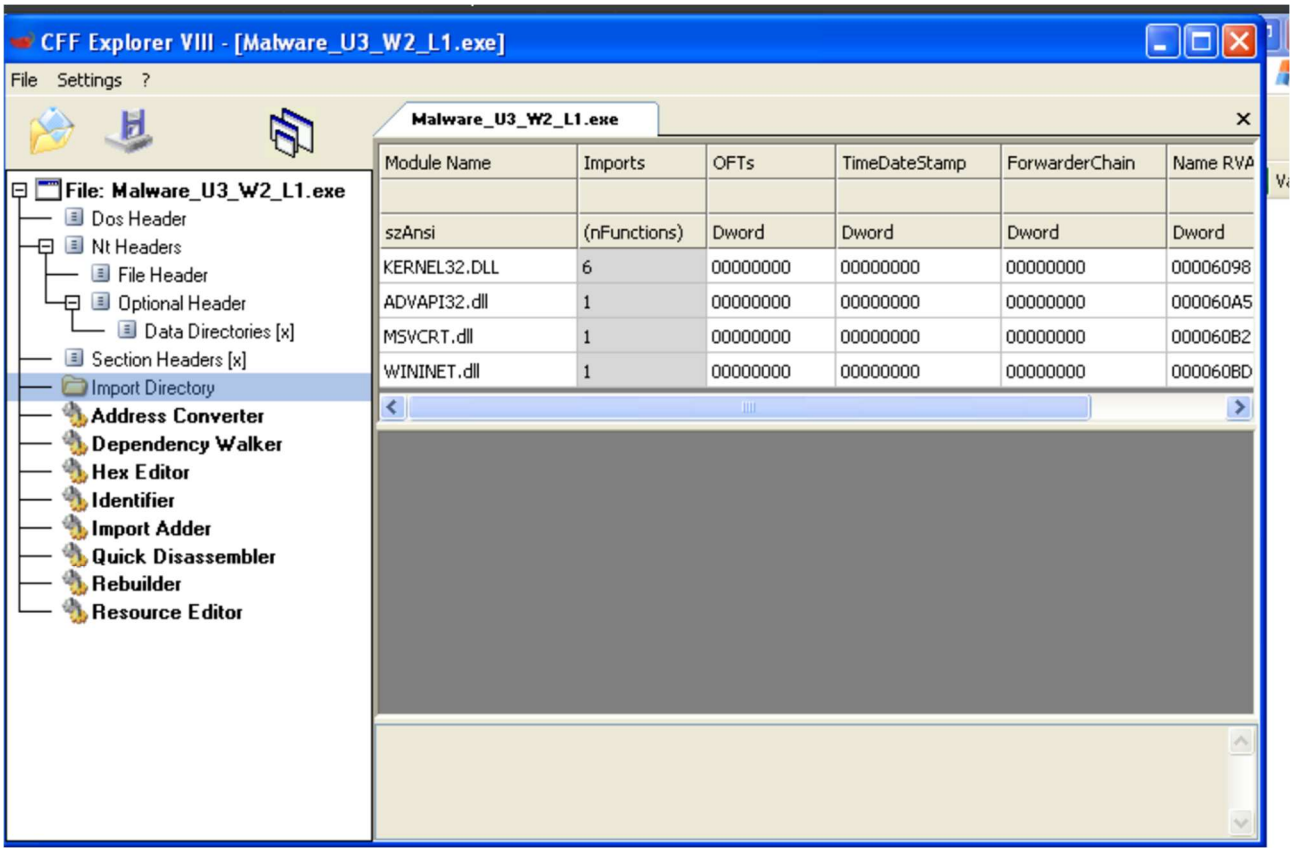
Esercizio S10-L1

Nell’esercizio di oggi era necessario analizzare un file (un malware fornitoci) utilizzando CFF explorer.



Le librerie riscontrabili sono: KERNEL32.dll, ADVAPI32.dll, MSVCRT.dll, WININET.dll.

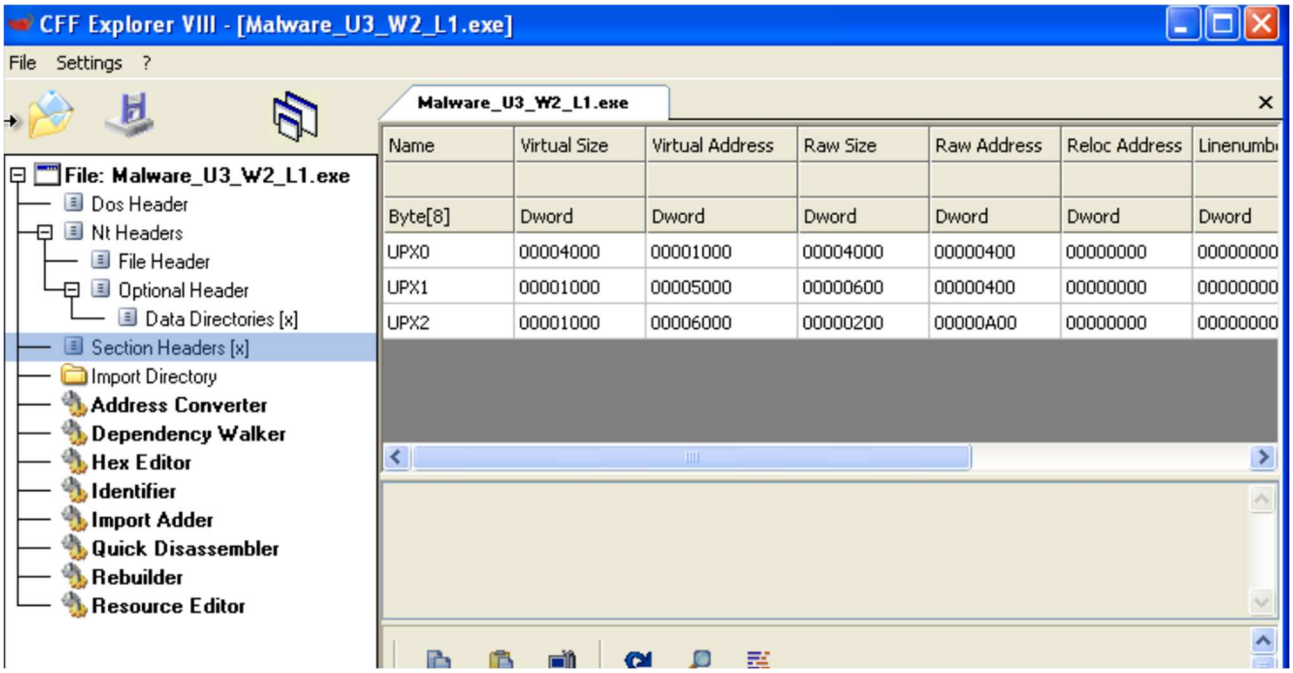
KERNEL32.dll contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

ADVAPI32.dll contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

MSVCRT.dll contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C

WININET.dll contiene le funzioni per l’implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Per vedere le sezioni basta andare, sempre su CFF, su Section headers:



Le sezioni sono compresse in formato UPX.

Si può decomprimerle con exeinfoPE, facendo cosi e poi riaprendo il file da CFF explorer si può notare che al posto di UPX0, UPX1, UPX2 ci sono .text, .rdata, .data.