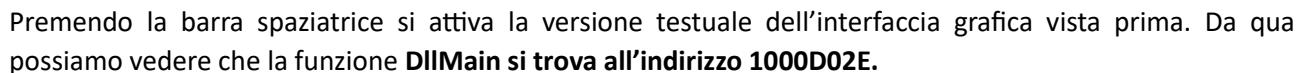


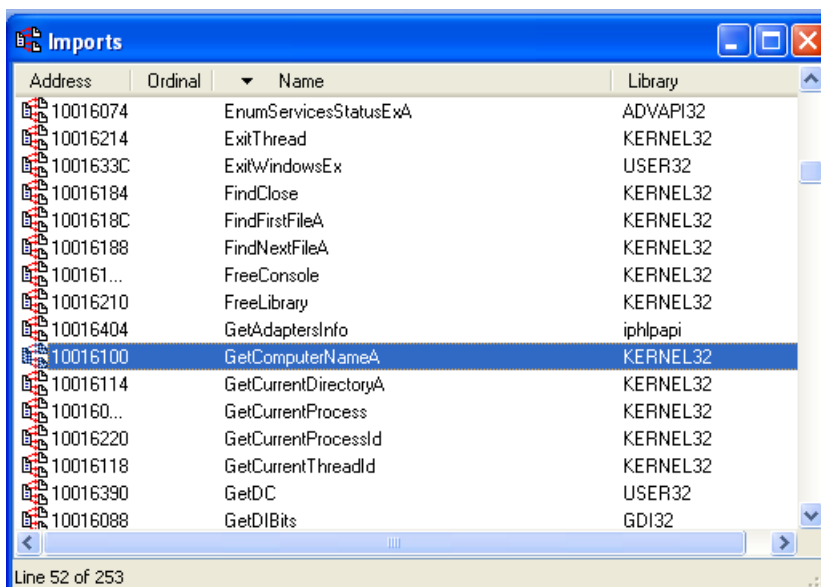
Malware_U3_W3_L2

Nel pannello centrale di IDA vengono mostrate le traduzioni in Assembly del codice macchina dell'eseguibile (in questo caso **Malware_U3_W3_L2.dll**). Nel rettangolo rosso vediamo la funzione DllMain.



2. Dalla scheda "Imports" individuare la funzione "GetComputerName". Qual è l'indirizzo dell'import?

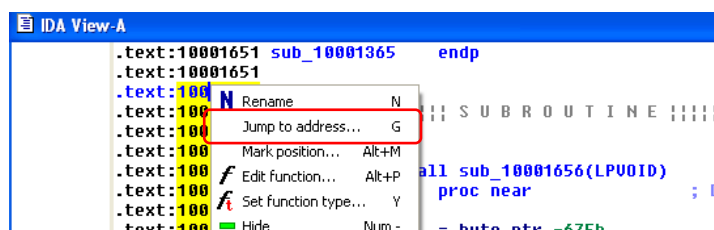
La scheda Imports mostra le funzioni importate dall'eseguibile. La prima colonna, Address, specifica l'indirizzo della funzione, che come evidenziato nell'immagine è **10016100**.



3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

4. Quanti sono invece i parametri della funzione sopra?

Dall'interfaccia testuale col tasto destro selezioniamo l'opzione "Jump to address.." per saltare all'indirizzo di memoria richiesto.



A questo indirizzo dall'interfaccia testuale di IDA possiamo vedere che viene chiamata la funzione DllMain.

```
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656 proc near ; DATA XREF: DllMain(x,x,x)+C8↓o
```

Nelle sezioni sottostanti vediamo in verde i parametri e le variabili della funzione. Con IDA sappiamo che la variabili hanno un offset negativo rispetto al registro ebp, mentre i parametri hanno un offset positivo.

L'offset, evidenziato nella figura sotto, è riportato in verde in coda al parametro / variabile.

.text:10001656		= byte ptr -675h
.text:10001656	var_675	= dword ptr -674h
.text:10001656	var_674	= dword ptr -670h
.text:10001656	hModule	= timeval ptr -66Ch
.text:10001656	timeout	= sockaddr ptr -664h
.text:10001656	name	= word ptr -654h
.text:10001656	var_654	= in_addr ptr -650h
.text:10001656	in	= byte ptr -644h
.text:10001656	Parameter	= byte ptr -63Fh
.text:10001656	CommandLine	= byte ptr -638h
.text:10001656	Data	= dword ptr -544h
.text:10001656	var_544	= dword ptr -50Ch
.text:10001656	var_50C	= dword ptr -500h
.text:10001656	var_500	= dword ptr -4FC
.text:10001656	var_4FC	= fd_set ptr -48Ch
.text:10001656	readfds	= HKEY__ ptr -388h
.text:10001656	phkResult	= dword ptr -380h
.text:10001656	var_380	= dword ptr -1A4h
.text:10001656	var_1A4	= dword ptr -194h
.text:10001656	var_194	= WSADATA ptr -190h
.text:10001656	WSADATA	= dword ptr 4
.text:10001656	arg_0	

Abbiamo un totale di 21 voci, di cui 20 hanno offset negativo rispetto a ebp, e sono quindi variabili della funzione, mentre 1, **arg_0**, ha un offset positivo. **arg_0** è quindi l'unico parametro della funzione.