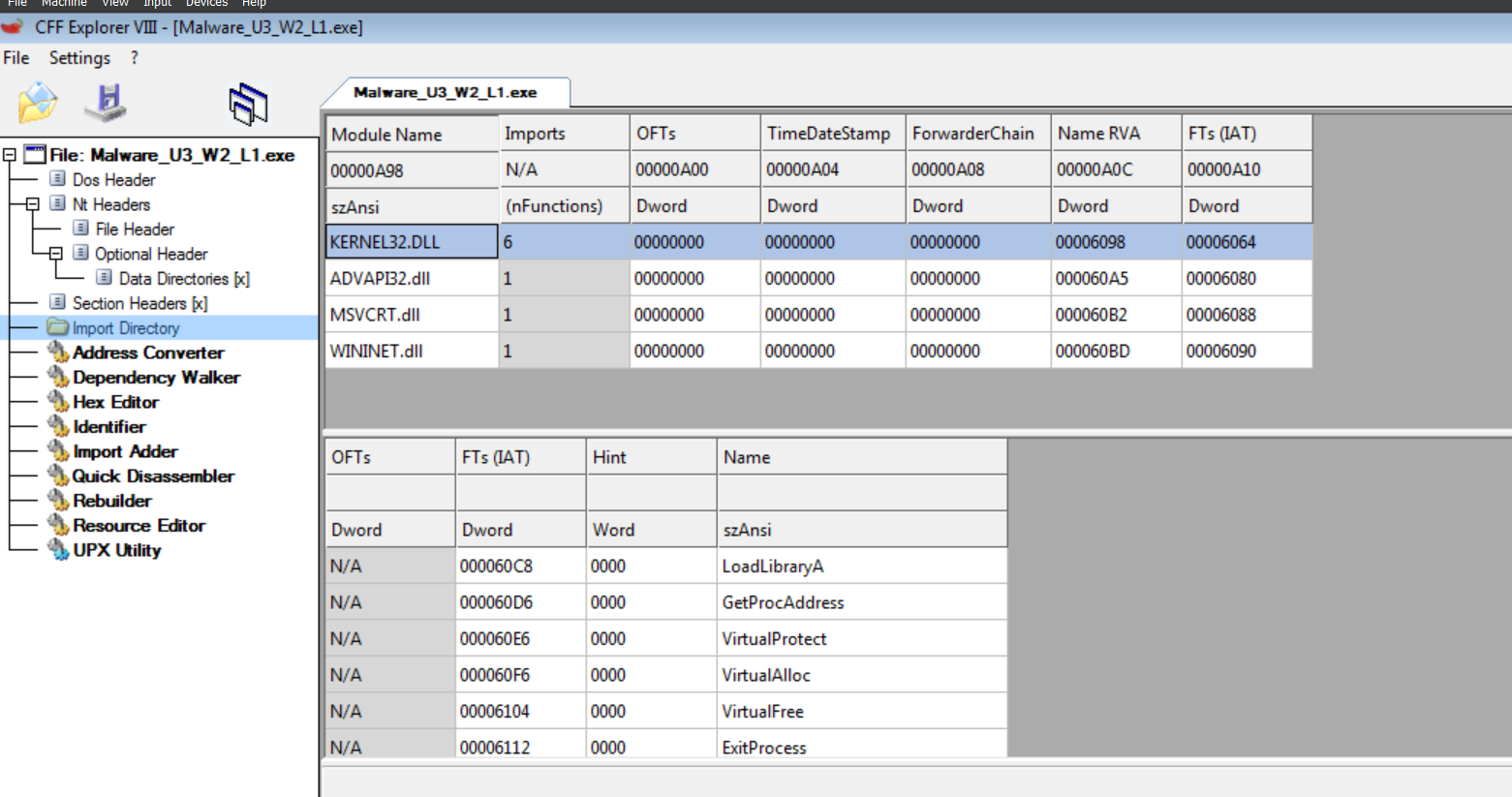
**Analisi statica Basica**

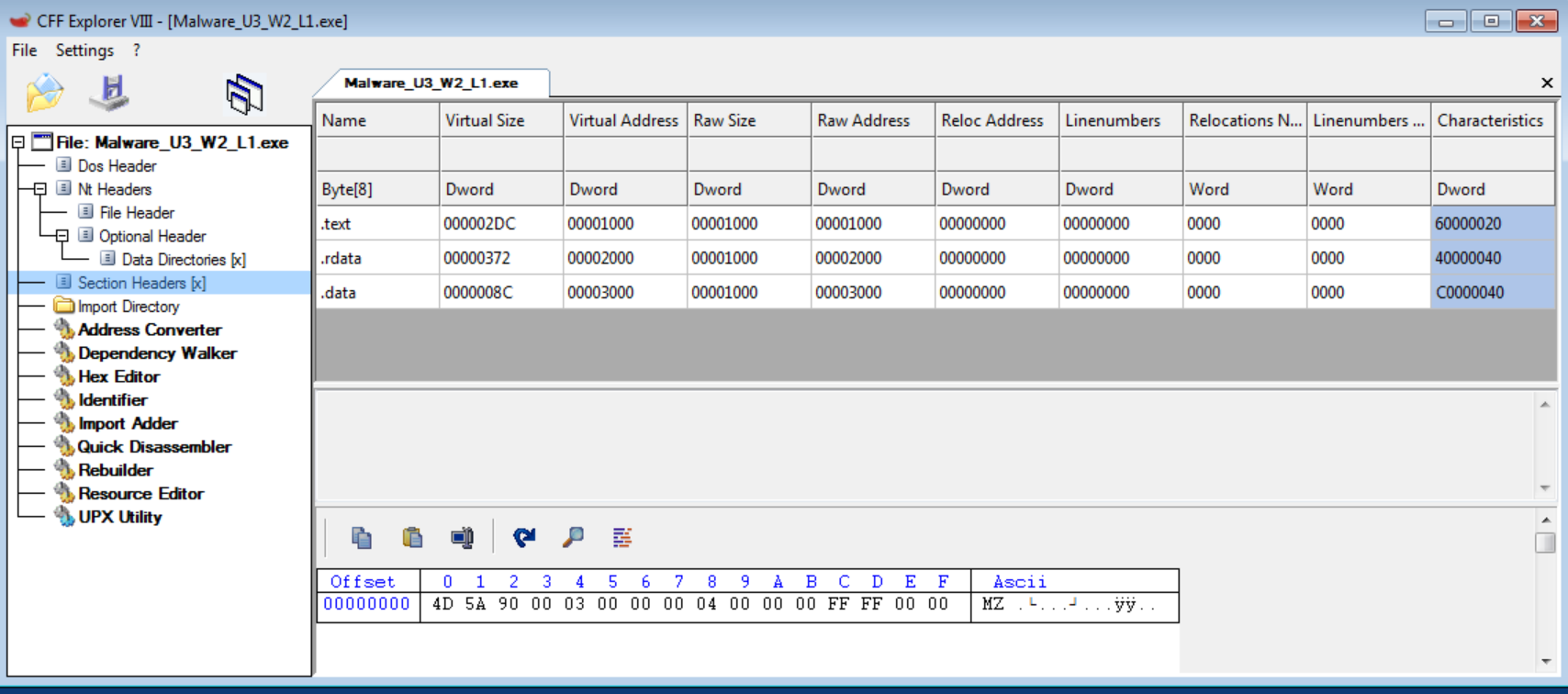
Traccia: Con riferimento al file eseguibile contenuto nella cartella «Esercizio\_Pratico\_U3\_W2\_L1» presente sul Desktop della vostra macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti:

* Indicare le librerie importate dal malware, fornendo una descrizioneper ognuna di esse
* Indicare le sezionidi cui si compone il malware, fornendo una descrizioneper ognuna di essa
* Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.



Dallo screenshot, possiamo vedere alcune informazioni riguardanti le librerie importate dal malware e le sezioni del file eseguibile:

* **KERNEL32.DLL**: Questa è una libreria fondamentale di Windows che contiene funzioni di base per la gestione della memoria, delle operazioni di input/output e dei processi. La presenza di questa libreria è comune in molti eseguibili perché fornisce funzioni di base necessarie per qualsiasi programma Windows.
* **ADVAPI32.DLL**: Questa libreria fornisce funzioni relative alla sicurezza, al registro di sistema e ai servizi di Windows. L'utilizzo di questa libreria potrebbe indicare che il malware ha funzionalità per manipolare i servizi o le impostazioni di sicurezza del sistema.
* **MSVCRT.DLL**: È la libreria standard C di Microsoft, utilizzata per fornire funzionalità di base del linguaggio C come manipolazione di stringhe, matematica e altre funzioni standard.
* **WININET.DLL**: Questa libreria è usata per le funzionalità di rete basate su Internet. La presenza di WININET.DLL potrebbe indicare che il malware è in grado di comunicare su internet o di eseguire operazioni di rete come il download o l'upload di dati.



Mentre per le sezioni di cui si compone il malware possiamo fornire le seguenti informazioni:

* **.text**: Contiene il codice eseguibile del programma.
* **.rdata**: Include dati di sola lettura, come stringhe costanti e import tables.
* **.data**: Destinata a contenere dati inizializzati e variabili globali.

**Considerazione finale**: Sulla base delle informazioni visualizzate in CFF Explorer, questo malware sembra avere caratteristiche di persistenza, capacità di manipolare il sistema e di comunicare con l'esterno. Queste azioni sono probabilmente parte di una strategia per mantenere l'accesso al sistema, celare la sua presenza e possibilmente eseguire compiti malevoli senza il consenso dell'utente.