



**Francesco
Fuschetto**

MALWARE ANALYSIS

Progetto n°10



INCIPIIT

Obiettivi

Dato un file malevolo Malware_U3_W2-L5

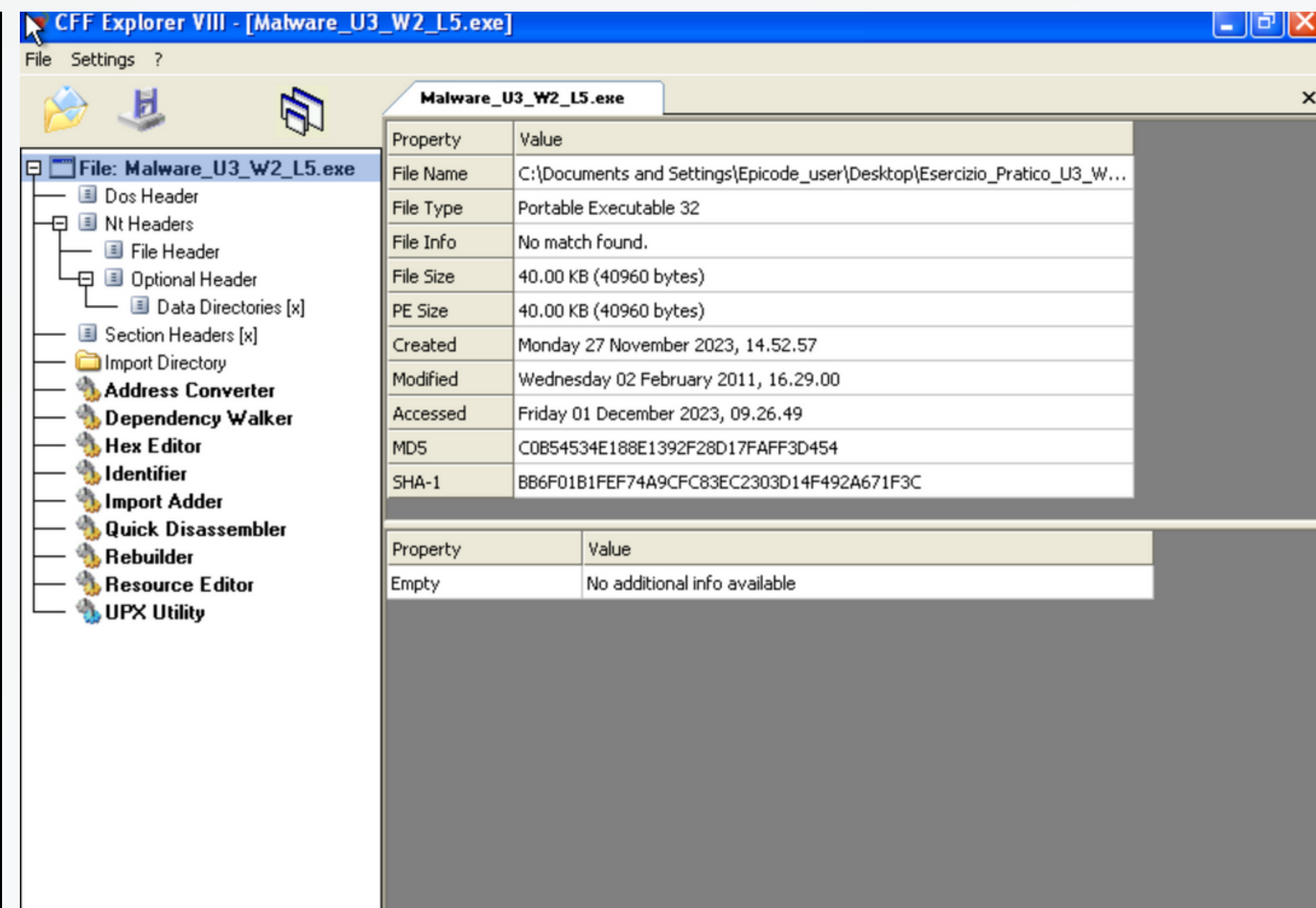
- Trovare le librerie importate del file eseguibile
- Trovare le sezioni di cui è composto il file eseguibile

Data la figura a pagina 6

- Identificare i costrutti noti
- Ipotesizzare il comportamento della funzionalità implementata

ANALISI STATICA

Tramite l'utilizzo del tool **CFF Explorer** stata analizzata la struttura interna del malware in oggetto. Si tratta infatti di un programma che consente l'analisi di software, in particolare è stato utilizzato per verificare la composizione delle sezioni del malware e l'importazione delle librerie



The screenshot displays the CFF Explorer VIII interface for the file **Malware_U3_W2_L5.exe**. The left pane shows the file's internal structure, including headers, sections, and various utilities. The right pane shows the file's properties.

File: Malware_U3_W2_L5.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Property	Value
File Name	C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	40.00 KB (40960 bytes)
PE Size	40.00 KB (40960 bytes)
Created	Monday 27 November 2023, 14.52.57
Modified	Wednesday 02 February 2011, 16.29.00
Accessed	Friday 01 December 2023, 09.26.49
MD5	C0B54534E188E1392F28D17FAFF3D454
SHA-1	BB6F01B1FEF74A9CFC83EC2303D14F492A671F3C

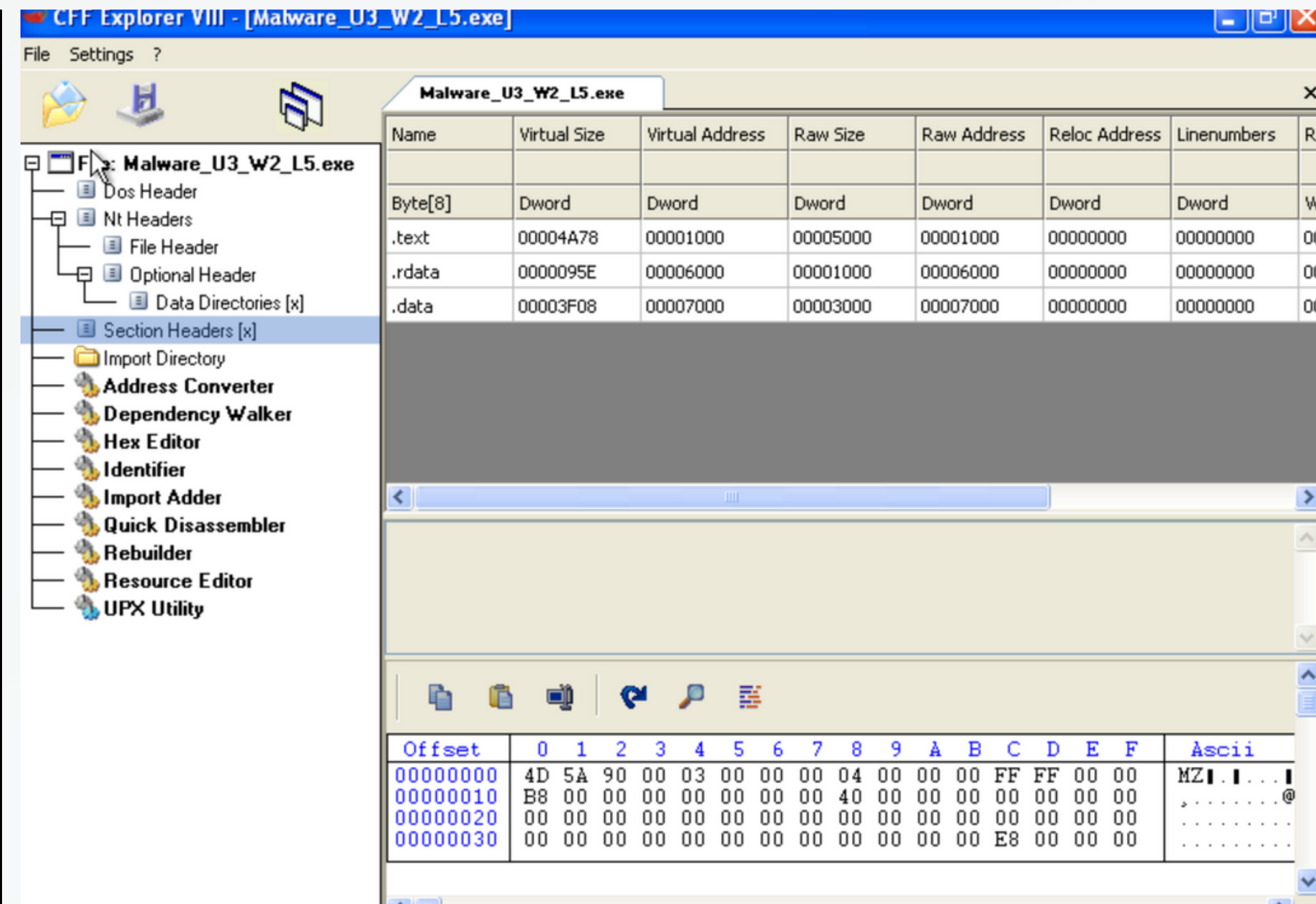
Property	Value
Empty	No additional info available

ANALISI STATICA

Da questa prima immagine si può apprezzare la composizione delle sessioni del malware:

- **.text** = contiene le ricche di codice che andranno eseguite dalla CPU
- **.rdata** = contiene le informazioni riguardo le librerie che verranno importate dal software
- **.data** = contiene le variabili globali che sono quindi richiamabili da qualsiasi funzione del codice

Queste sessioni definiscono in toto il software analizzato e la loro analisi restituisce informazioni come 'peso' 'indirizzi virtuali' e 'caratteristiche'.



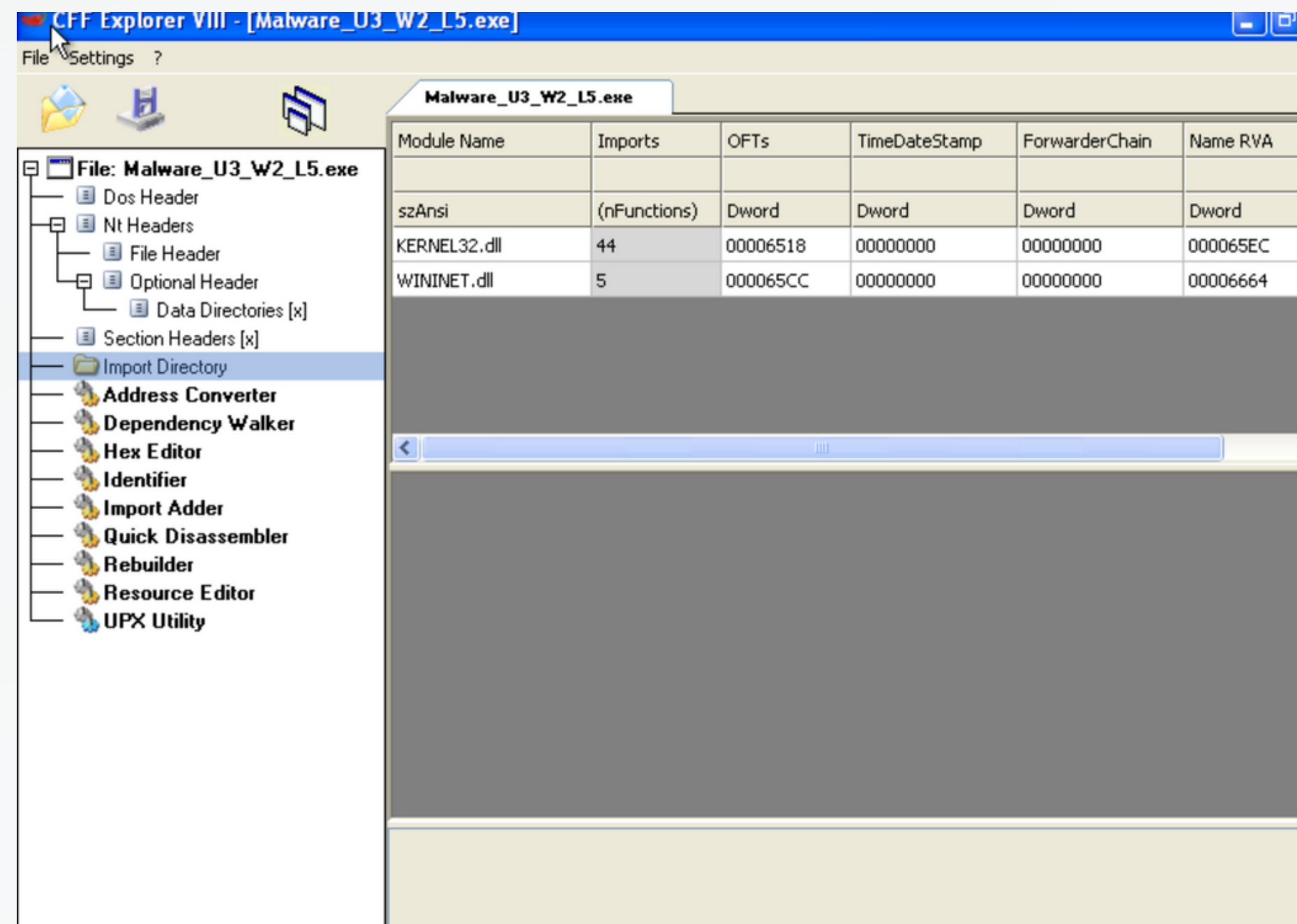
ANALISI STATICA

Da questa immagine si può osservare la sezione dedica alle librerie che verranno importate dal software malevolo. Inoltre è possibile visualizzare le funzioni che queste richiamano e tramite esse iniziare a capire come potrebbe comportarsi il malware.

In questo caso le librerie importate sono due:

- **Kernel32.dll** = essa contiene le funzioni principali per interagire col sistema operativo
- **Wininet.dll** = essa contiene le funzioni per l'interazione con i protocolli di rete.

Con un analisi delle funzioni di entrambe le librerie è possibile capire che il malware utilizzerà le funzioni di libreria in Runtime e cercherà di definire la connessione ad internet della macchina infetta.



ASSEMBLY

Tramite l'utilizzo del linguaggio Assembly si possono riconoscere ed evidenziare diversi costrutti noti:

- Creazione dello Stack
- Chiamata di funzione
- Ciclo IF
- Rimozione dello Stack

```
push    ebp
mov     ebp, esp
push    ecx
push    0          ; dwReserved
push    0          ; lpdwFlags
call    ds:InternetGetConnectedState
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
push    offset aSuccessInterne ;
call    sub_40117F
add     esp, 4
mov     eax, 1
jnp     short loc_40103A
loc_40102B:                ; "Error
push    offset aError1_1NoInte
call    sub_40117F
add     esp, 4
xor     eax, eax
loc_40103A:
mov     esp, ebp
pop     ebp
retn
sub_401000 endp
```

ASSEMBLY

Data l'analisi della figura precedente possiamo fare delle ipotesi sul tipo di malware analizzato. Il codice appena visto è progettato in modo da cercare una connessione ad internet sulla macchina infetta, restituendo l'esito della tentata operazione come 'Successo' o 'Errore'.

Un codice del genere, potrebbe dare diverse connotazioni ad un malware. Potrebbero essere infatti diversi i malware che contengono una componente del genere, quali:

- **Trojan;** esso potrebbe cercare di stabilire una connessione a Internet per scaricare ulteriori componenti dannosi, ricevere comandi da un server remoto o inviare informazioni sensibili.
- **Spyware;** potrebbe connettersi a Internet per inviare informazioni rubate, come password, dati personali o dettagli finanziari, a un server remoto controllato dall'attaccante.
- **Worm;** potrebbe connettersi a Internet per cercare nuovi bersagli, scaricare aggiornamenti o ricevere istruzioni da un server remoto.
- **Ransomware;** per comunicare con i server degli attaccanti, inviare informazioni sulla vittima o ricevere istruzioni su come procedere
- **Botnet;** Un malware che trasforma un dispositivo infetto in parte di una botnet può connettersi a Internet per ricevere comandi dal server centrale. I dispositivi infetti possono quindi essere coordinati per eseguire azioni dannose come attacchi DDoS