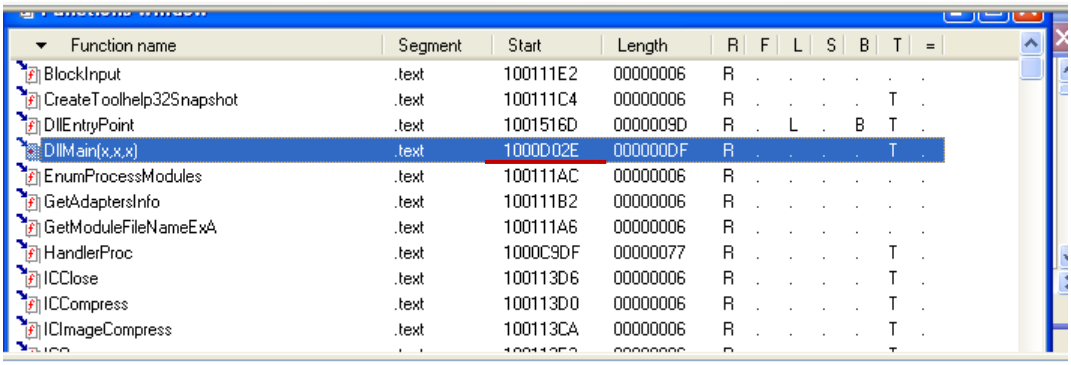
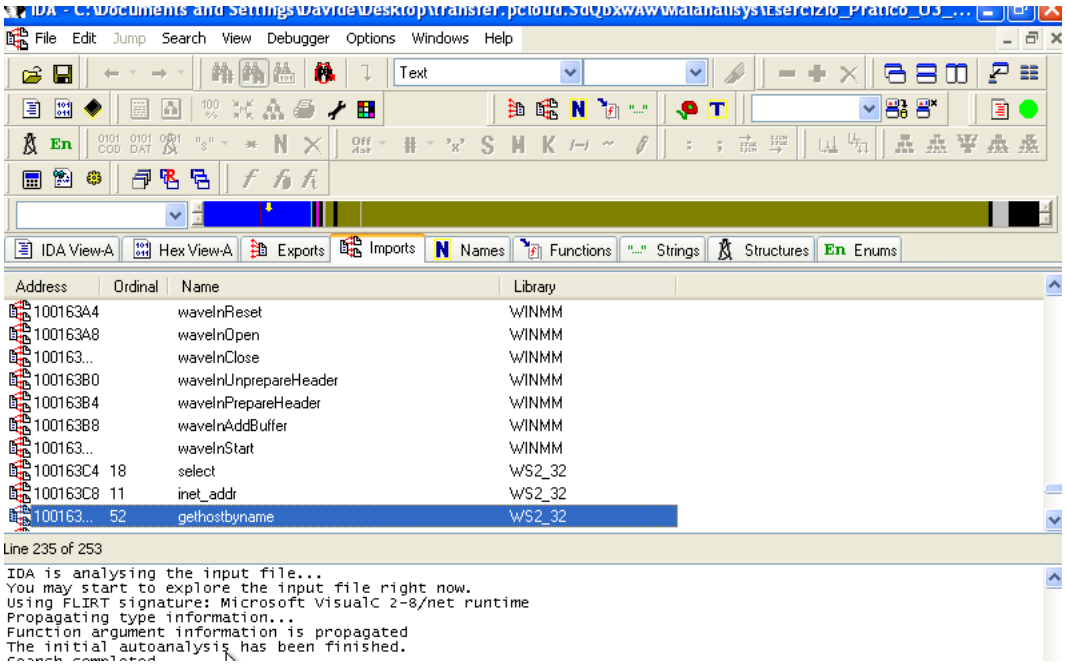
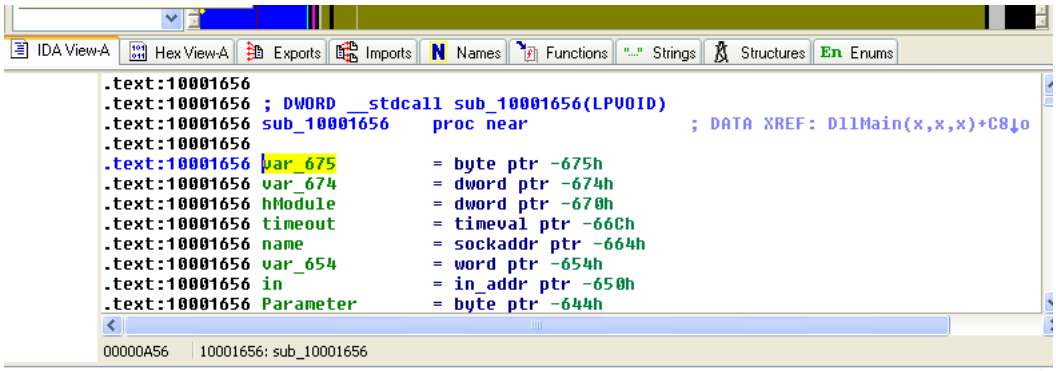


1. Nello screen possiamo vedere l'indirizzo della funzione DllMain



2. Dalla scheda "imports" possiamo individuare la funzione **gethostbyname** e il suo rispettivo indirizzo **100163CC**



3. Facendo una ricerca dell'allocazione di memoria della funzione **0x10001656** possiamo andare a vedere le sue variabili che sono 20

4. Invece abbiamo 2 parametri della funzione sopra

5. Il malware è probabilmente uno spyware con una backdoor oltre ad eseguire svariate altre funzioni.