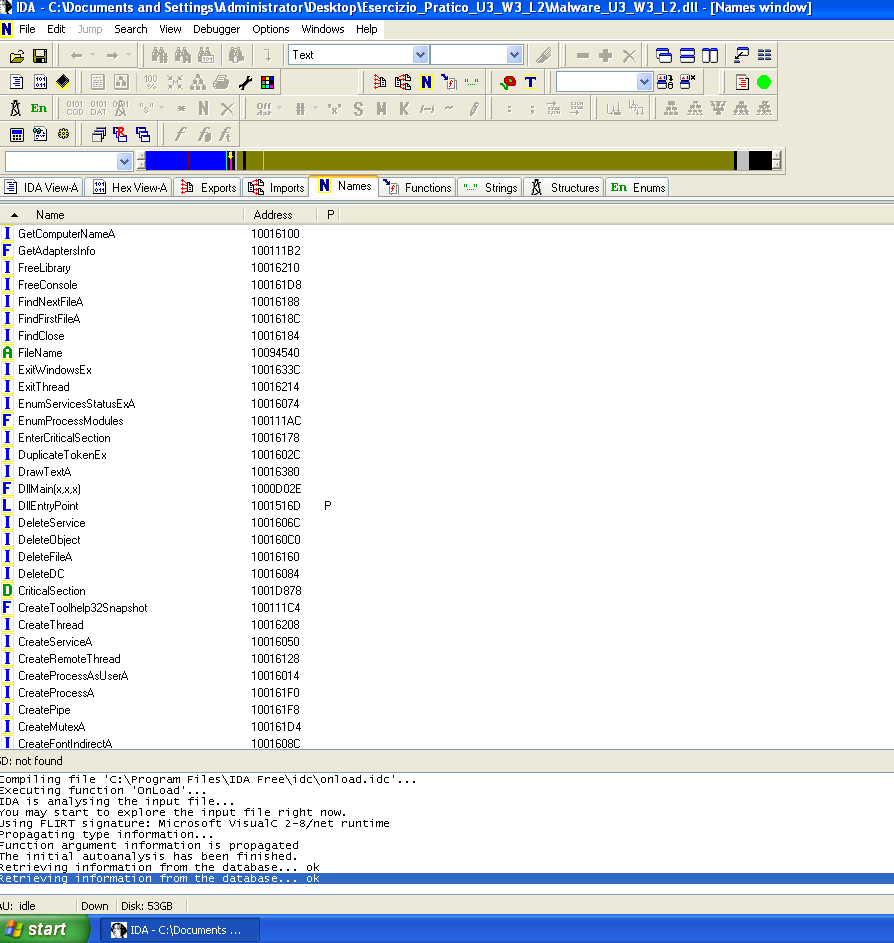
Analisi statica avanzata

L’esercizio di oggi ci chiedeva di analizzare un malware con IDA per:

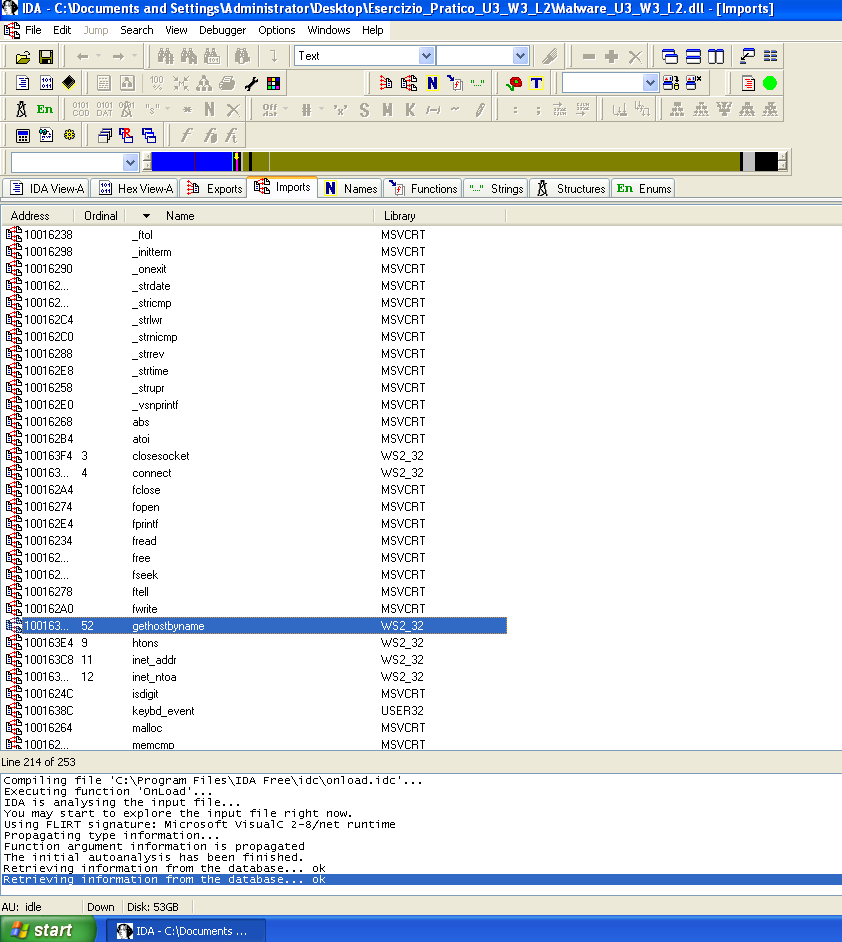
* Individuare l’indirizzo della funzione **DLLMain**
* Indirizzo funzione **gethostbyname**
* Individuare le variabili locali e parametri della funzione alla locazione di memoria 0x10001656

Indirizzo funzione DLLMain



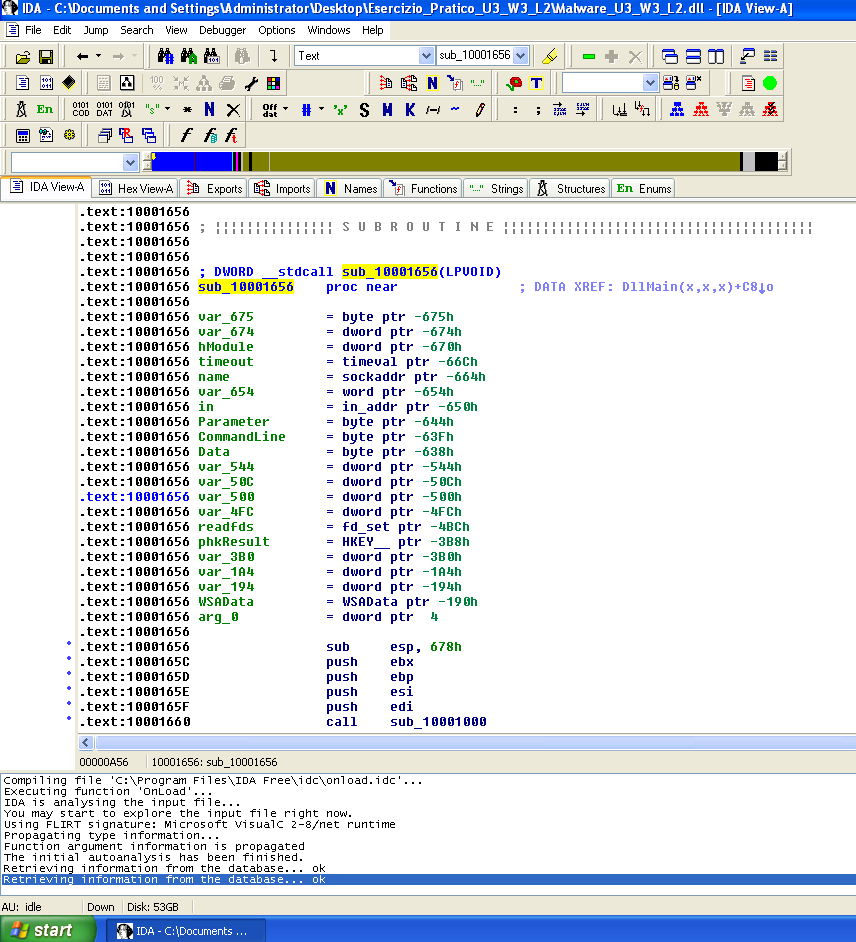
Qui possiamo notare l’indirizzo della funzione evidenziata.

Indirizzo funzione gethostbyname



Qui evidenziato c’è l’indirizzo della funzione **gethostbyname** ovvero **100163CC**.

Variabili e parametri di una funzione



Nell’immagine possiamo notare le variabili e i parametri della funzione. Si possono distinguere in quanto le variabili hanno offset negativo rispetto ad EBP, mentre i parametri hanno offset positivo rispetto ad EBP.