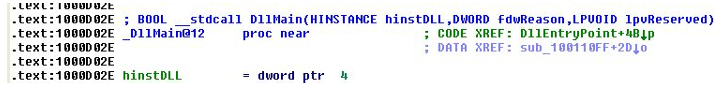
**ANALISI STATICA CON IDA PRO**

**- Individuare l’indirizzo della funzione DLLMain**

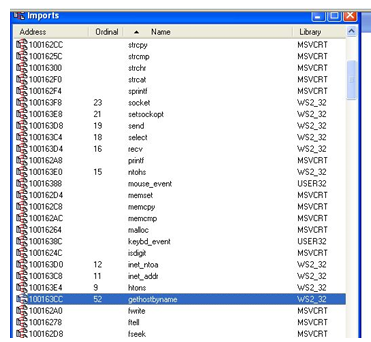
Una volta caricato l’eseguibile in IDA Pro, premiamo la barra spaziatrice per passare nella modalità testuale e recuperare l’indirizzo della funzione main che sarà: **1000D02E**



-**Individuare l’indirizzo dell’import** **«gethostbyname»**

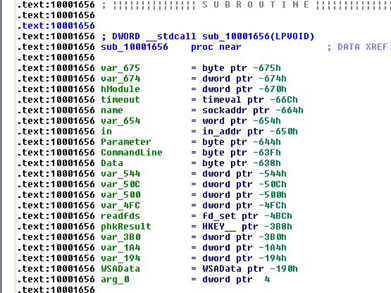
Apriamo la finestra degli «imports» da IDA Pro, e localizziamo la funzione cercata.

«gesthostbyname» è all’indirizzo **100163CC**



- **Quante sono le variabili locali della funzione alla locazione di memoria 10001656**

Per prima cosa bisogna spostarsi all’indirizzo ricercato tramite la ricerca o la barra laterale. A questo indirizzo troviamo 20 variabili con offset negativo rispetto ad EBP



Dalla stessa figura, possiamo notare un solo argomento passato alla funzione, avente offset positivo rispetto ad EBP. IDA ha chiamato questo parametro **«arg\_0».**