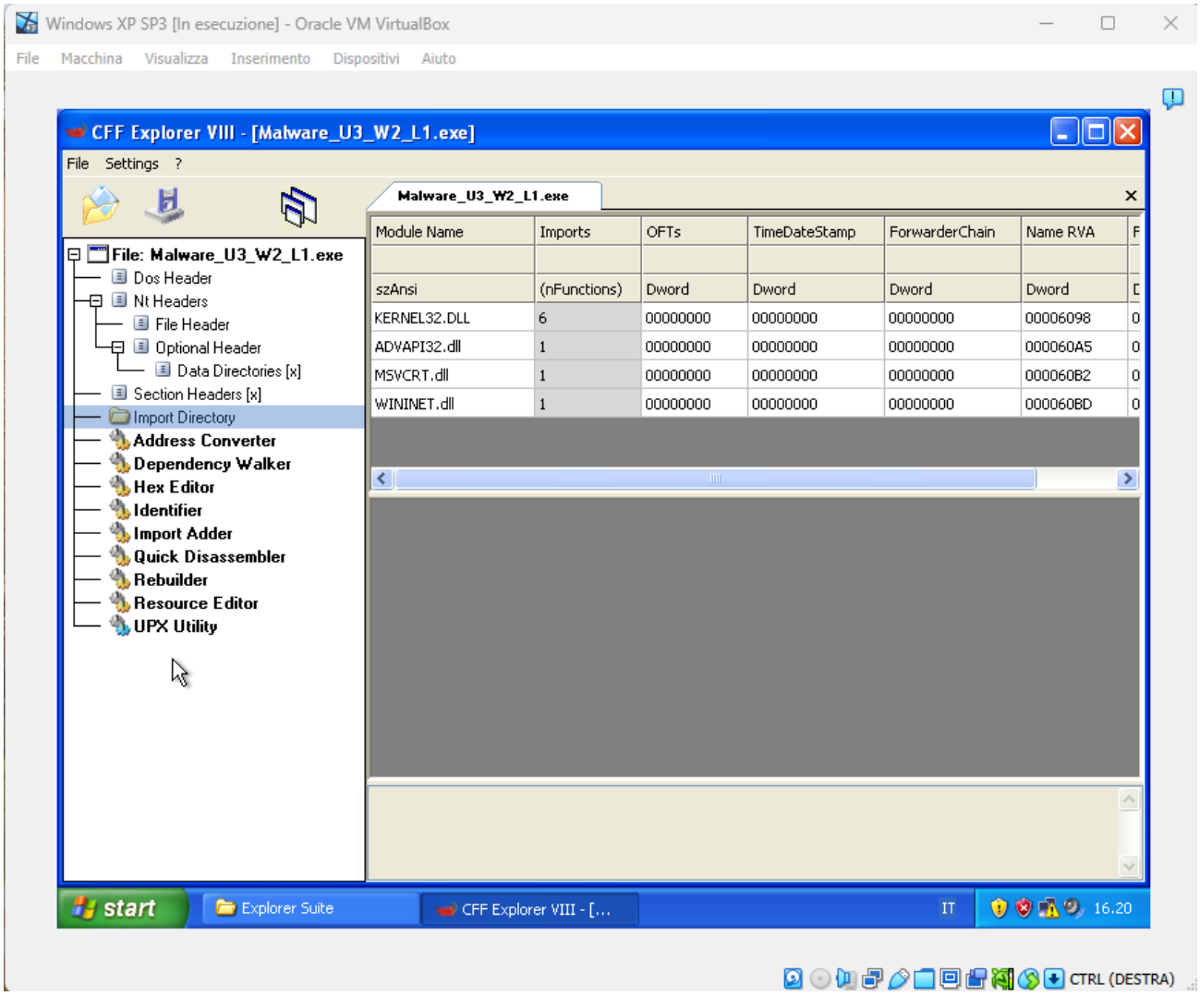
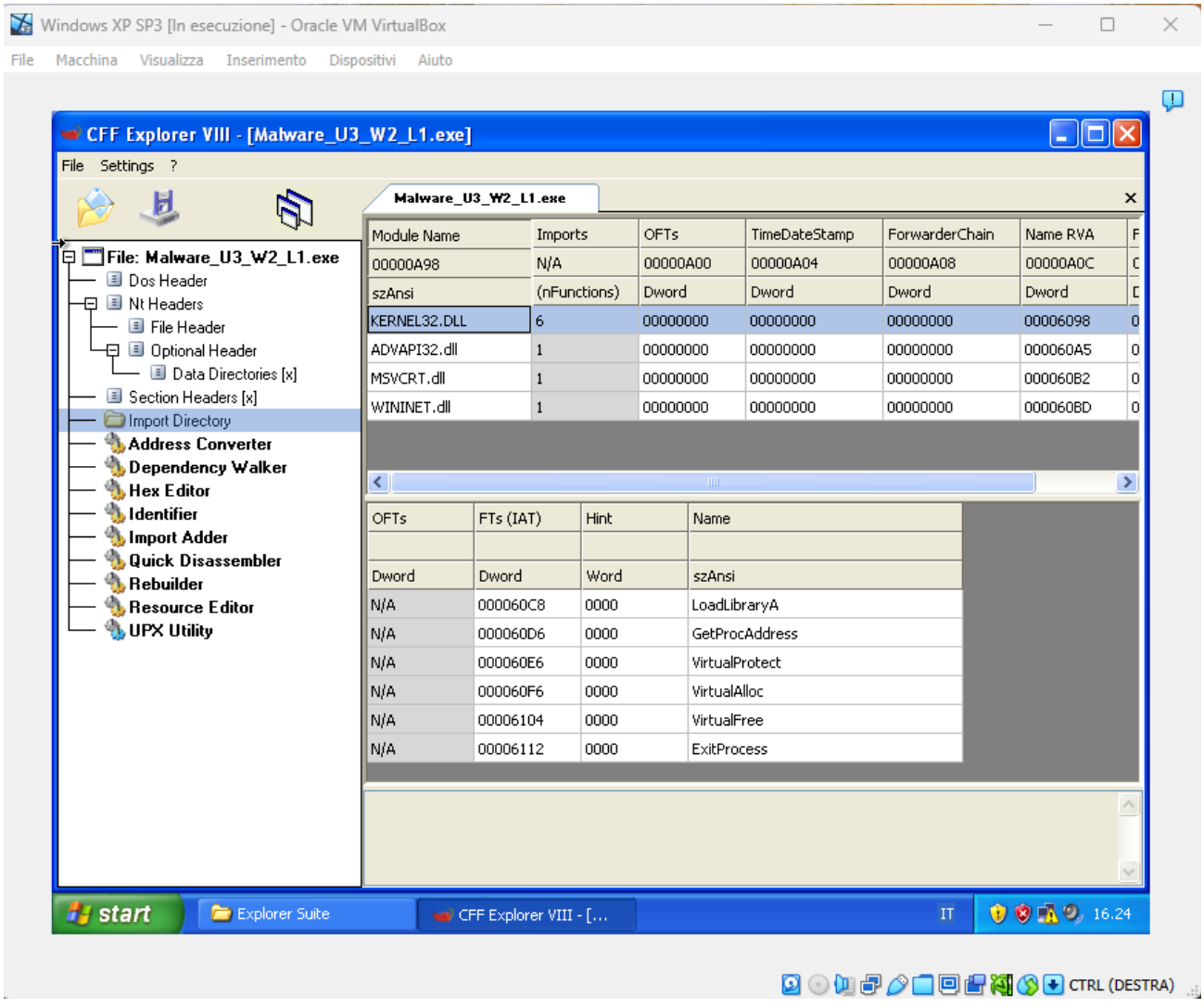
MALWARE ANALYSIS
ANALISI STATICA BASICA

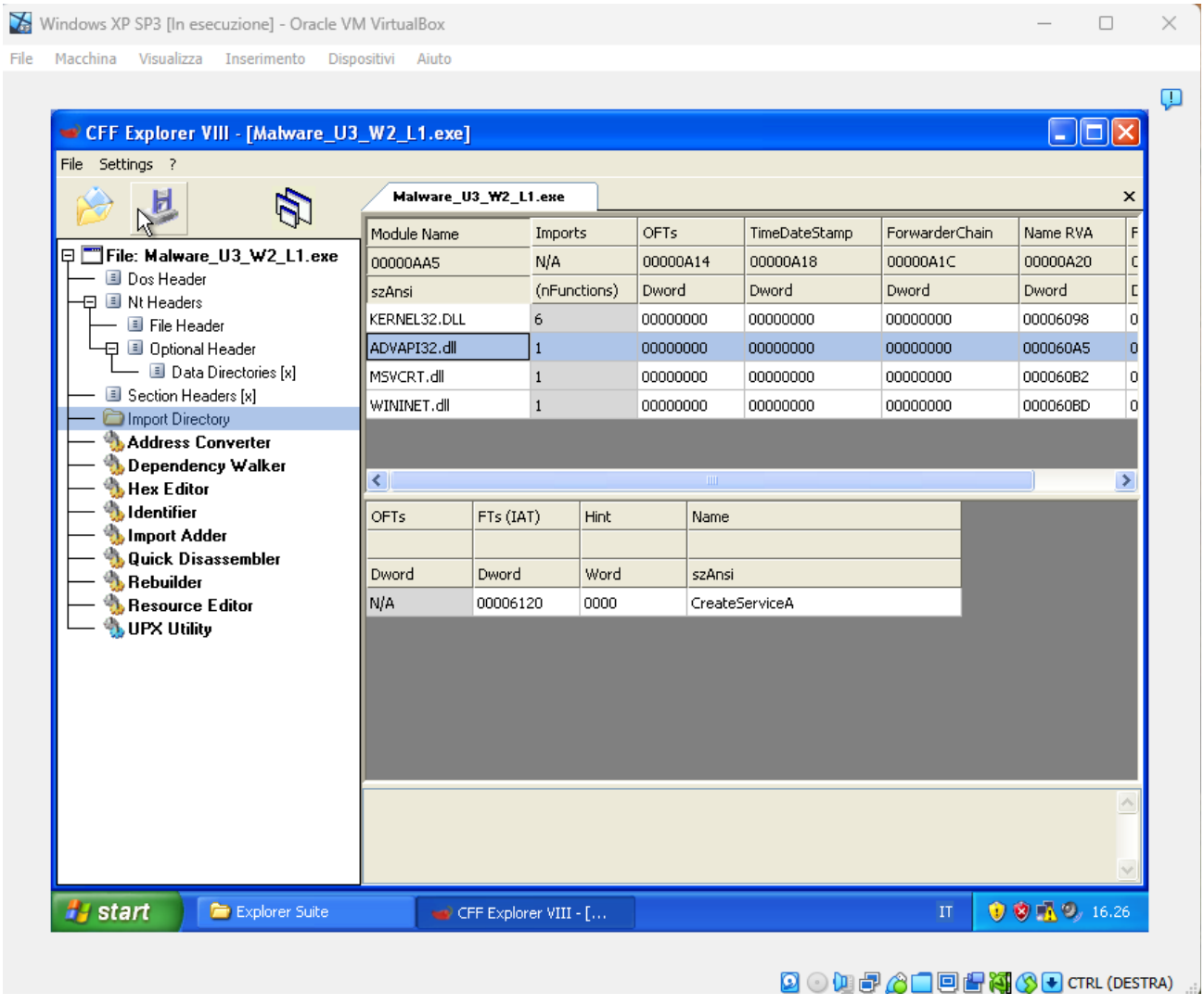
L’esercizio odierno serve ad avviarsi nella pratica dell’analisi dei malware (software malevoli) e per questo compito specifico utilizzo su una macchina virtuale Windows XP il tool CFF Explorer, creato per controllare le funzioni importate ed esportate da un malware, ovvero i vari comandi che un file eseguibile elabora.



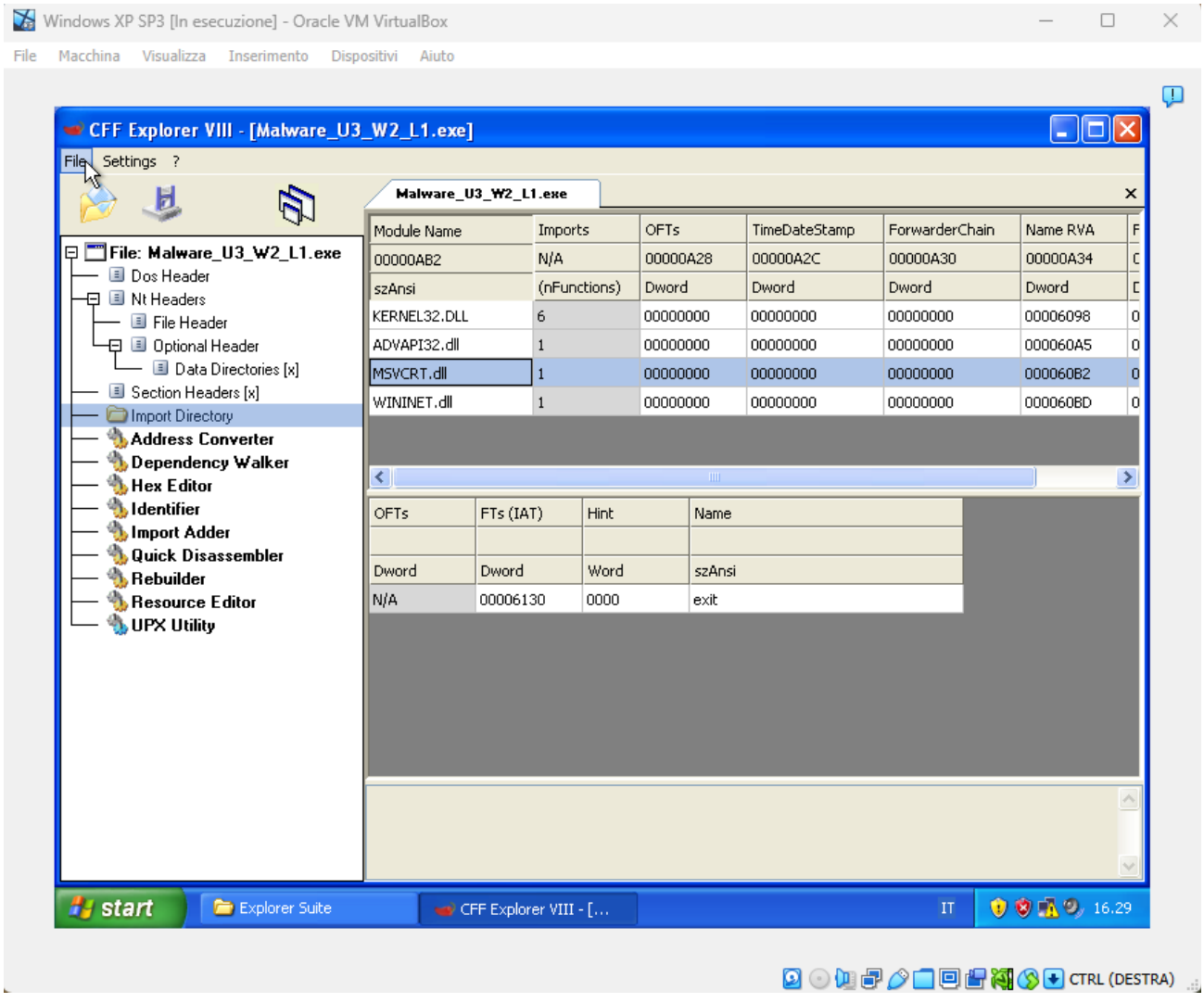
Una volta avviato CFF Explorer scegliamo il software malevolo da esaminare, spostandoci poi sulla voce “Import Directory” possiamo visionare le librerie importate (sulla finestra dx in alto), e voce per voce (in basso a sx) le funzioni richieste per ogni libreria.



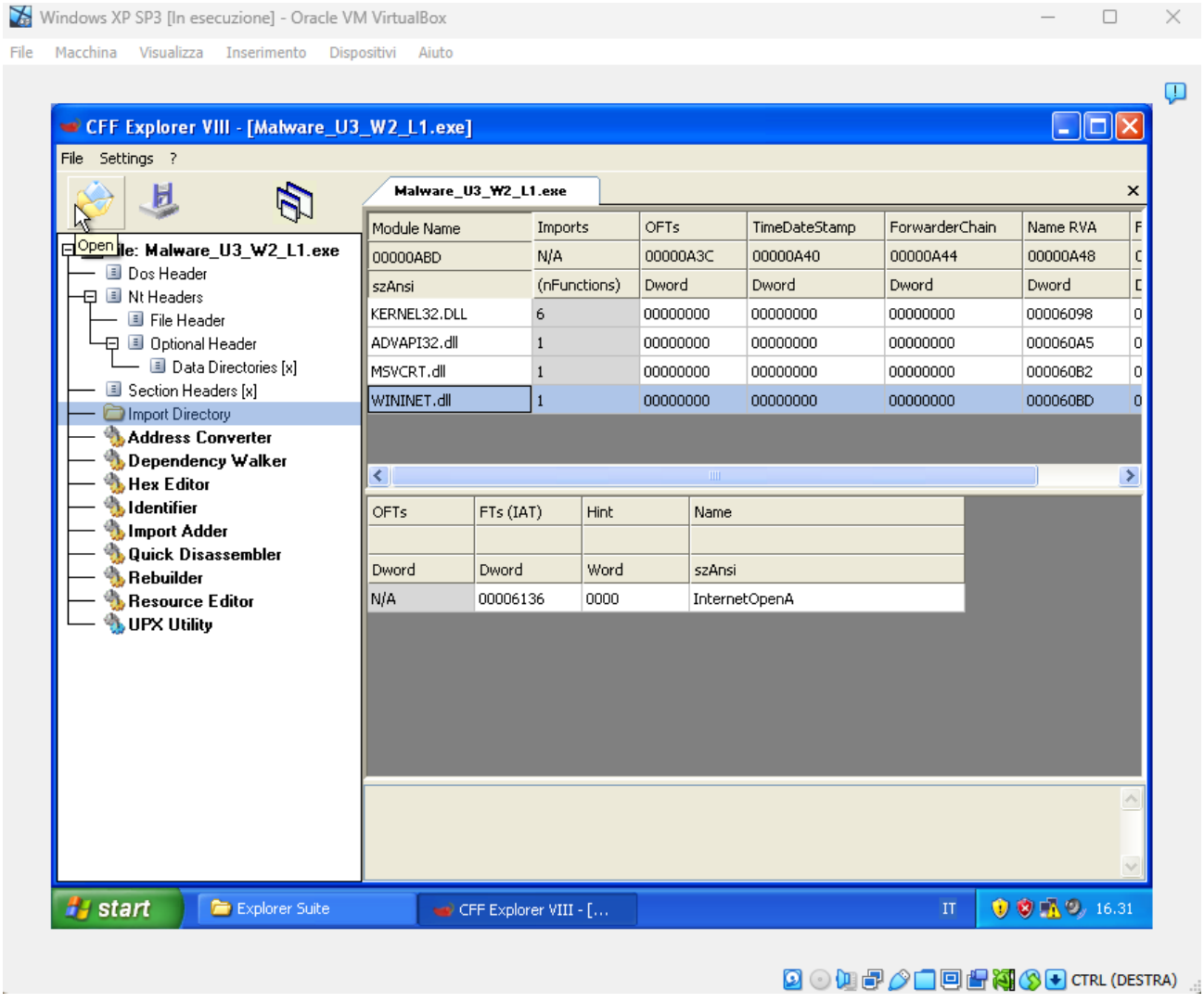
Kernel32.dll serve ad interagire con il sistema operativo.



Advapi32.dll serve per interagire con i servizi ed i registri, ossia i processi e le memorie principali.

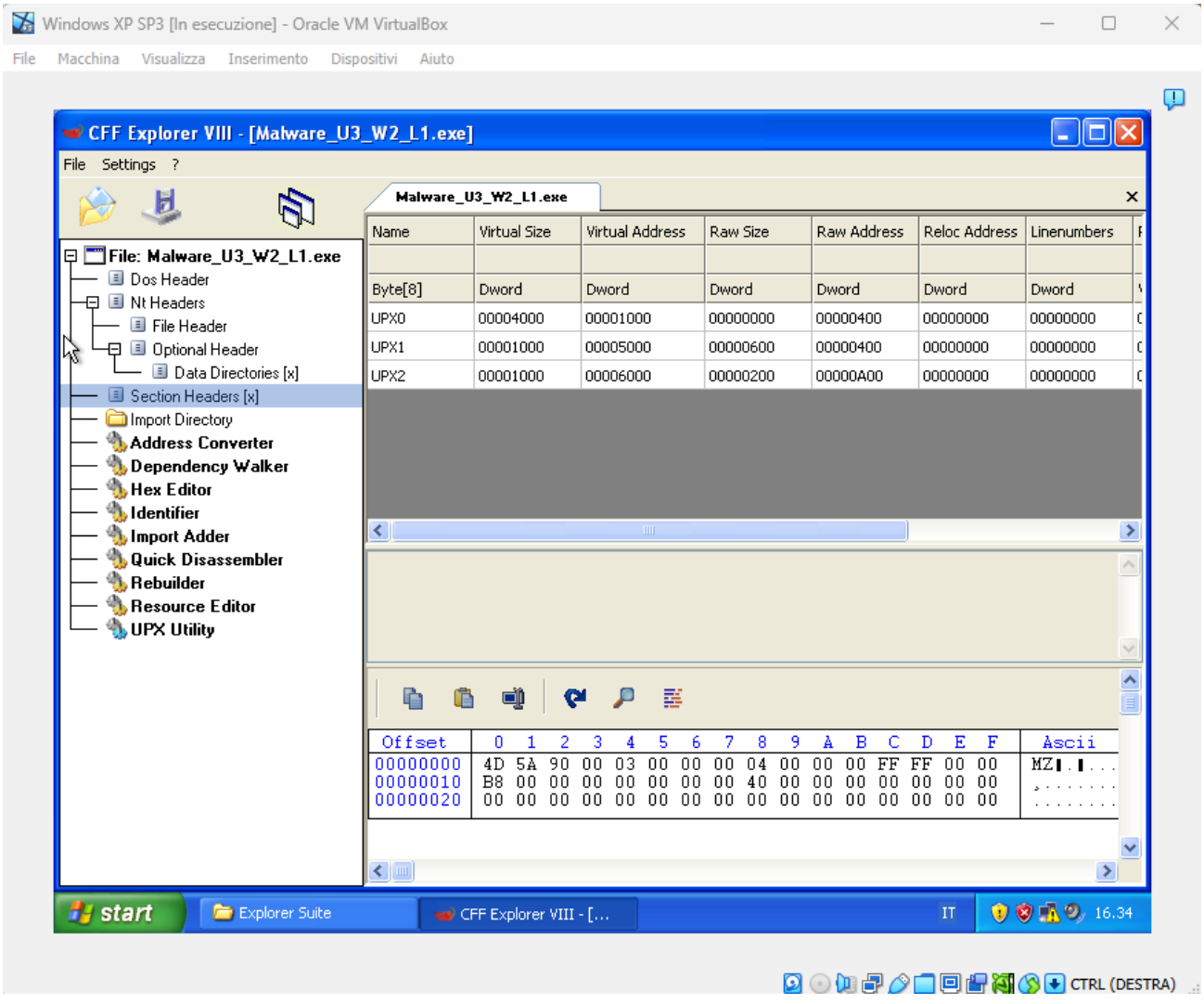


Msvcrt.dll serve a manipolare stringhe, allocazione memoria ed altro.

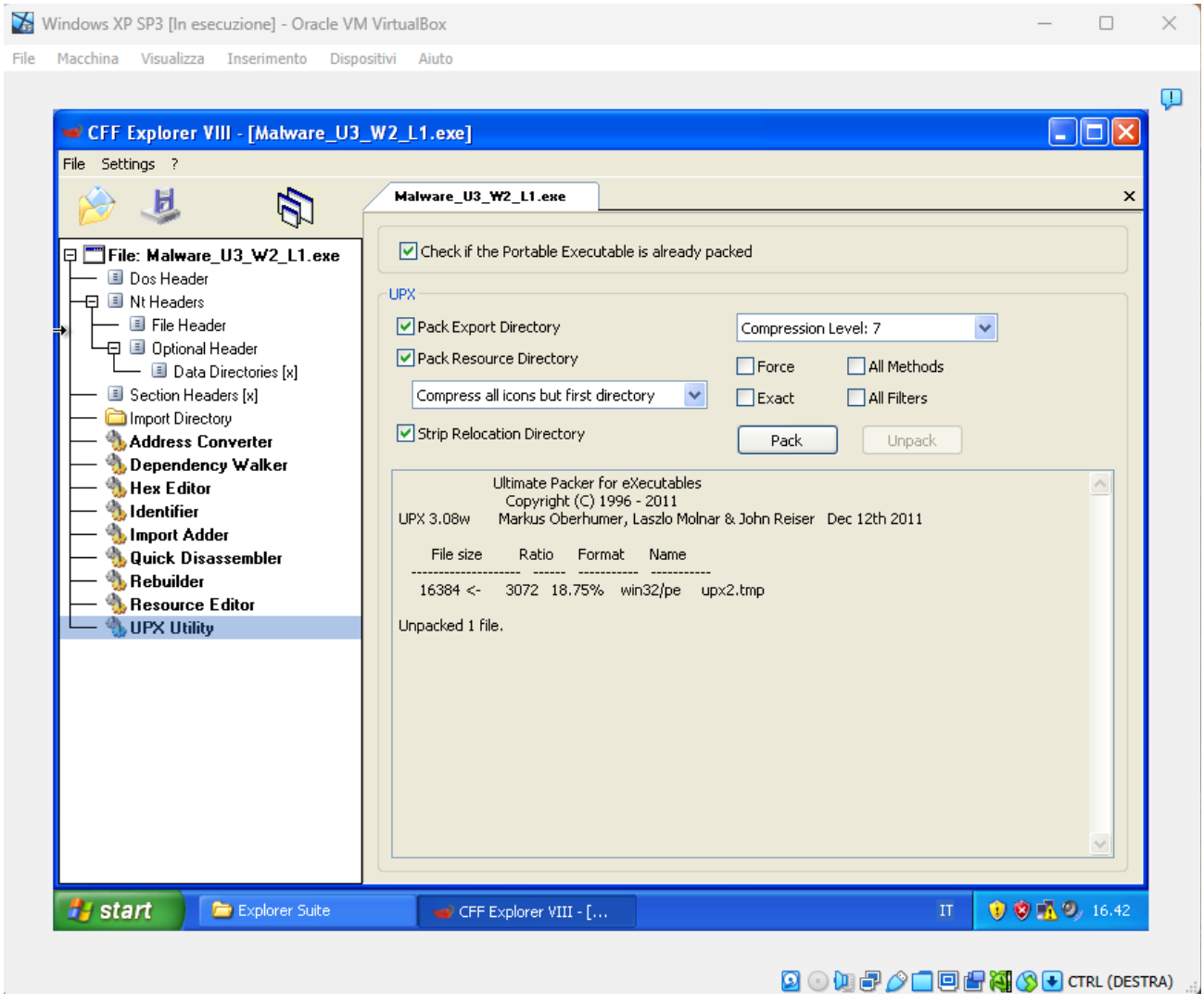


Wininet.dll contiene funzioni per alcuni dei protocolli di rete.

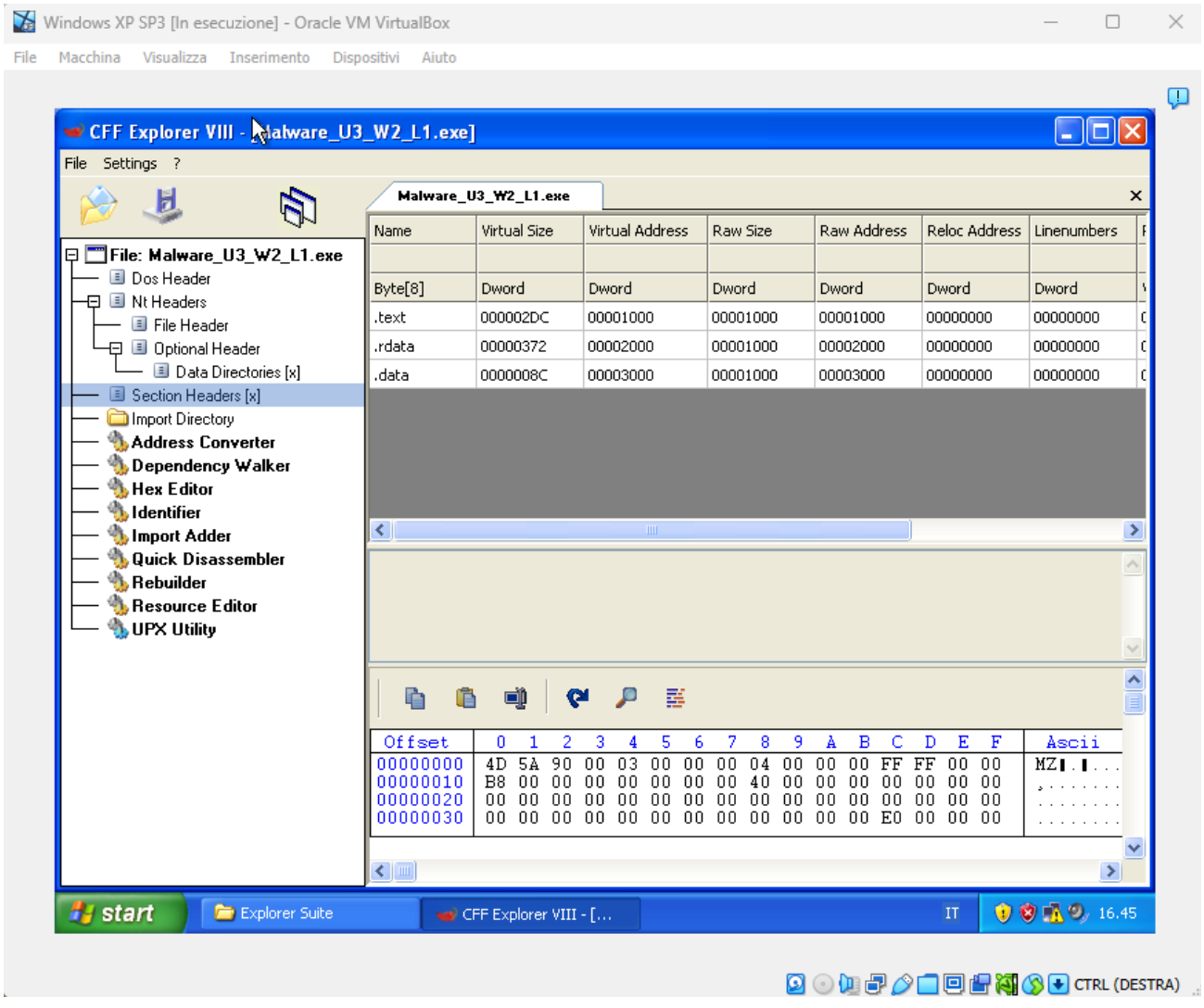
Spostandoci su “Section Headers” invece possiamo visionare altre informazioni, come ad esempio le sezioni che compongono il malware.



In questo caso notiamo 3 file UPX, che sono dei file compressi.



Tramite la sezione “UPX Utility” possiamo decomprimerli.



Notiamo quindi adesso 3 estensioni, .text che contiene le righe di codice che la CPU eseguirà all'avvio del software, .rdata include le librerie e le funzioni importate ed esportate dall'eseguibile ed infine .data che contiene i dati e le variabili globali del programma eseguibile, globali perché non fanno parte di un singolo contesto di una funzione, ma accessibili da qualsiasi funzione all'interno dell'eseguibile.

Ne possiamo quindi dedurre che si tratta di un software molto pericoloso poiché collegato al kernel del sistema operativo e quindi lavora nelle fondamenta del dispositivo infetto, ed avendo istruzioni di collegamento in rete probabilmente potrebbe inviare dati all'esterno come ad esempio un keylogger, o anche creare un ingresso secondario come un RAT (backdoor a scopi malevoli) per permettere all'attaccante di entrare a suo piacimento nella macchina.