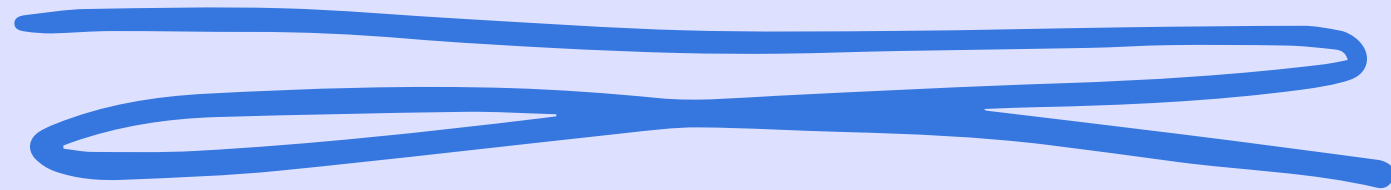


# Malware analysis





# ***Indice***

- **Traccia**
- **Librerie**
- **CFF Explorer VIII**
- **Section Headers**
- **Conclusione**



# ***Traccia***

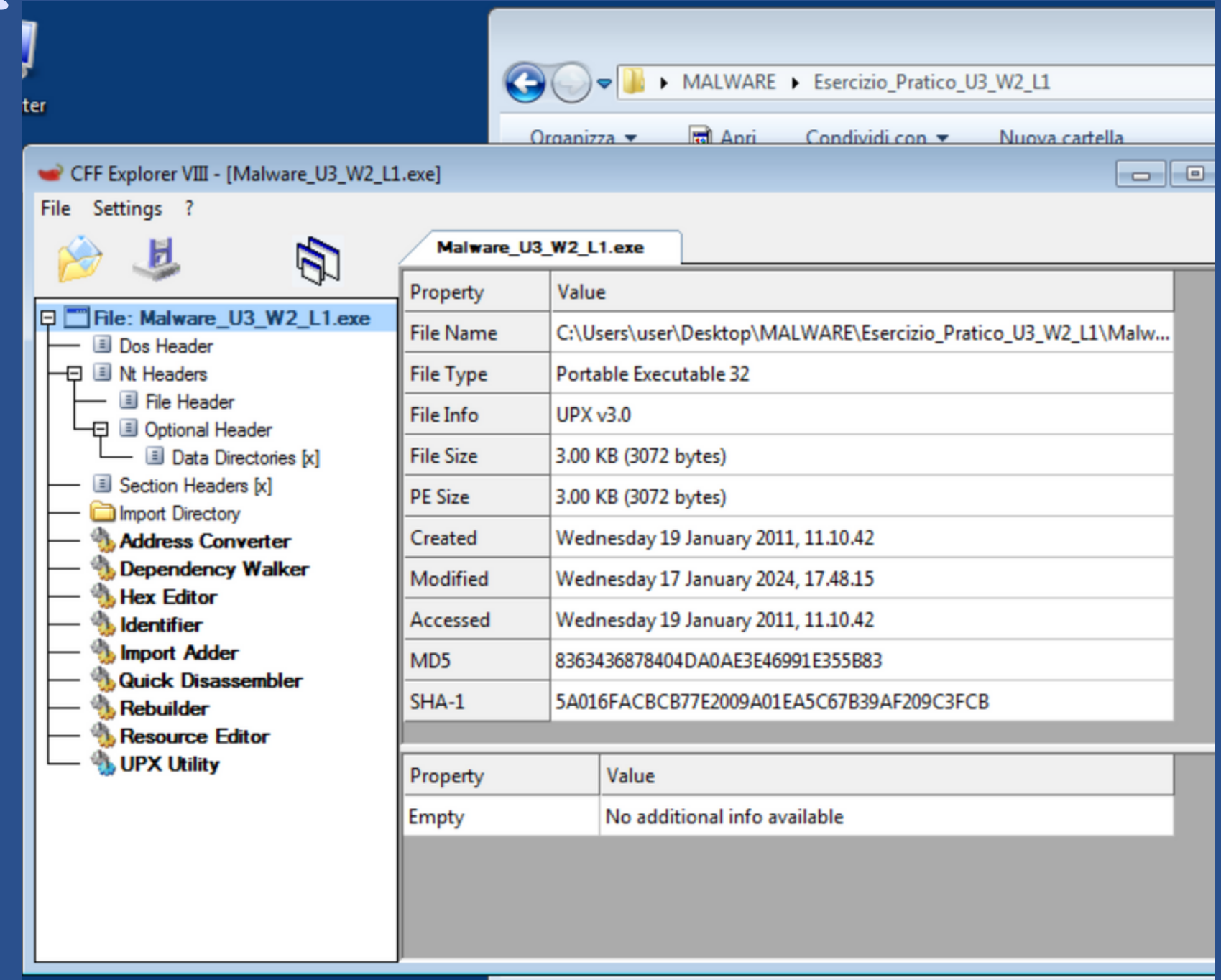


Con riferimento al file eseguibile contenuto nella cartella «**Esercizio\_Pratico\_U3\_W2\_L1**» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- **Indicare le librerie importate dal malware, fornendo una 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**

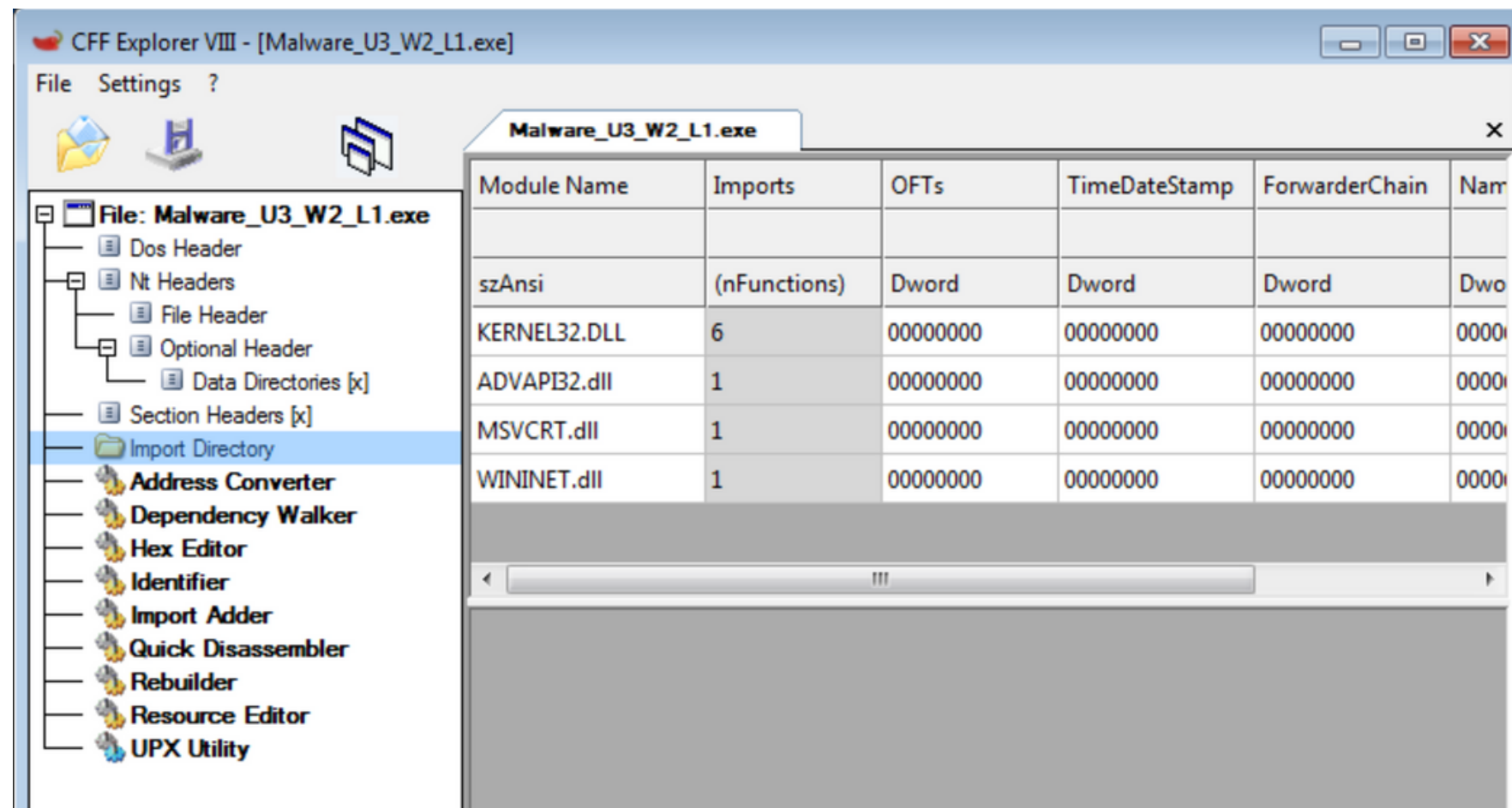
# CFF explorer VIII

CFF Explorer è stato progettato per rendere il PE editing il più semplice possibile, ma senza perdere di vista la struttura interna dell'eseguibile. Questa applicazione include una serie di strumenti che potrebbero aiutare sia il *reverse engineering* sia i programmatori. Offre un ambiente multi-file e una comoda interfaccia facilmente navigabile.



# ***Librerie***

Possiamo vedere che importa 4 librerie:



**KERNEL32.dll** > è un file DLL di Windows. DLL è l'acronimo di Dynamic Link Library. I file DLL sono programmi o estensioni del browser web necessari, perché contengono le risorse, i dati e il codice del programma. Quindi include le funzione core del sistema operativo

**ADVAPI32.dll** > è una libreria dinamica contenente numerose funzioni che vanno dall'avvio, pausa ed interruzione dei servizi del sistema operativo alla disconnessione dell'utente ed operazioni sul registro. Quindi include le funzioni per interagire con i registri e i servizi Windows

**MSVCRT.dll** > è un modulo che contiene le funzioni di libreria C Standard quale il printf, memcpy e cos. è una parte della libreria Runtime di Microsoft C; serve per la manipolazione scritte o allocazione di memoria

**WININET.dll** > è un modulo che contiene le funzioni Internet-relative usate dalle applicazioni di Windows, le funzioni per implementare i servizi di rete come ftp, ntp, http in crescita del 5%

# Section Headers



Nella sezione “**Section Headers**” possiamo vedere che l’e eseguibile si compone di 3 sezioni: “UPX0”, “UPX1” e “UPX3”; il malware ha nascosto il vero nome delle sezioni e quindi non siamo in grado di capire di che tipo di sezioni si tratta.

CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

File: Malware\_U3\_W2\_L1.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

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address
Byte[8]	Dword	Dword	Dword	Dword	Dword
UPX0	00004000	00001000	00000000	00000400	00000000
UPX1	00001000	00005000	00000600	00000400	00000000
UPX2	00001000	00006000	00000200	00000A00	00000000

Offset0123456789A B C D E FAsc000000004D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00MZ



# Conclusioni

Possiamo capire che ci troviamo di fronte ad un malware di tipo avanzato che non ci permette di recuperare molte informazioni sul suo comportamento solo con l'analisi statica basica. Queste supposizioni vengono supportate in quanto tra le funzioni importate troviamo *“LoadLibrary e GetProcAddress”*, esse possono essere sfruttate per nascondere le attività dannose. Vengono usate dai malware per caricare in modo dinamico il codice dannoso all'interno di un processo in esecuzione e per ottenere puntatori a funzioni all'interno di queste librerie per eseguire operazioni dannose, come il furto di informazioni o il danneggiamento del sistema.



CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

File: Malware\_U3\_W2\_L1.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

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	N
00000A98	N/A	00000A00	00000A04	00000A08	0
szAnsi	(nFunctions)	Dword	Dword	Dword	D
KERNEL32.DLL	6	00000000	00000000	00000000	0
ADVAPI32.dll	1	00000000	00000000	00000000	0
MSVCRT.dll	1	00000000	00000000	00000000	0

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc