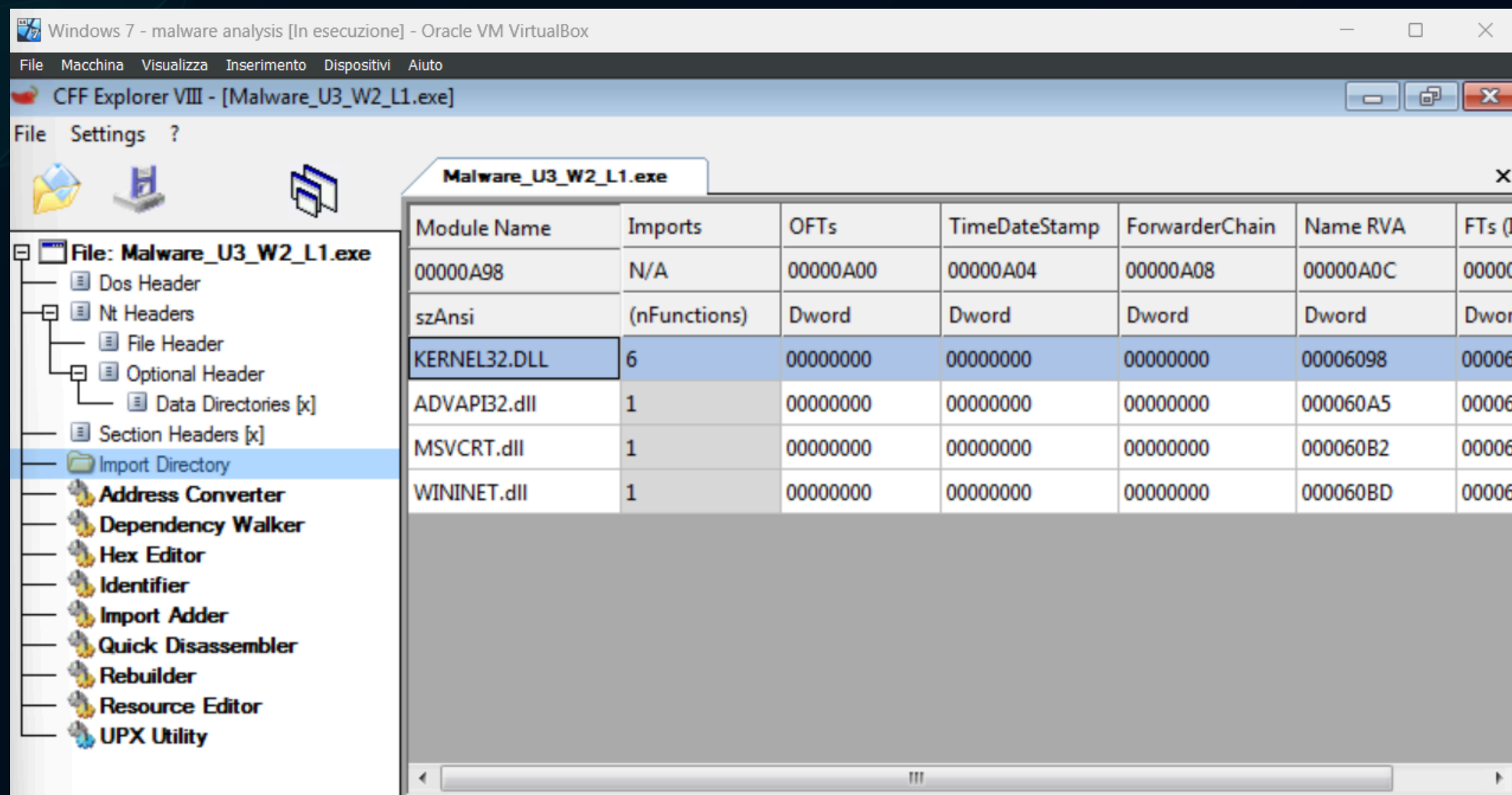


# REPORT S10-L1

Kernel32.dll è una libreria dinamica fondamentale per il sistema operativo Windows. Essa fornisce un'interfaccia tra le applicazioni e il kernel del sistema operativo, offrendo una vasta gamma di funzioni per gestire operazioni di basso livello come:

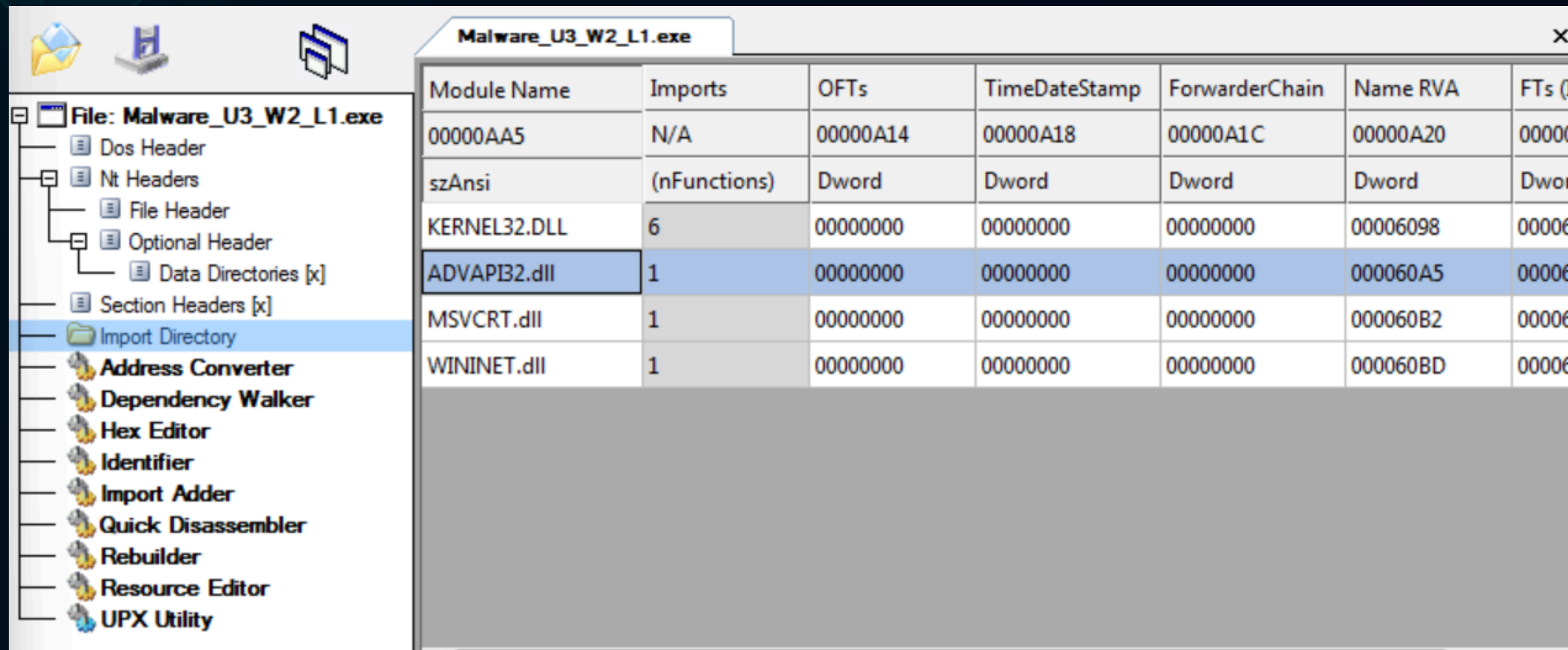
- Gestione della memoria: allocazione, deallocazione, protezione della memoria.
- Input/Output: gestione dei file, operazioni di lettura/scrittura, accesso al disco.
- Processi e thread: creazione, terminazione, sincronizzazione, gestione dei processi e dei thread.
- Gestione del tempo: timer, sleep, wait.
- Interazione con il sistema operativo: informazioni sul sistema, gestione degli errori, registrazione eventi.



ADVAPI32.dll è un'altra libreria dinamica fondamentale per il sistema operativo Windows. A differenza di kernel32.dll, che offre funzionalità di base, ADVAPI32.dll fornisce un livello più avanzato di accesso al sistema operativo.

Funzionalità principali di ADVAPI32.dll:

- Sicurezza: Gestione degli utenti, gruppi, politiche di sicurezza, controllo degli accessi.
- Registro di sistema: Accesso e manipolazione delle chiavi e dei valori del registro.
- Servizi di sistema: Controllo dei servizi in esecuzione, creazione, installazione e disinstallazione dei servizi.
- Eventi: Generazione e registrazione di eventi di sistema.



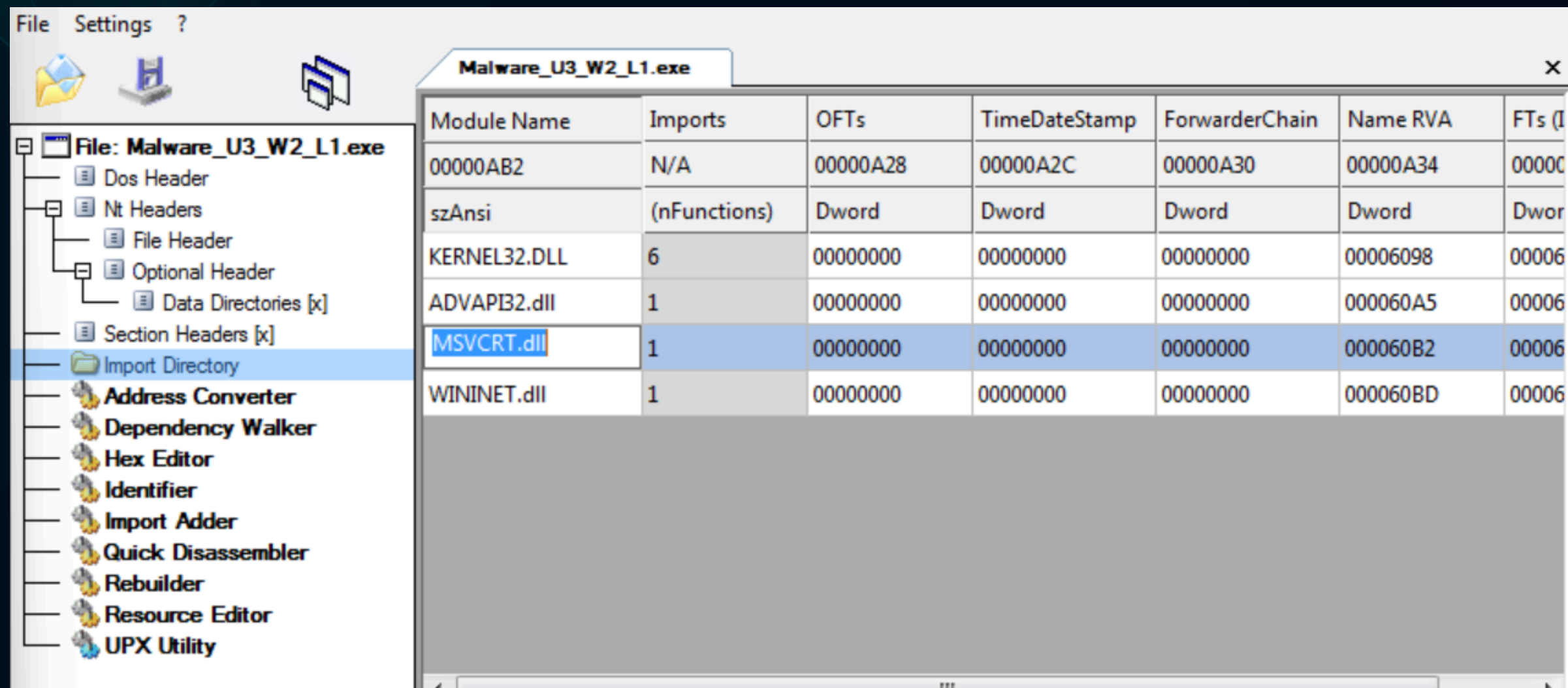
Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (I
00000AA5	N/A	00000A14	00000A18	00000A1C	00000A20	00000
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dwor
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006
WININET.dll	1	00000000	00000000	00000000	000060BD	00006



MSVCRT.dll (Microsoft Visual C++ Runtime Library) è una libreria dinamica fondamentale per l'esecuzione di applicazioni sviluppate con il compilatore Microsoft Visual C++. Contiene un insieme di funzioni di base per la gestione della memoria, input/output, matematica, stringhe e altre operazioni comuni.

### Funzioni principali di MSVCRT.dll

- Gestione della memoria: allocazione e deallocazione di memoria, gestione dei puntatori.
- Input/output: operazioni di lettura e scrittura su file, console e altri dispositivi.
- Matematica: funzioni matematiche di base come seno, coseno, esponenziali, logaritmi.
- Stringhe: manipolazione di stringhe, confronto, ricerca, conversione.



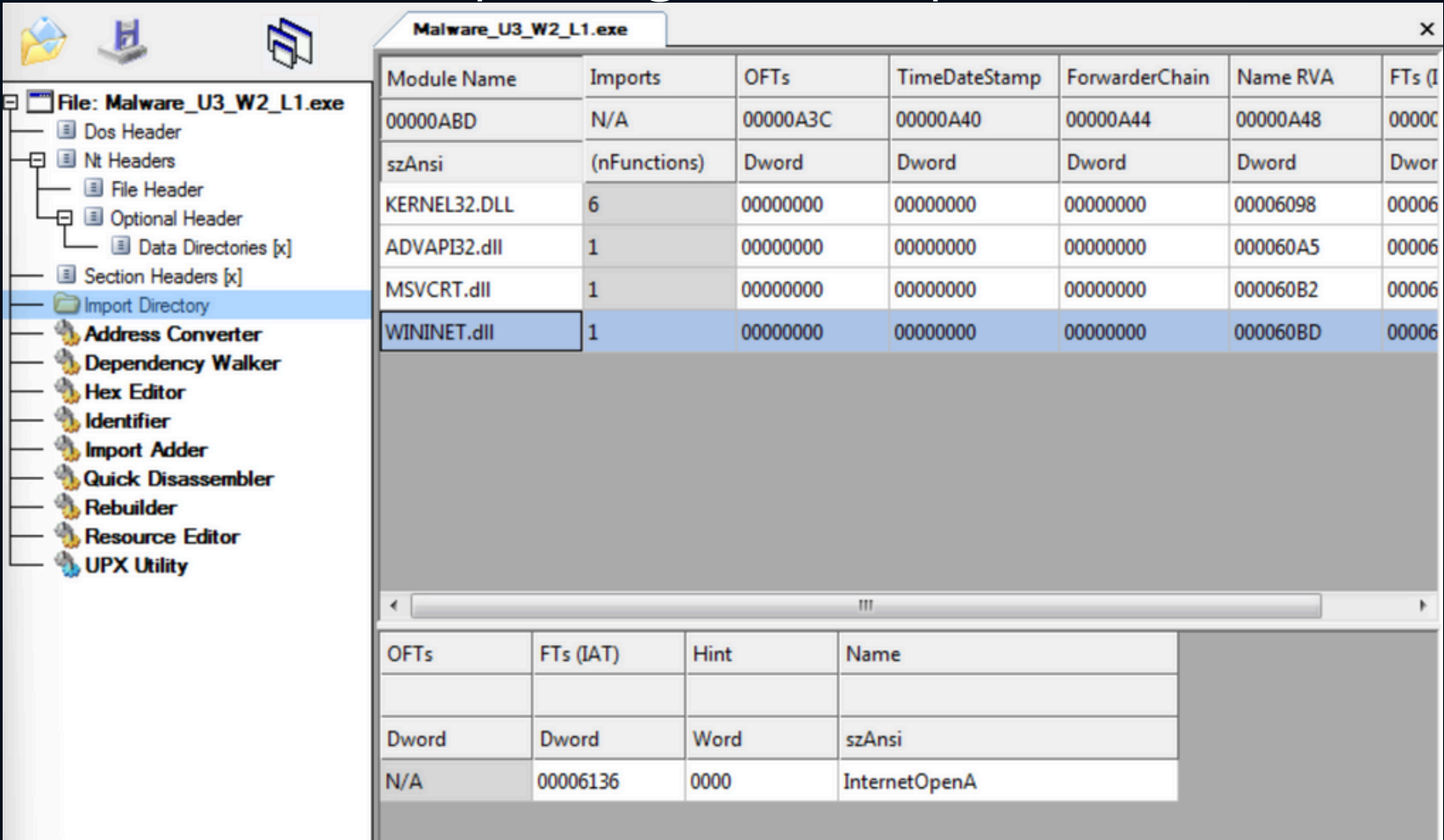
The screenshot shows a PE Explorer window titled "Malware\_U3\_W2\_L1.exe". The left sidebar displays the file structure, with "Import Directory" selected. The main pane shows a table of imported modules.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (I
00000AB2	N/A	00000A28	00000A2C	00000A30	00000A34	00000
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dwor
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006
WININET.dll	1	00000000	00000000	00000000	000060BD	00006

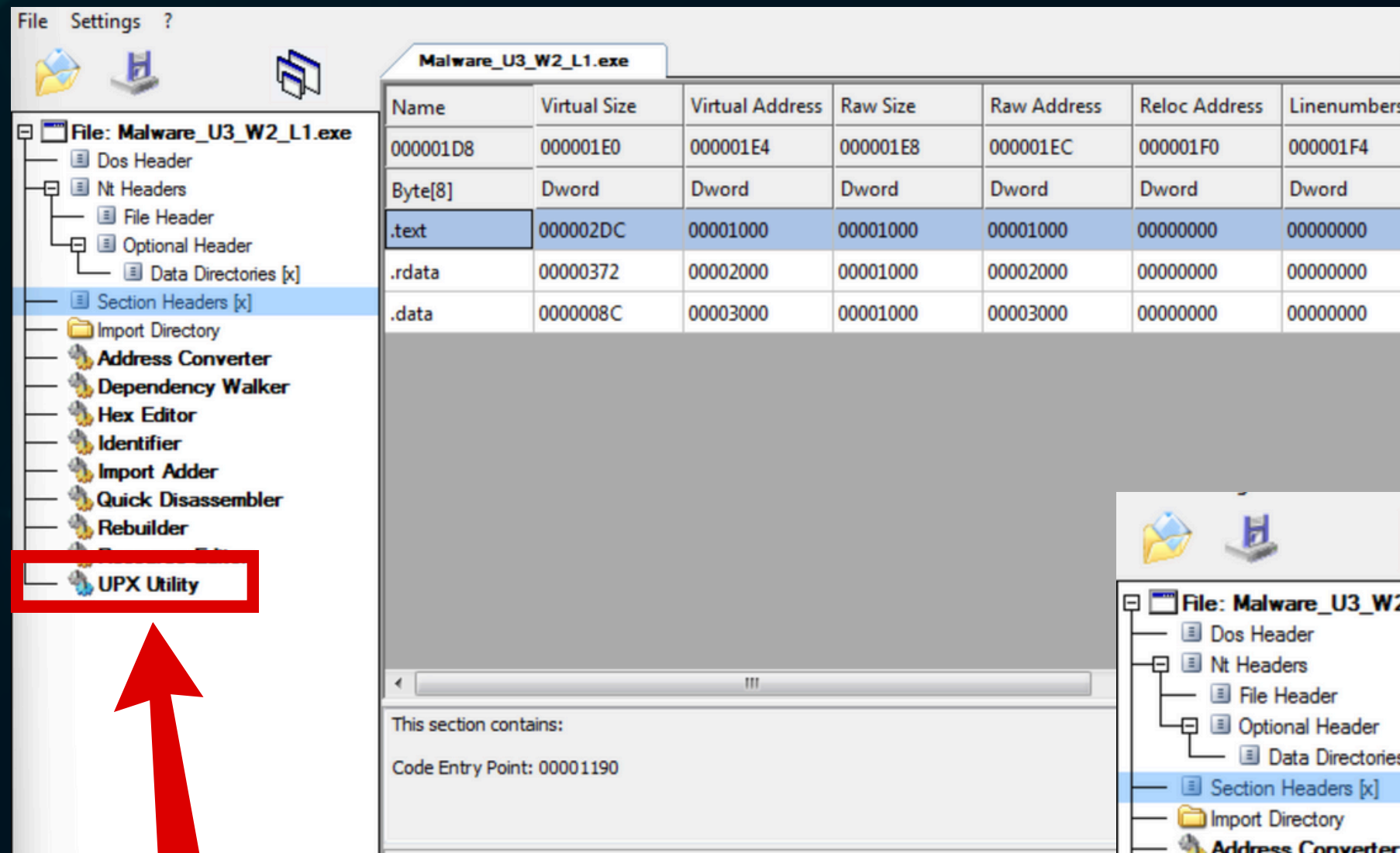
WININET.dll è una libreria dinamica fondamentale per le applicazioni Windows che necessitano di interagire con Internet. Essa fornisce un'interfaccia per accedere alle risorse web utilizzando i protocolli HTTP e FTP.

Funzionalità principali di WININET.dll

- HTTP e FTP: Gestisce le richieste e le risposte per i protocolli HTTP e FTP, consentendo il download e l'upload di file.
- Cookie: Supporta la gestione dei cookie, inclusi la creazione, la lettura e la scrittura.
- Autenticazione: Fornisce meccanismi di autenticazione per accedere a risorse protette.
- Proxy: Supporta la configurazione e l'utilizzo dei proxy per l'accesso alla rete.
- Cache: Gestisce la cache delle risorse web per migliorare le prestazioni.







Andando nella sezione UPX Utility è possibile fare l'unpack dei section headers così da leggerne il contenuto

Nella sezione .text sono contenute le istruzioni che verranno eseguite dalla CPU  
Nella sezione .rdata sono contenute le varie librerie  
Nella sezione .data sono contenute le variabili globali

