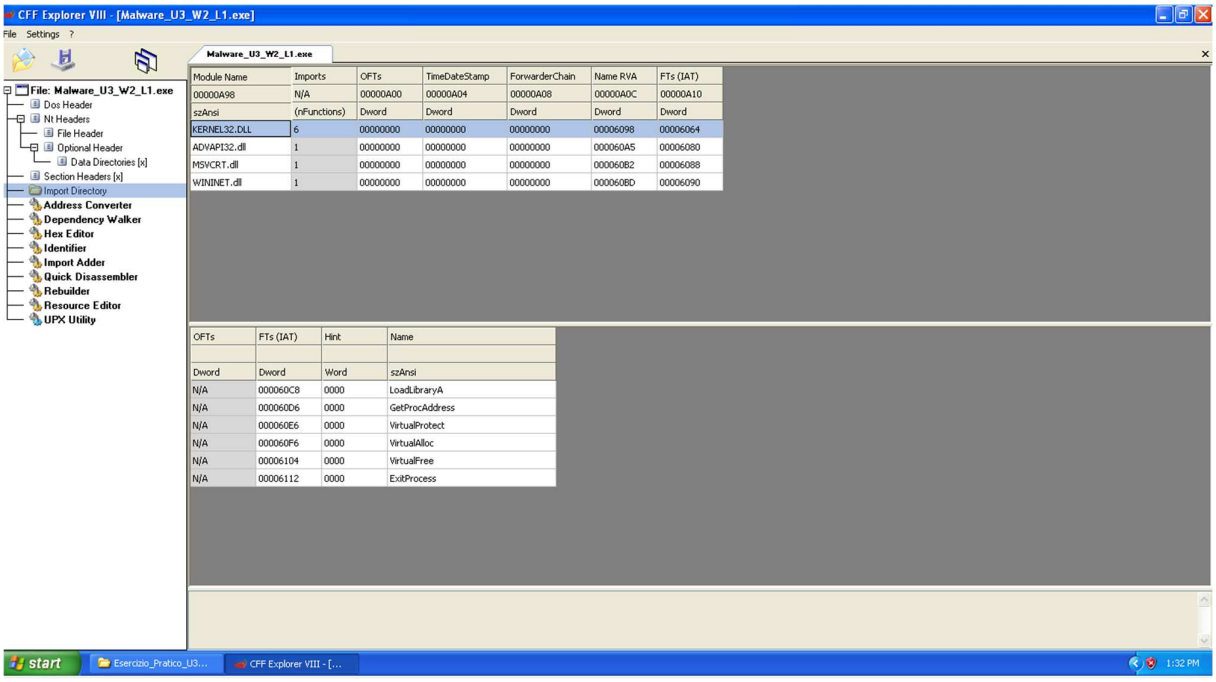
ESERCIZIO S10-L1

Lo scopo dell'esercizio di oggi è quello di analizzare un malware presente nella cartella "Esercizio_Pratico_U3_W2_L1" nella macchina virtuale e rispondere ai seguenti quesiti:

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

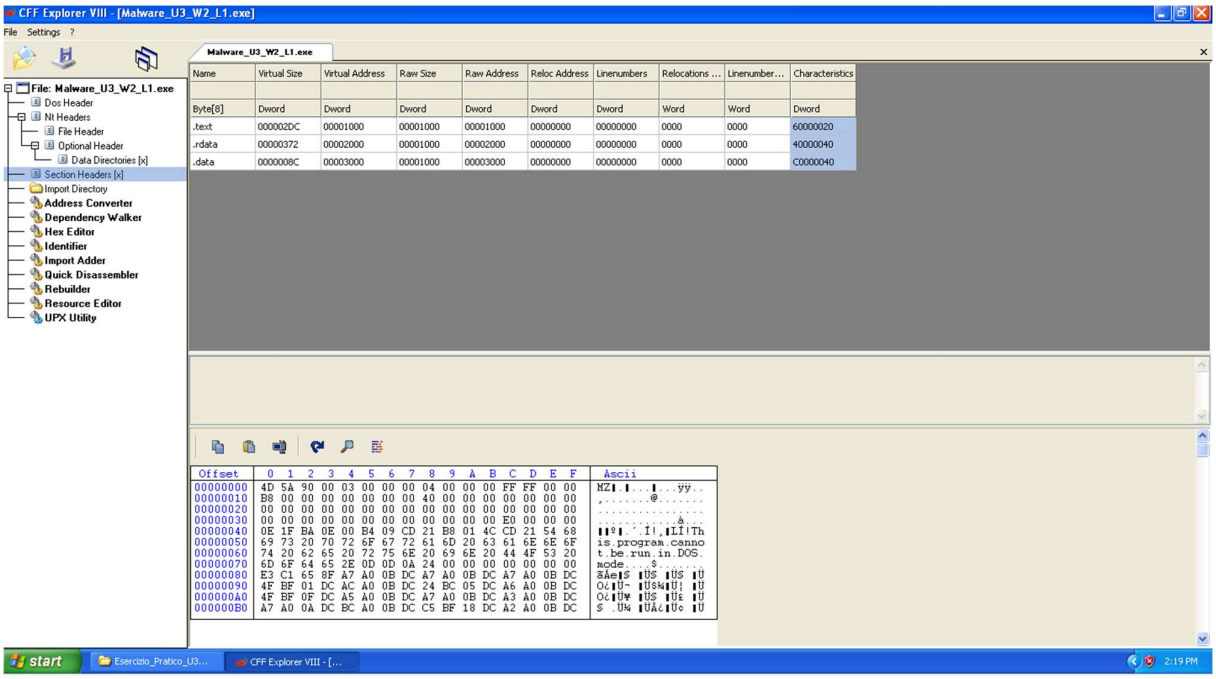
Per vedere le librerie importate dal malware ho usato un tool installato nella macchina virtuale, cioè "CFF explorer" utile per l'analisi dei malware. Caricando il file eseguibile si hanno le varie informazioni. Per quanto riguarda le librerie importate, quest'ultime sono:

- Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio la manipolazione dei file, la gestione della memoria.
- Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo.
- Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.
- MSVCRT.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro.



Le sezioni di cui si compone il malware sono: UPX0, UPX1, UPX2. si riferiscono a diversi livelli di compressione applicabili tramite UPX su un file eseguibile. UPX è uno strumento utilizzato per comprimere ed eseguire la decompressione di file eseguibili in vari formati. Quindi avranno utilizzato la compressione per nascondere le sezioni, per decomprimerle ho cliccato sull'opzione "UPX utility" e poi su "unpack" e sono venute fuori le sezioni:

- .text: contiene le righe di codice che la CPU eseguirà una volta che il software sarà avviato. Questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.
- .rdata: include generalmente le informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile.
- .data: contiene tipicamente i dati, le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.



Un ulteriore analisi che si può fare è quella di ricavare l'hash del file e verificarlo su "VirusTotal", quest'ultimo ci dice che si tratta di un trojan, ovvero un malware che si nasconde in file innoqui che si attiva quando la vittima apre il file.