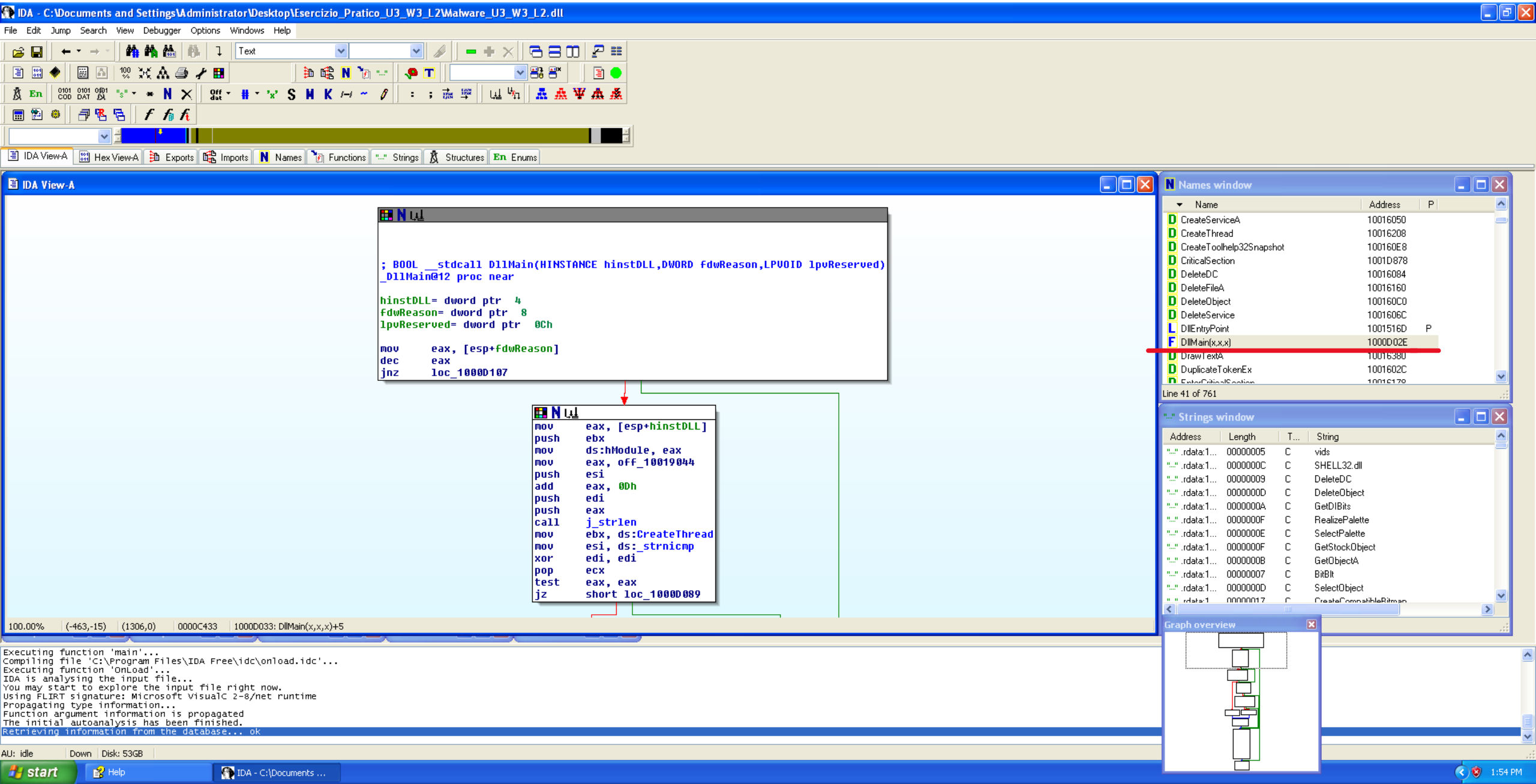
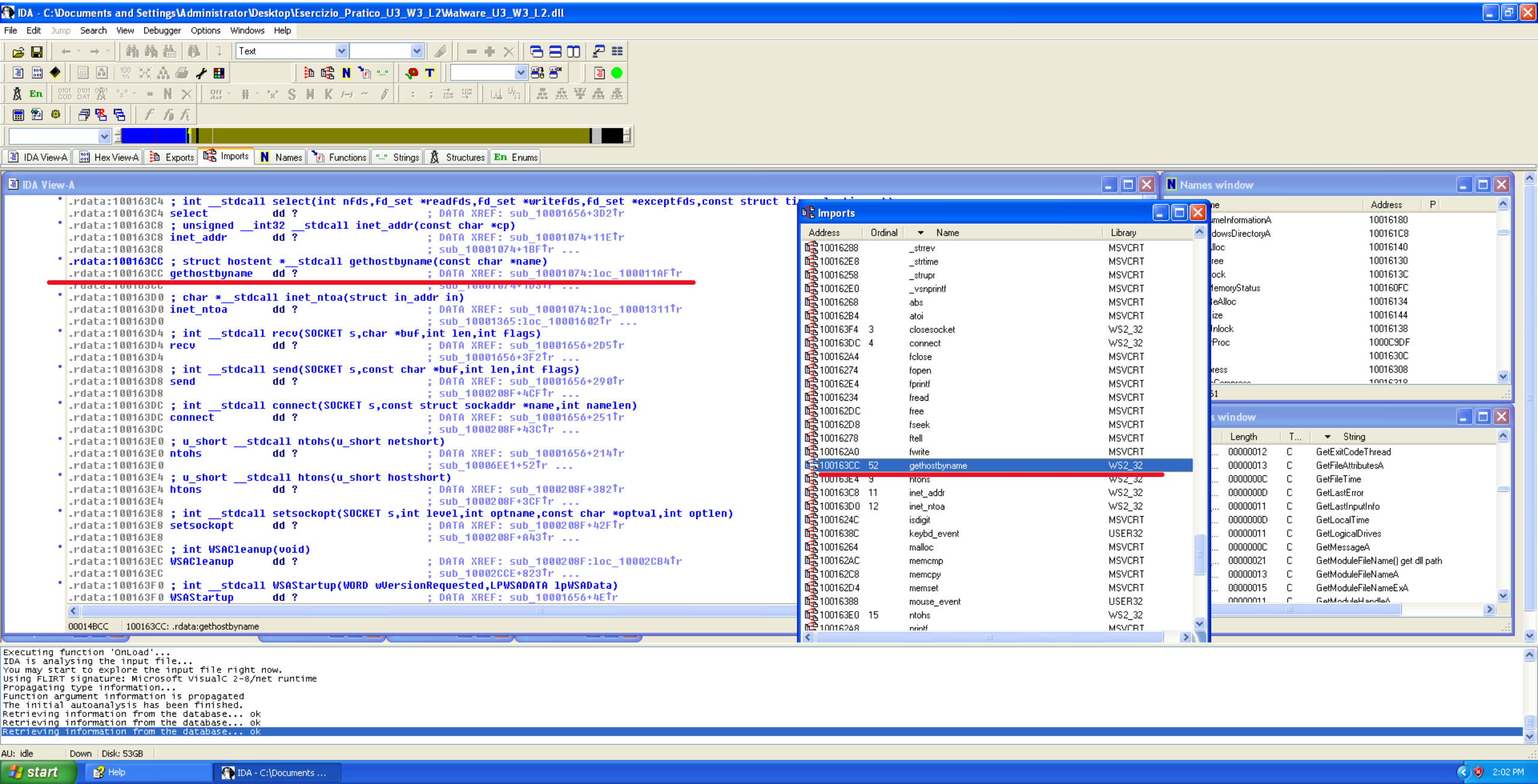
Troviamo l'indirizzo di memoria della funzione DDLMain in esadecimale (1000D02E)



Individuiamo la funzione "gethostbyname" tramite la sezione imports (indirizzo 100163CC).



Per ultimo, possiamo notare le variabili locali ed i parametri all'indirizzo di memoria 0x10001656.

Le variabili locali sono in totale 20, riconoscibili dall'offset negativo (esempio; -675h/-190h).
L'offset è la differenza, positiva o negativa, dal valore di riferimento nella variabile.

I parametri, al contrario, hanno un offset positivo. Ce n'è uno soltanto ed è "arg_0" con offset di 4.

```
.text:10001656
.text:10001656 var_675          = byte ptr -675h
.text:10001656 var_674          = dword ptr -674h
.text:10001656 hModule          = dword ptr -670h
.text:10001656 timeout          = timeval ptr -66Ch
.text:10001656 name             = sockaddr ptr -664h
.text:10001656 var_654          = word ptr -654h
.text:10001656 in               = in_addr ptr -650h
.text:10001656 Parameter        = byte ptr -644h
.text:10001656 CommandLine      = byte ptr -63Fh
.text:10001656 Data             = byte ptr -638h
.text:10001656 var_544          = dword ptr -544h
.text:10001656 var_50C          = dword ptr -50Ch
.text:10001656 var_500          = dword ptr -500h
.text:10001656 var_4FC          = dword ptr -4FCh
.text:10001656 readfds          = fd_set ptr -4BCh
.text:10001656 phkResult        = HKEY__ ptr -3B8h
.text:10001656 var_3B0          = dword ptr -3B0h
.text:10001656 var_1A4          = dword ptr -1A4h
.text:10001656 var_194          = dword ptr -194h
.text:10001656 WSAData          = WSAData ptr -190h
.text:10001656 arg_0            = dword ptr  4
.text:10001656
```

Possiamo anche dedurre che sia una backdoor poiché all'interno del codice si trovano alcune variabili inerenti ad un ipotetico server di backdoor.

```
xdoors_d:10093D74 ; char aBackdoorServer[]
xdoors_d:10093D74 aBackdoorServer db 0Dh,0Ah             ; DATA XREF: sub_100042DB+B5↑o
xdoors_d:10093D74                 db 0Dh,0Ah
xdoors_d:10093D74                 db '******************************',0Dh,0Ah
xdoors_d:10093D74                 db '[BackDoor Server Update Setup]',0Dh,0Ah
xdoors_d:10093D74                 db '******************************',0Dh,0Ah
xdoors_d:10093D74                 db 0Dh,0Ah,0
xdoors_d:10093DDB                 align 4
```