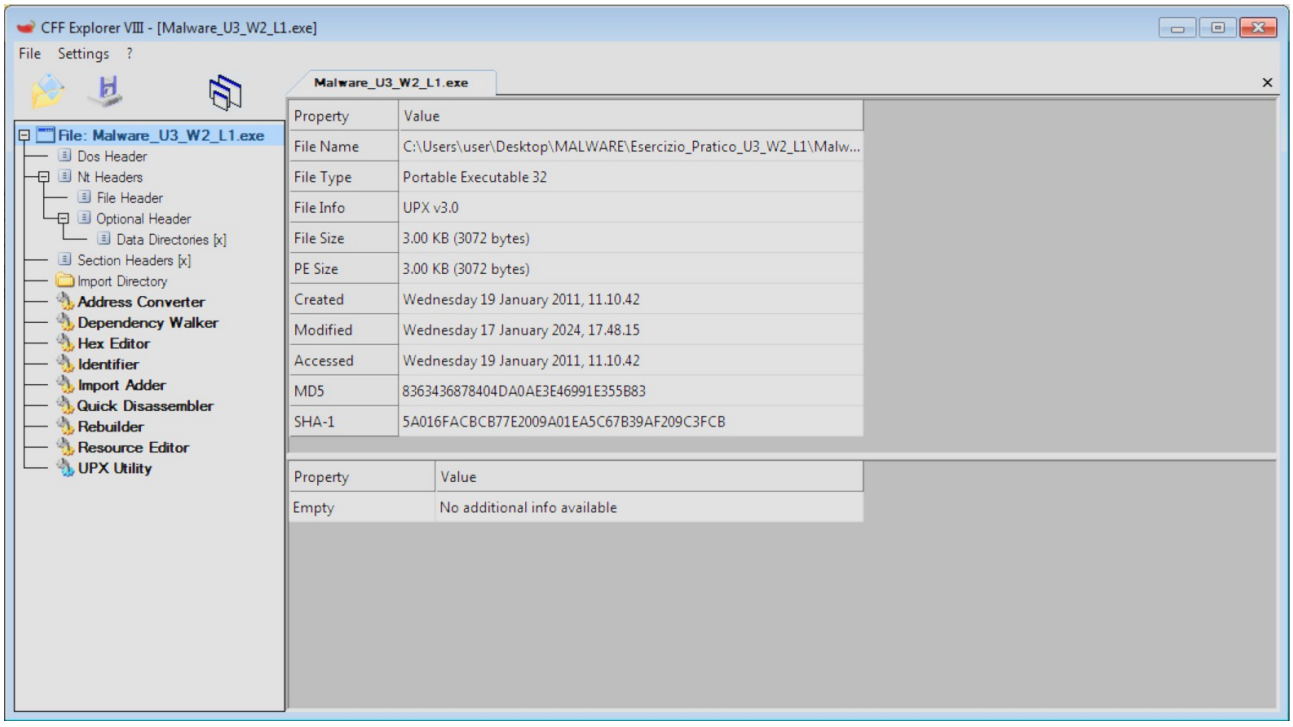
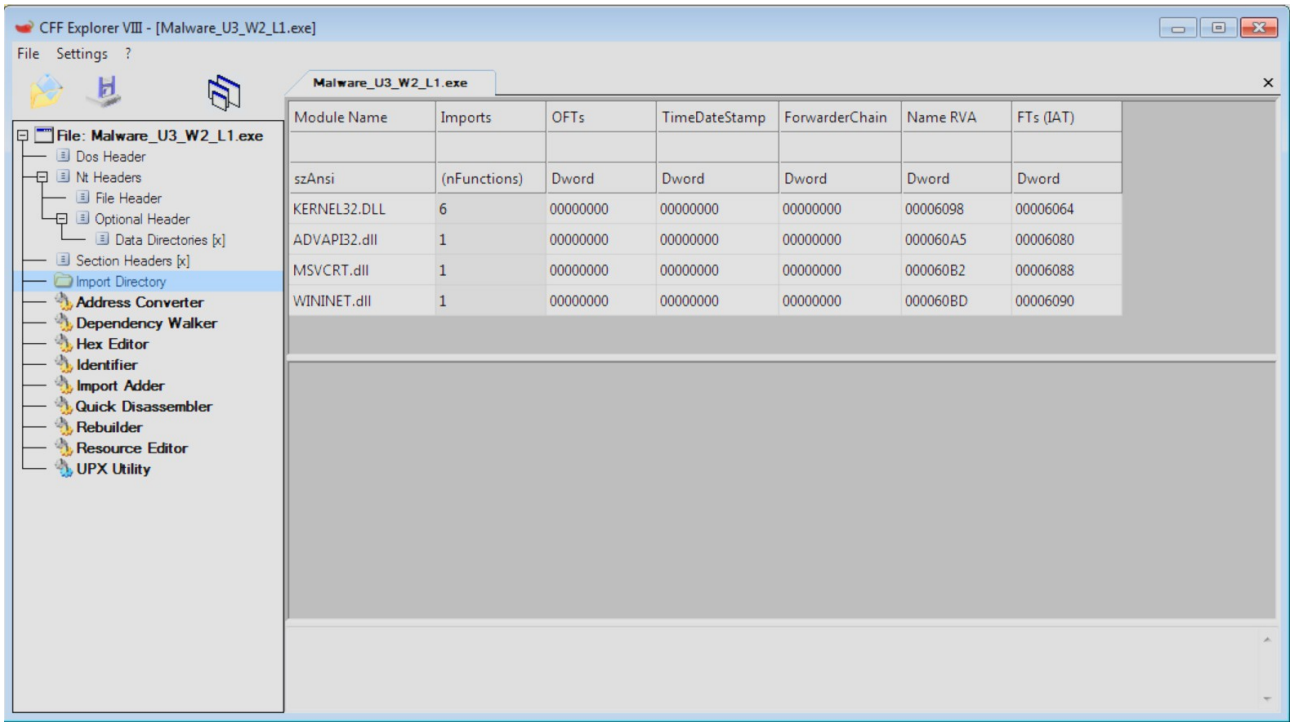
Analisi statica del malware
oggi andiamo ad analizzare in maniera statica, cioè senza l'esecuzione, un **malware**.



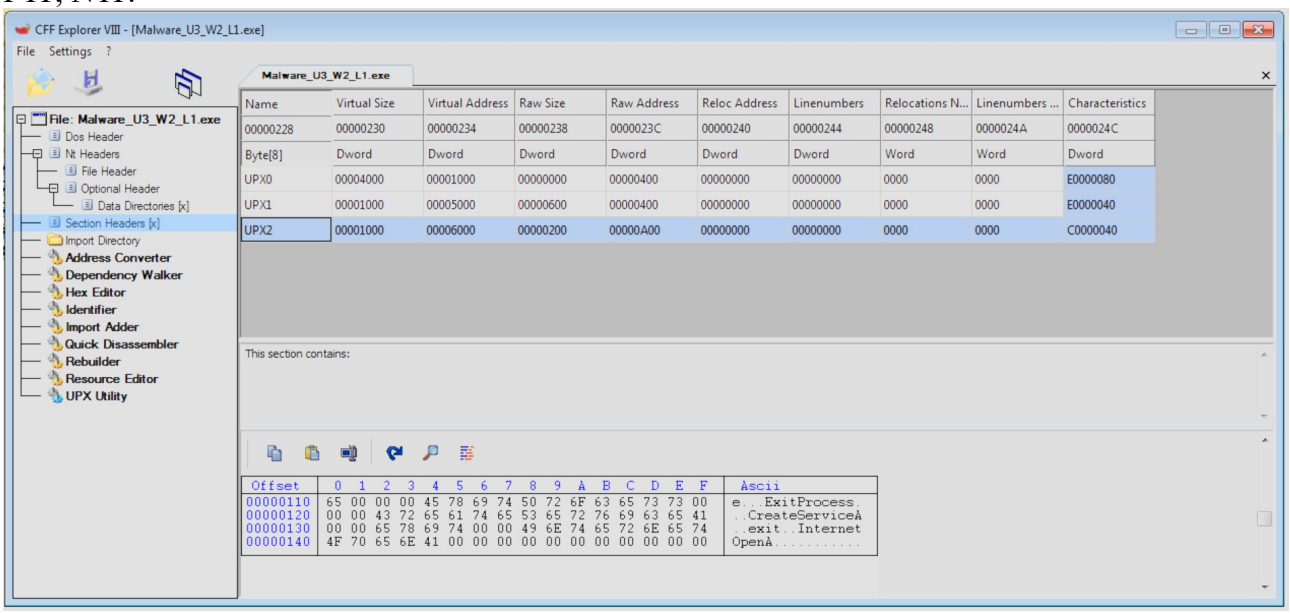
Andiamo ad analizzare il programma con la utility **cff explorer**.
All'interno del malware andiamo a visualizzare le **librerie** importate.



Vediamo che le librerie sono:
kernel32.dll – si occupa principalmente di interagire con il sistema operativo, contiene funzioni, ad esempio, per poter manipolare i gile e gestire la memoria

advapi32.dll – contiene le funzioni per interagire con i servizi ed i registri del sistema operativo,

msvcrt.dll – contiene funzioni per la manipolazione di stringhe, allocazione della memoria e altro come chiamate per input/output, come nel linguaggio C,
winnet.dll – contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.



Nella sezione header del file possiamo individuare 3 sezioni con i nomi nascosti.
Difficilmente possiamo andare a capire di che virus si tratti solo dall'analisi statistica