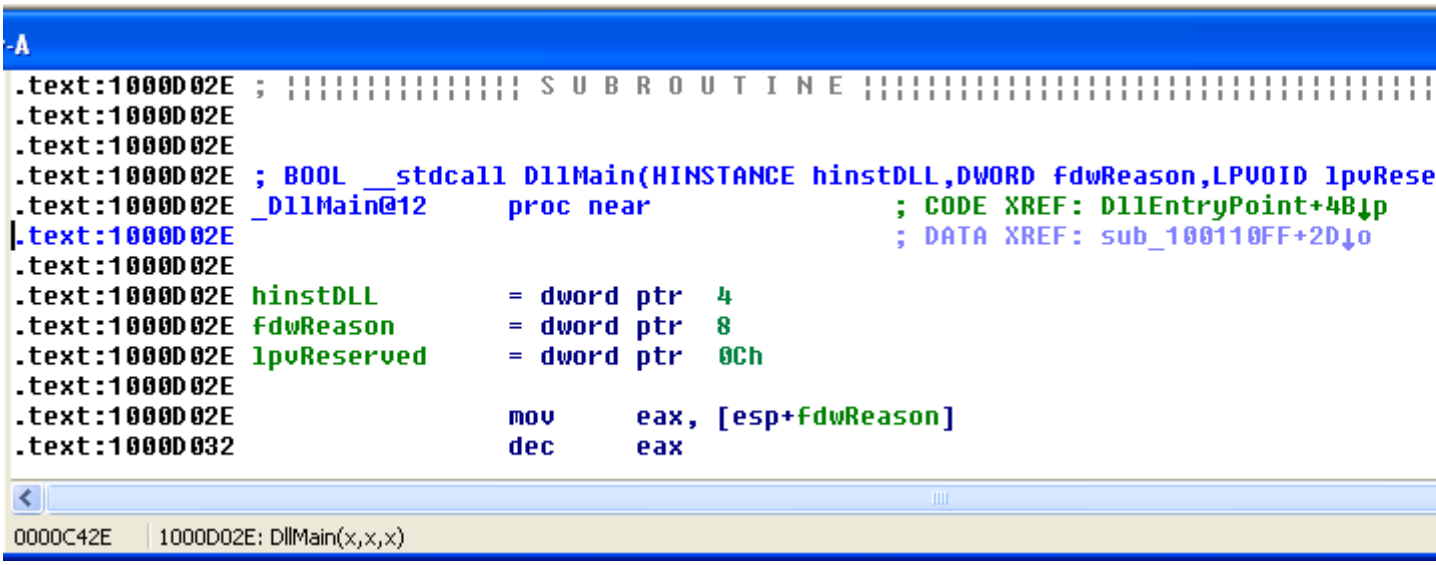
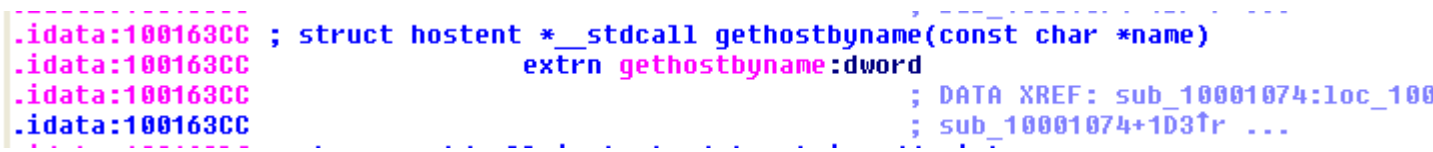
Oggi andremo ad analizzare il malware dato dall'esercizio con ida pro, un noto dissassambler. Una volta caricato su ida, cerchiamo la funzione dll main del codice:



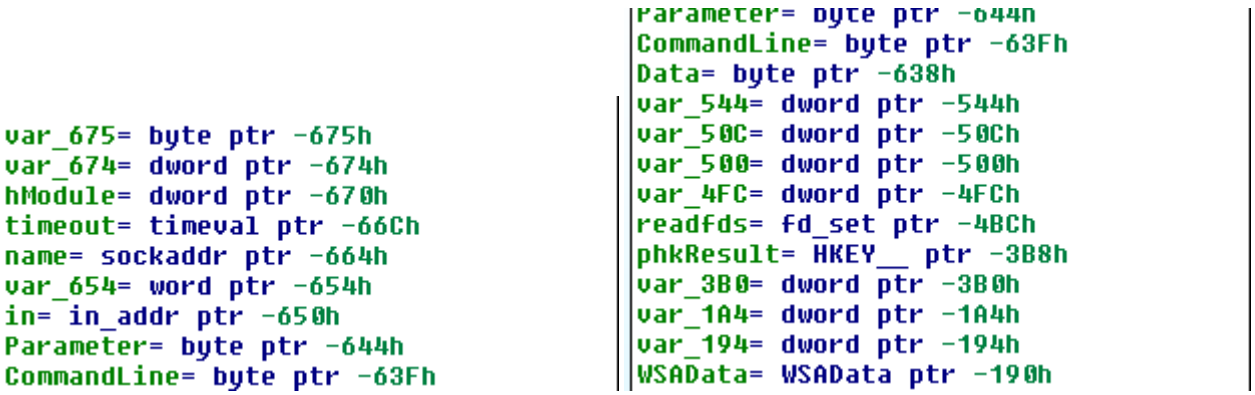
In questo modo ne ricaviamo anche l'indirizzo di memoria :

Una volta trovata, da imports individuiamo la funzione "gethostbyname:



E ne ricaviamo l'indirizzo: 

Dopo aver cercato l'indirizzo di memoria 0x10001656 abbiamo trovato le variabili locali della funzione alla suddetto indirizzo:



Queste sono tutte variabili locali della funzione in quanto, come studiato nella lezione della mattina, hanno un offsett negativo rispetto ad ebx.

Invece l'unico parametro all'interno della funzione che stiamo studiando è il seguente:

```
arg_0= dword ptr  4
```

In quanto è l'unico ad avere offset positivo.

Infine abbiamo appurato che il malware in questione è una backdoor, in quanto, dopo aver effettuato un'analisi statica basica ed aver estrapolato il suo hash ed averlo cercato su virus total, il risultato è il seguente: