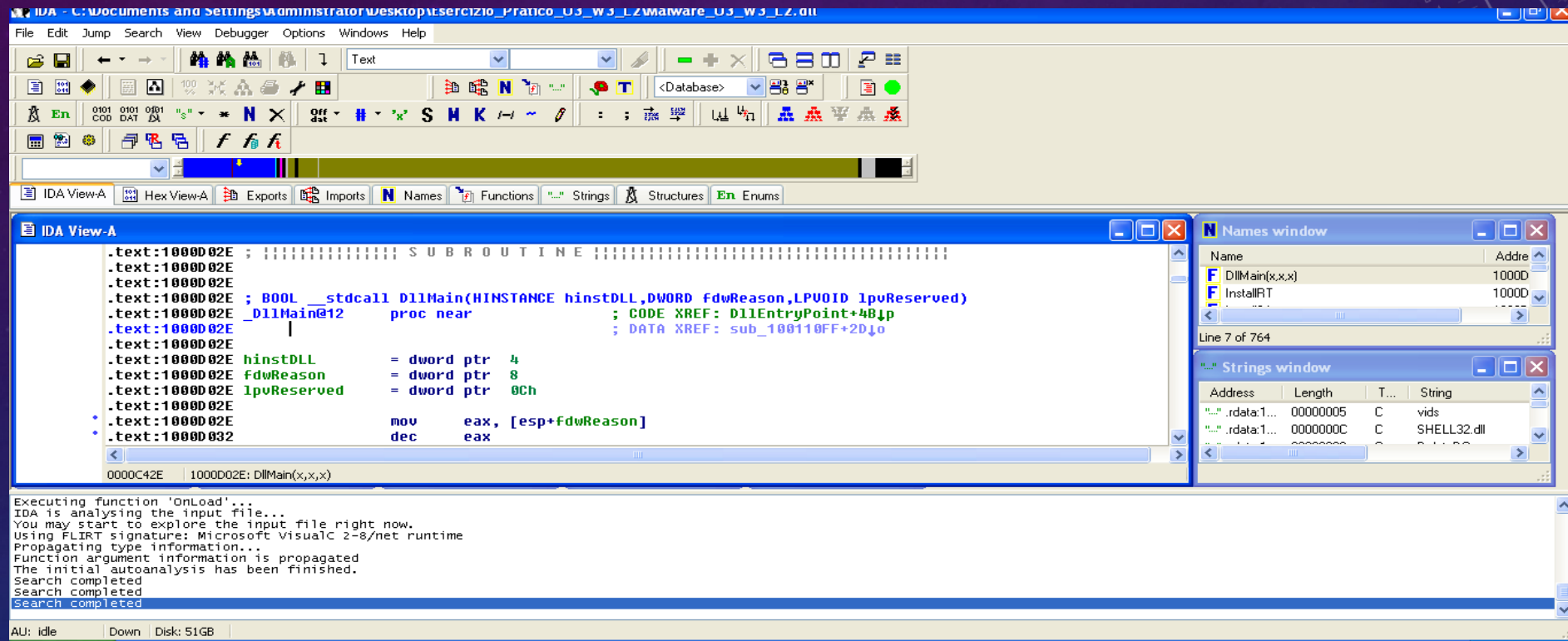


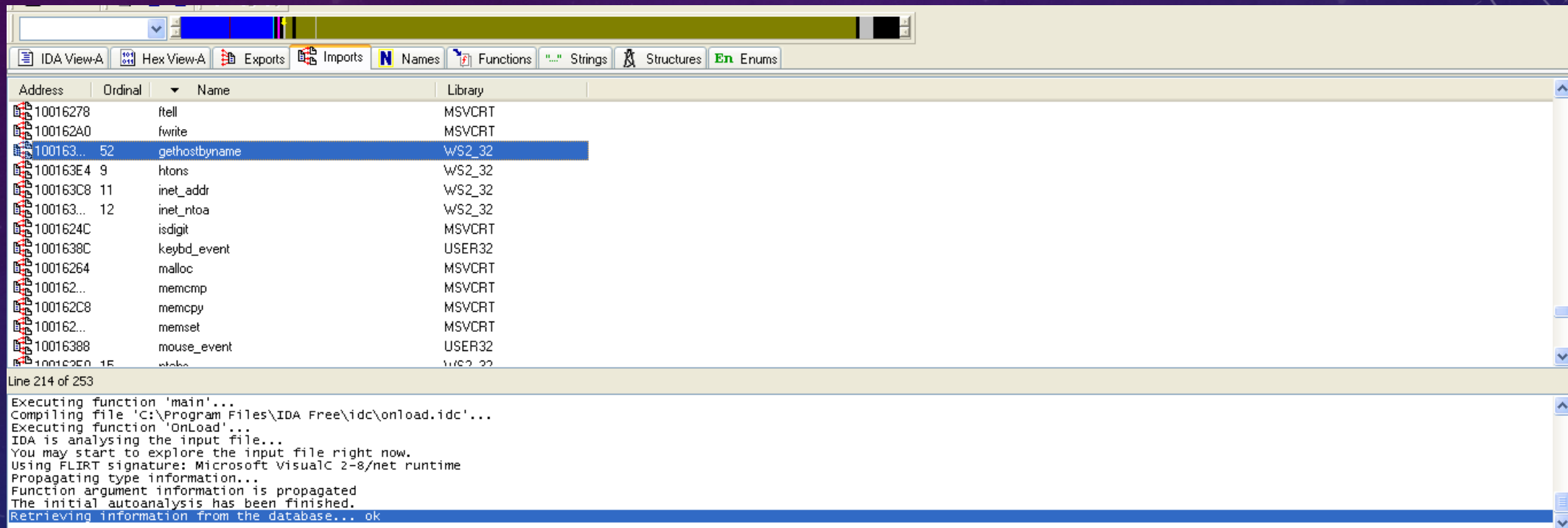
TRACCIA: LO SCOPO DELL'ESERCIZIO DI OGGI È DI ACQUISIRE ESPERIENZA CON IDA, UN TOOL FONDAMENTALE PER L'ANALISI STATICA. A TAL PROPOSITO, CON RIFERIMENTO AL MALWARE CHIAMATO «MALWARE_U3_W3_L2» PRESENTE ALL'INTERNO DELLA CARTELLA «ESERCIZIO_PRATICO_U3_W3_L2» SUL DESKTOP DELLA MACCHINA VIRTUALE DEDICATA ALL'ANALISI DEI MALWARE, RISPONDERE AI SEGUENTI QUESITI, UTILIZZANDO IDA PRO.

1. INDIVIDUARE L'INDIRIZZO DELLA FUNZIONE DLLMAIN
2. DALLA SCHEDA «IMPORTS» INDIVIDUARE LA FUNZIONE «GETHOSTBYNAME». QUAL È L'INDIRIZZO DELL'IMPORT?
3. QUANTE SONO LE VARIABILI LOCALI DELLA FUNZIONE ALLA LOCAZIONE DI MEMORIA 0X10001656?
4. QUANTI SONO, INVECE, I PARAMETRI DELLA FUNZIONE SOPRA?

INDIVIDUARE L'INDIRIZZO DELLA FUNZIONE DLLMAIN: PERTROVARE L'INDIRIZZO DELLA FUNZIONE DLLMAIN, CARICHIAMO IL FILE CON IDA PRO. PREMIAMO LA BARRA PER PASSARE NELLA MODALITÀ TESTUALE (TEXT,DATABASE) RECUPERIAMO L'INDIRIZZO DELLA FUNZIONE MAIN CHE SARÀ: 1000D02E



QUAL È L'INDIRIZZO DELL'IMPORT «GETHOSTBYNAME»? APRIAMO LA FINESTRA «IMPORTS» SEMPRE CON IDA PRO, E LOCALIZZIAMO LA FUNZIONE CERCATA. «GESTHOSTBYNAME» È ALL'INDIRIZZO 100163CC, COME MOSTRATO IN FIGURA.



QUANTE SONO I PARAMETRI DELLA FUNZIONE ALLA LOCAZIONE DI MEMORIA 10001656? PER PRIMA COSA BISOGNA SPOSTARSI ALL'INDIRIZZO TROVATO TRAMITE LA RICERCA O LA BARRA LATERALE. A QUESTO INDIRIZZO TROVIAMO 20 VARIABILI CON OFFSET NEGATIVO RISPETTO AD EBP

```
.text:10001656 ; ::::::::::::::: S U B R O U T I N E :::::::::::::::
.text:10001656
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656      proc near                                ; DATA XREF:
.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
```