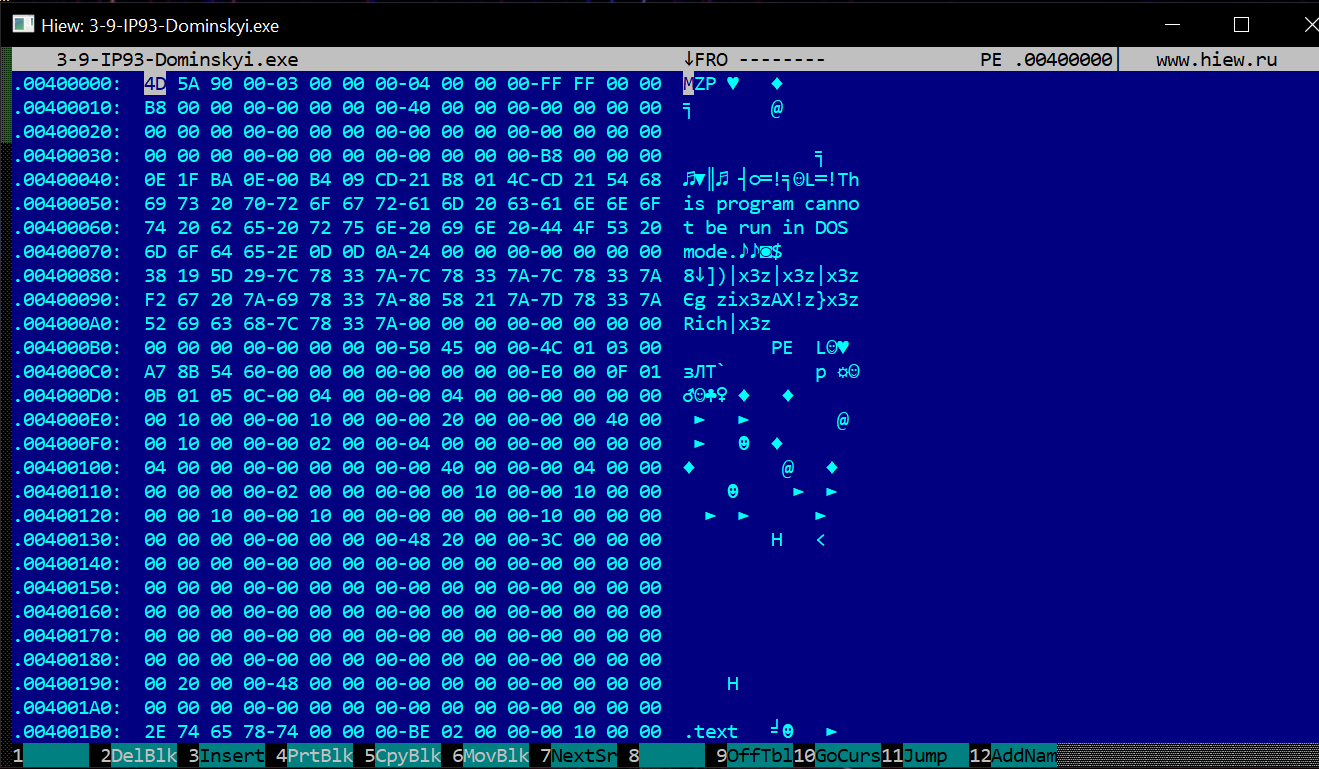


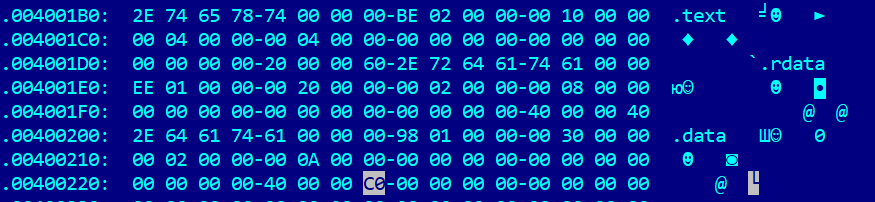
Decode:



1. На скриншоті перших 25 рядків вмісту файлу обвести кольоровим олівцем або фломастером області MS-DOS заголовка (DOS\_HEADER), PE заголовка (PE\_HEADER) і таблиці секцій (SECTION\_HEADERS). Скріншот привести в звіті по лабораторній роботі, де:

* Червоний – MS-DOS заголовок
* Синій - Machine Type
* Жовтий – PE заголовок
* Білий - Optional Header Standard Fields
* Зелений - таблиці секцій





1. Відповідно до опису секцій скласти таблицю, в яку занести параметри свого файлу, вказані в розділах 3.3.1, 3.4.1 і 4
2. У останньому стовпчику таблиці розшифрувати виписані значення полів заголовка файлу. Таблицю привести в звіті по лабораторній роботі

|  |  |  |
| --- | --- | --- |
| Поле | Значення | Опис |
| **Machine Types** | | |
| IMAGE\_FILE\_MACHINE\_I386 | 0x14c  01 4C | Intel 386 or later, and compatible processors. |
| **Optional Header Standard Fields** | | |
| Magic | 01 0B | Unsigned integer identifying the state of the  image file. The most common number is  0413 octal (0x10B), identifying it as a  normal executable file. 0407 (0x107)  identifies a ROM image |
| MajorLinkerVersion | 05 | Linker major version number |
| MinorLinkerVersion | 0C | Linker minor version number |
| SizeOfCode | 00 04 00 00 | Size of the code (text) section, or the sum of  all code sections if there are multiple  sections. |
| SizeOfInitializedData | 00 04 00 00 | Size of the initialized data section, or the  sum of all such sections if there are multiple  data sections. |
| SizeOfUninitializedData | 00 00 00 00 | Size of the uninitialized data section (BSS),  or the sum of all such sections if there are  multiple BSS sections. |
| AddressOfEntryPoint | 00 01 00 00 | Address of entry point, relative to image  base, when executable file is loaded into  memory. For program images, this is the  starting address. For device drivers, this is  the address of the initialization function. An  entry point is optional for DLLs. When none  is present this field should be 0 |
| BaseOfCode | 00 10 00 00 | Address, relative to image base, of  beginning of code section, when loaded into  memory |
| BaseOfData | 00 20 00 00 | Address, relative to image base, of  beginning of data section, when loaded into  memory |
| **Section Table (Section Headers)** | | |
| Name | 00 00 00 74  78 65 74 2E | An 8-byte, null-padded ASCII string. There is no  terminating null if the string is exactly eight  characters long. For longer names, this field  contains a slash (/) followed by ASCII representation  of a decimal number: this number is an offset into  the string table. Executable images do not use a  string table and do not support section names longer  than eight characters. Long names in object files will  be truncated if emitted to an executable file. |
| VirtualSize | 00 00 02 BE | Total size of the section when loaded into memory.  If this value is greater than Size of Raw Data, the  section is zero-padded. This field is valid only for  executable images and should be set to 0 for object  files |
| VirtualAddress | 00 00 10 00 | For executable images this is the address of the first  byte of the section, when loaded into memory,  relative to the image base. For object files, this field  is the address of the first byte before relocation is  applied; for simplicity, compilers should set this to  zero. Otherwise, it is an arbitrary value that is  subtracted from offsets during relocation. |
| SizeOfRawData | 00 00 04 00 | Size of the section (object file) or size of the  initialized data on disk (image files). For executable  image, this must be a multiple of FileAlignment from  the optional header. If this is less than VirtualSize  the remainder of the section is zero filled. Because  this field is rounded while the VirtualSize field is not  it is possible for this to be greater than VirtualSize as  well. When a section contains only uninitialized data,  this field should be 0 |
| PointerToRawData | 00 00 04 00 | File pointer to section’s first page within the COFF  file. For executable images, this must be a multiple  of FileAlignment from the optional header. For  object files, the value should be aligned on a fourbyte boundary for best performance. When a section  contains only uninitialized data, this field should be  0 |
| PointerToRelocations | 00 00 00 00 | File pointer to beginning of relocation entries for the  section. Set to 0 for executable images or if there  are no relocations |
| PointerToLinenumbers | 00 00 00 00 | File pointer to beginning of line-number entries for  the section. Set to 0 if there are no COFF line  numbers |
| NumberOfRelocations | 00 00 | Number of relocation entries for the section. Set to 0  for executable images |
| NumberOfLinenumbers | 00 00 | Number of line-number entries for the section |
| Characteristics | 60 00 00 20 | Flags describing section’s characteristics |

1. Провести дослідження того ж файлу за допомогою меню "PE Editor" безкоштовної програми PE Tools. Всі скріншоти вікон програми з даними, відповідними раніше побудованій таблиці, привести в звіті по лабораторній роботі

Головна сторінка:

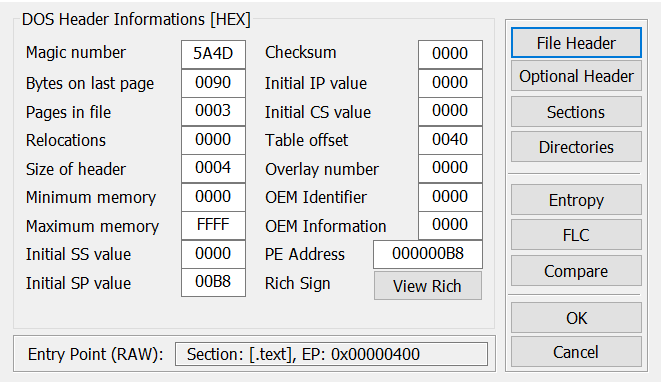


Image File Header Editor:

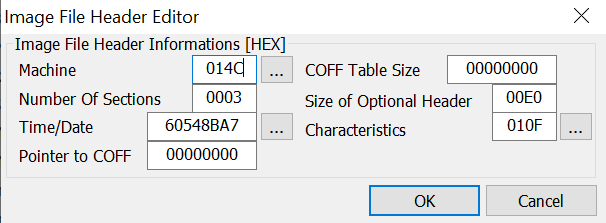
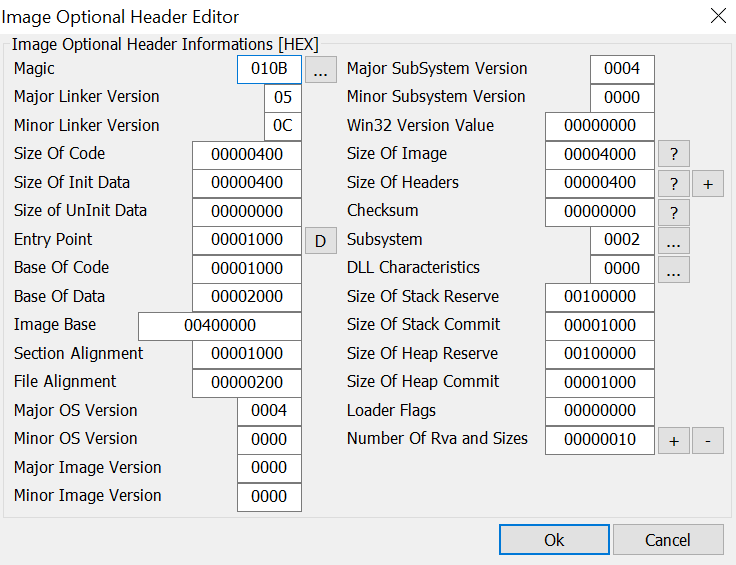
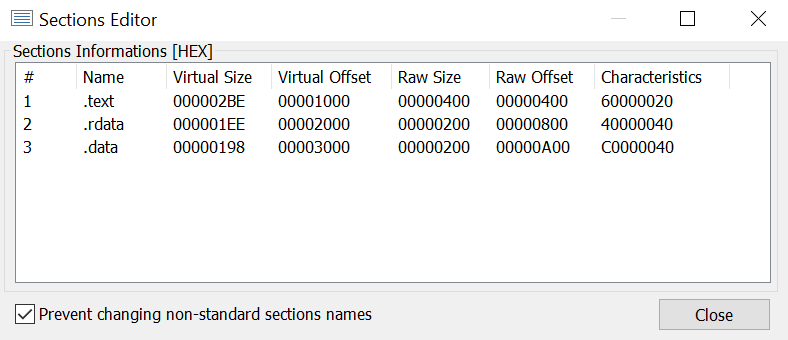


Image Optional Header Editor:

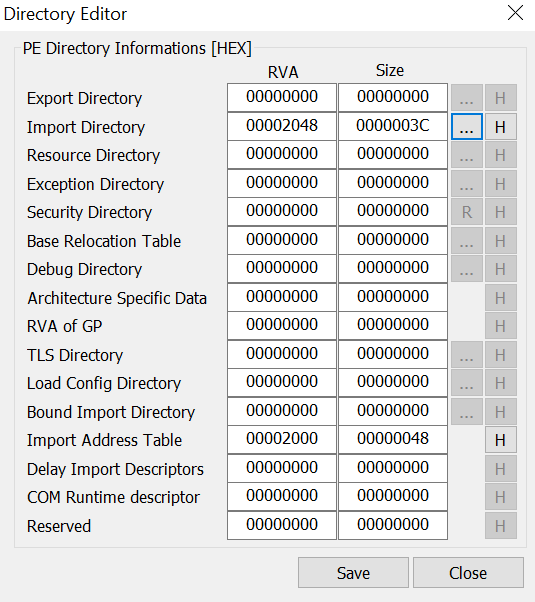


Sections Editor:

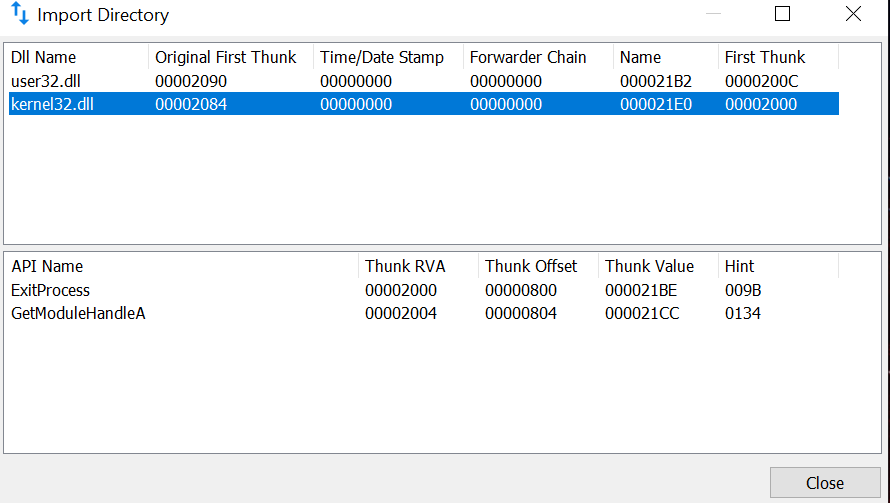
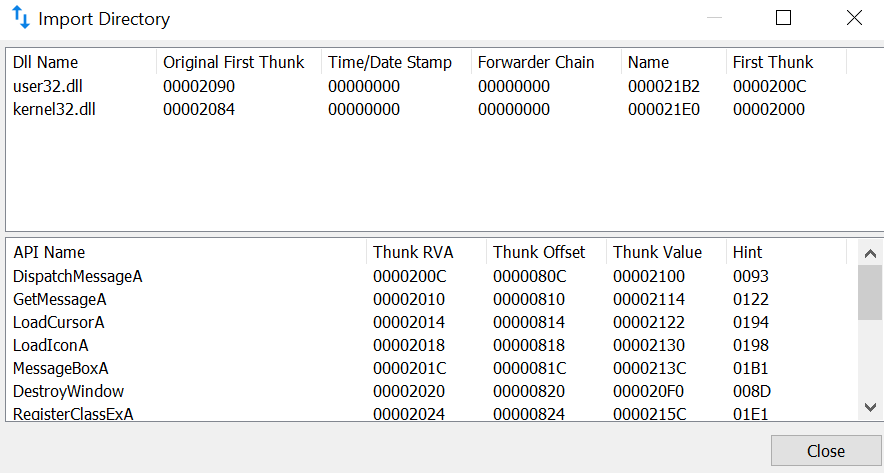


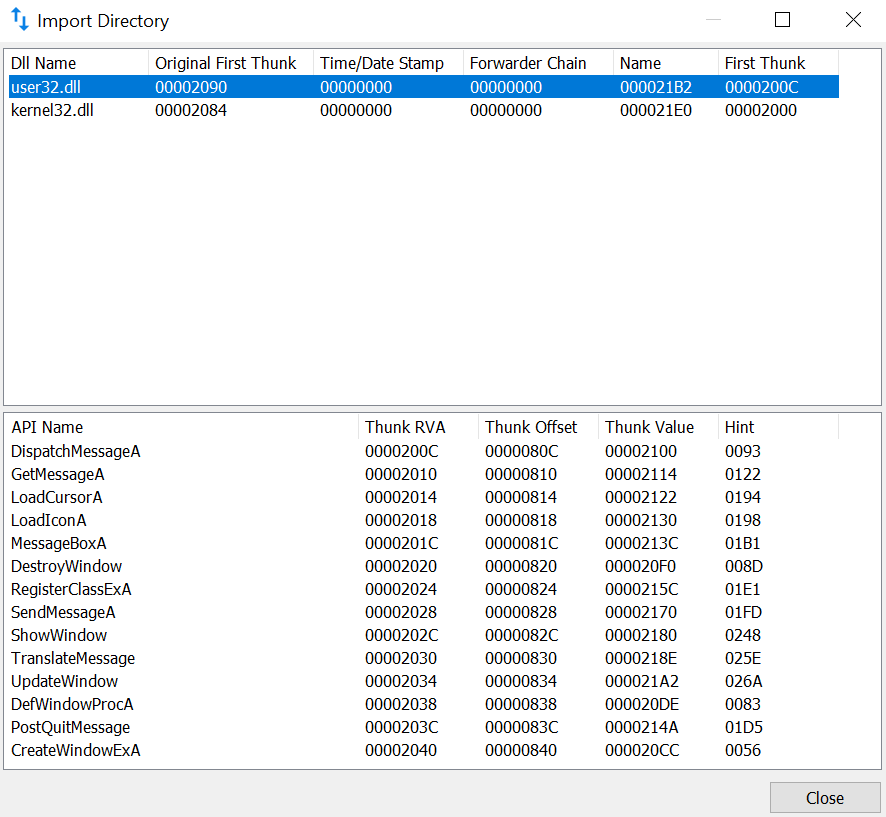
1. Дослідити таблицю імпорту (Import Directory) даного файлу і визначити, які саме функції використовуються з бібліотек, що підключаються. Скріншоти вікон Import Directory з функціями, що імпортуються, з кожного бібліотечного файлу привести в звіті по лабораторній роботі

Directory Editor:



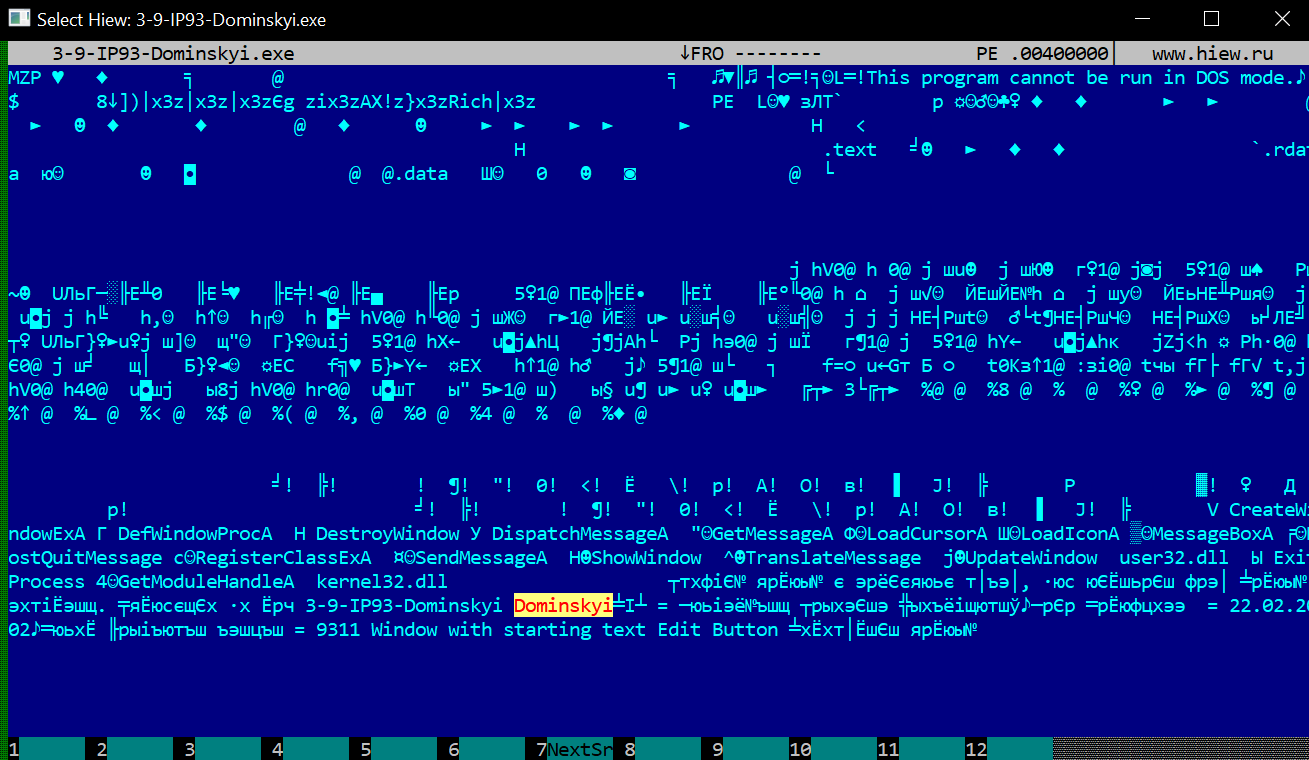
Бібліотеки:



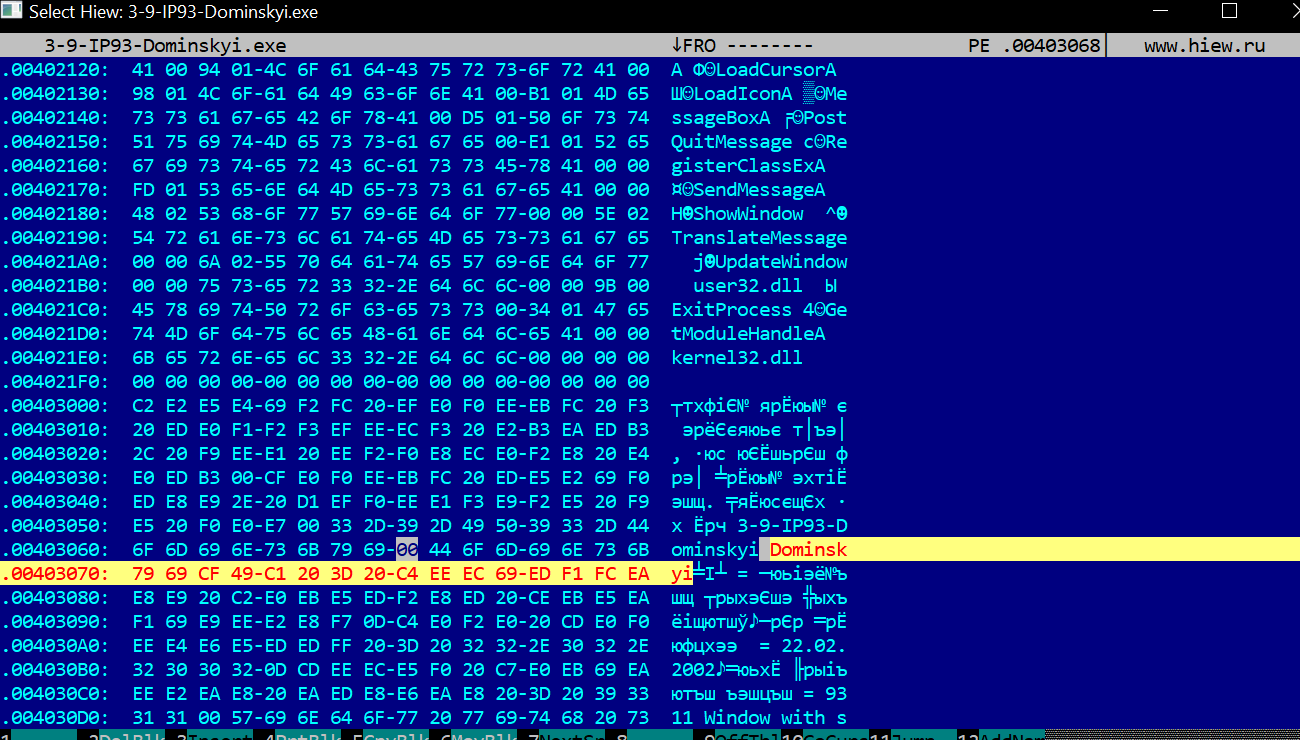


1. Знайти в тексті файлу по зсуву, узятому з побудованої таблиці, секцію з даними і переконатися, що текст оригінала пароля, що міститься в тексті програми, може бути легко виявлений за допомогою HEX-редактора. Привести скриншот цього фрагмента програми у вигляді HEX - коду в звіті по лабораторній роботі:

Text:



HEX:



1. Виконати шифрування пароля за допомогою функції XOR, знову скомпілювати EXE - файл і переконатися, що тепер вони не виявляються явним чином в тексті виконуваного EXE - файлу. Привести скріншоти цієї програми в режимах «Hex» і «Text» в звіті по лабораторній роботі:

; Processors

.386

.model **flat,** **stdcall**

option **CaseMap:None**

WinMainProto proto **:dword,:dword,:dword**

; Libraries And Macroses

include \masm32\include\windows.inc

include \masm32\include\user32.inc

include \masm32\include\kernel32.inc

includelib \masm32\lib\user32.lib

includelib \masm32\lib\kernel32.lib

.data?

hInstance HINSTANCE **?** ; Handle of our program

hWndOfMainWindow HWND **?** ; Handle of our editbox

hWndOfEditbox HWND **?** ; Handle of our editbox

StringFromUser DB 128 dup**(?)**

; Data Segment

.data

StartingText DB "Введiть пароль у наступому вікні, щоб отримати дані"**,** 0

FailureText DB "Пароль невiрний. Спробуйте ще раз"**,** 0

; Name Of Message Box

MsgBoxName DB "3-9-IP93-Dominskyi"**,** 0

; We can write password in two ways:

Password DB "Mfd`gzbp`"

; And another one is:

; Password DB 31h 32h 33h

PasswordCount **=** **$-**Password

XORKey DB 9h

; Text To Show

InformationText DB "ПIБ = Домiнський Валентин Олексiйович"**,** 13**,**

"Дата Народження = 22.02.2002"**,** 13**,**

"Номер Залiковки книжки = 9311"**,** 0

NameOfTheStartingWindows DB "Window with starting text"**,** 0 ; the name of our window class

NameOfTheEditBox DB "Edit"**,** 0 ; the name of our editbox class

NameOfTheButton DB "Button"**,** 0 ; the name of our button class

TextForButton DB "Перевірити пароль"**,** 0

; Code Segment

.code

start**:** ; Generates program start-up code

invoke MessageBox**,** 0**,** offset StartingText**,** offset MsgBoxName**,** MB\_OK

invoke GetModuleHandle**,** NULL

**mov** hInstance**,** **eax**

invoke WinMainProto**,** hInstance**,**NULL**,** SW\_SHOWDEFAULT ;invoke function

invoke ExitProcess**,** **eax** ; quit program. code returns in EAX register from Main Function.

; function declaration of WinMain

WinMainProto proc hInst**:**HINSTANCE**,**hPrevInst**:**HINSTANCE**,**CmdShow**:dword**

; there we need local variables

local wc**:**WNDCLASSEX

local msg**:**MSG

local hwnd**:**HWND

; assign variables of WNDCLASSEX

; window class is a specification of a window

**mov** wc.cbSize**,** sizeof WNDCLASSEX

**mov** wc.style**,** CS\_HREDRAW **or** CS\_VREDRAW

**mov** wc.lpfnWndProc**,** offset WndProc

**mov** wc.cbClsExtra**,** NULL

**mov** wc.cbWndExtra**,** NULL

**push** hInstance

**pop** wc.hInstance

**mov** wc.hbrBackground**,** COLOR\_WINDOW**+**2

**mov** wc.lpszMenuName**,** NULL

**mov** wc.lpszClassName**,** offset NameOfTheStartingWindows

invoke LoadIcon**,** NULL**,** IDI\_APPLICATION

**mov** wc.hIcon**,** **eax**

**mov** wc.hIconSm**,** **eax**

invoke LoadCursor**,** NULL**,** IDC\_ARROW

**mov** wc.hCursor**,** **eax**

; create class of the window

invoke RegisterClassEx**,** **addr** wc

invoke CreateWindowEx**,** NULL**,**

offset NameOfTheStartingWindows**,**

offset MsgBoxName**,**

WS\_OVERLAPPEDWINDOW **or** DS\_CENTER**,**

470**,** 280**,** 300**,** 200**,**

NULL**,** NULL**,** hInst**,** NULL

**mov** hWndOfMainWindow**,** **eax**

; write window handle in eax

**mov** hwnd**,eax**

; Show window

invoke ShowWindow**,** hwnd**,**CmdShow

; update screen

invoke UpdateWindow**,** hwnd

; waits for message

.while TRUE

;returns FALSE if WM\_QUIT message is received and will kill the loop

invoke GetMessage**,** **addr** msg**,**NULL**,**0**,**0

.break .if **(**!**eax)**

;takes raw keyboard input and generates a new message

invoke TranslateMessage**,** **addr** msg

;sends the message data to the window procedure responsible for the specific window the message is for

invoke DispatchMessage**,** **addr** msg

; end while

.endw

; code returns in EAX register from Main Function.

**mov** **eax,** msg.wParam

; return

**ret**

;The ENDP directive defines the end of the procedure

;and has the same name as in the PROC directive

WinMainProto endp

WndProc proc hWnd**:**HWND**,** ourMSG**:**UINT**,** wParam**:**WPARAM**,** lParam**:**LPARAM

; on window close

.if ourMSG**==**WM\_CLOSE

; exit program

invoke PostQuitMessage**,**NULL

.elseif ourMSG**==**WM\_CREATE

invoke CreateWindowEx**,**NULL**,**

offset NameOfTheEditBox**,** NULL**,**

WS\_VISIBLE **or** WS\_CHILD **or** ES\_LEFT **or** ES\_AUTOHSCROLL **or** ES\_AUTOVSCROLL **,**

65**,**20**,**150**,** 30**,**

hWnd**,** 7000**,** hInstance**,** NULL

**mov** hWndOfEditbox**,** **eax**

invoke CreateWindowEx**,**NULL**,**

offset NameOfTheButton**,** offset TextForButton**,**

WS\_VISIBLE **or** WS\_CHILD **or** BS\_CENTER **or** BS\_TEXT **or** BS\_VCENTER**,**

60**,** 90**,** 170**,** 30**,**

hWnd**,** 7001**,** hInstance**,** NULL

.elseif ourMSG**==**WM\_COMMAND

**mov** **bx,** 03h ; counter for tries

**cmp** wParam**,** 7001

**jne** ExitCode

invoke SendMessage**,** hWndOfEditbox**,** WM\_GETTEXT**,** PasswordCount**+**2**,** offset StringFromUser

**mov** **edi,** 0

**cmp** **ax,** PasswordCount

**jne** WrongPasswordByUser

LoopItself**:**

**inc** **edi** ; incrementing

**loop** IsPasswordCorrect

IsPasswordCorrect**:**

**cmp** **edi,** PasswordCount

**je** CorrectPasswordByUser

**mov** **ah,** StringFromUser**[edi]**

**xor** **ah,** XORKey

**cmp** **ah,** Password**[edi]** ; Compare

**je** LoopItself ; Jump Equal

**jmp** WrongPasswordByUser ; Unconditional jump

WrongPasswordByUser**:**

; counting tries

**add** **bx,** **-**01h ; decrementing

**cmp** **bx,** **-**01h ; negative possible tries

**je** TotalExitCode

invoke MessageBox**,** hWnd**,** offset FailureText**,** offset MsgBoxName**,** MB\_OK

**jmp** ExitCode

CorrectPasswordByUser**:**

invoke MessageBox**,** hWnd**,** offset InformationText**,** offset MsgBoxName**,** MB\_OK

**jmp** ExitCode

TotalExitCode**:**

invoke DestroyWindow**,**hWndOfMainWindow

.else

; process the message

invoke DefWindowProc**,**hWnd**,**ourMSG**,**wParam**,**lParam

**ret**

.ENDIF

ExitCode**:**

**xor** **eax,eax**

**ret**

WndProc endp

end start

Шифрування паролю:

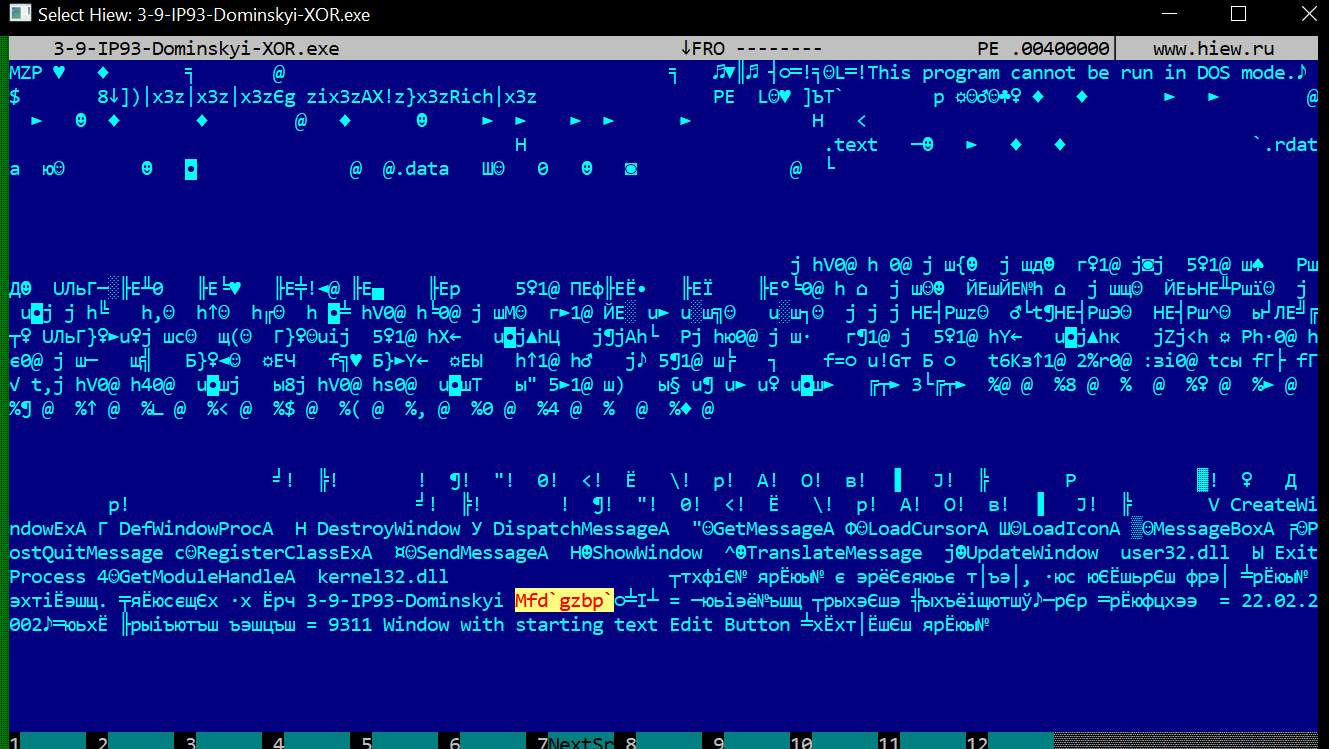
Ключ – 9 (номер у списку)

Пароль до шифрування – Dominskyi

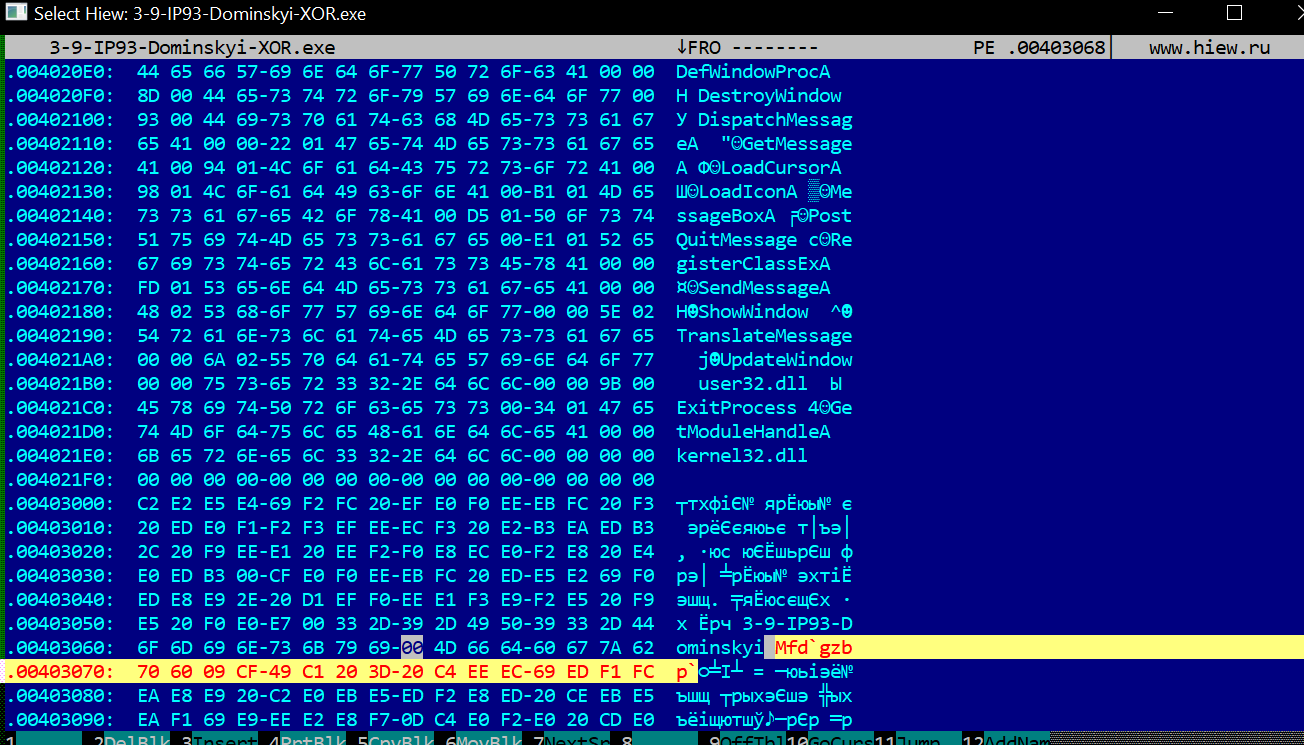
Пароль після шифрування - Mfd`gzbp`

* D -> 0100 0100 -> 0100 1101 -> M
* o -> 0110 1111 -> 0110 0110 -> f
* m -> 0110 1101 -> 0110 0100 -> d
* i -> 0110 1001 -> 0110 0000 -> `
* n -> 0110 1110 -> 0110 0111 -> g
* s -> 0111 0011 -> 0111 1010 -> z
* k -> 0110 1011 -> 0110 0010 -> b
* y -> 0111 1001 -> 0111 0000 -> p
* i -> 0110 1001 -> 0110 0000 -> `

Text:



HEX:



1. Зробити висновки по лабораторній роботі:

**Висновок:**

Я навчився працювати з різними віконними інтерфейсами та форматом EXE в середовищі Masm32. Закріпив на практиці шифрування та розшифрування паролі. Використав програму HIEW для читання лістингу та провів дослідження файлу за допомогою PE-Editor