

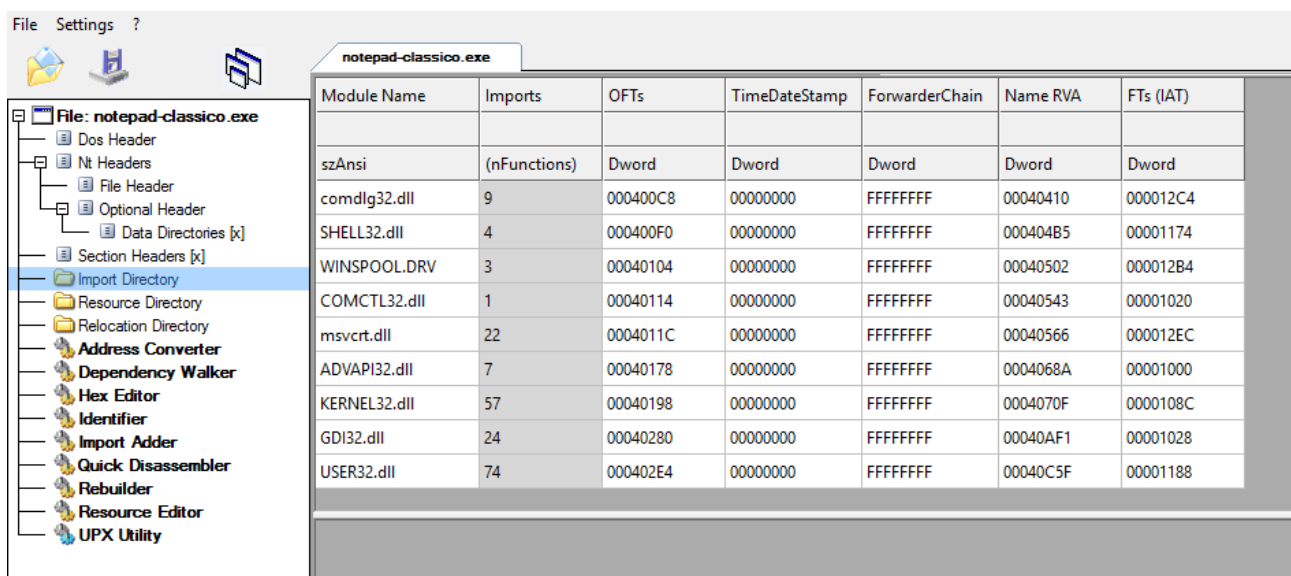
S9L2

U3

Marco Falchi

Librerie importate

Ho trovato le librerie importate all'interno del file scaricato dopo averlo importato all'interno del programma CFF Explorer VIII e verificandole all'interno della sessione "Import Directory"



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
comdlg32.dll	9	000400C8	00000000	FFFFFFFF	00040410	000012C4
SHELL32.dll	4	000400F0	00000000	FFFFFFFF	000404B5	00001174
WINSPOOL.DRV	3	00040104	00000000	FFFFFFFF	00040502	000012B4
COMCTL32.dll	1	00040114	00000000	FFFFFFFF	00040543	00001020
msvcrt.dll	22	0004011C	00000000	FFFFFFFF	00040566	000012EC
ADVAPI32.dll	7	00040178	00000000	FFFFFFFF	0004068A	00001000
KERNEL32.dll	57	00040198	00000000	FFFFFFFF	0004070F	0000108C
GDI32.dll	24	00040280	00000000	FFFFFFFF	00040AF1	00001028
USER32.dll	74	000402E4	00000000	FFFFFFFF	00040C5F	00001188

Spiegazione delle librerie tramite ai:

Librerie di Windows (DLL)

- **comdlg32.dll**: Questa libreria gestisce le **finestre di dialogo comuni** di Windows. Pensa a quando un'applicazione ti chiede di aprire un file (la classica finestra "Apri") o di salvare un documento (la finestra "Salva con nome"). Queste sono le finestre che comdlg32.dll aiuta a gestire.
- **SHELL32.dll**: È una delle librerie più importanti. Contiene funzioni che gestiscono la **shell di Windows**, ovvero l'interfaccia utente. Si occupa di cose come la gestione delle icone, il desktop, il menu Start, il cestino e le operazioni sui file come copiare, incollare ed eliminare.
- **WINSPOOL.DRV**: Questa non è una DLL, ma un **driver** (l'estensione .DRV sta per "driver"). Nello specifico, WINSPOOL.DRV è il driver del **servizio di stampa** di

Windows (il "print spooler"). È responsabile di inviare i documenti alla stampante in coda e di gestire le operazioni di stampa.

- **COMCTL32.dll**: Contiene i **controlli comuni** dell'interfaccia utente. Sono elementi grafici standard come le barre di avanzamento, le barre degli strumenti, le caselle di selezione (checkbox) e le schede (tab) che vedi in molte applicazioni. Aiuta a dare un aspetto coerente alle finestre.
- **msvcrt.dll**: Questa è la libreria di runtime di base di **Microsoft Visual C++**. Fornisce funzioni comuni per i programmi scritti in C e C++, come la gestione della memoria, le operazioni matematiche e l'input/output da tastiera e schermo.
- **ADVAPI32.dll**: Abbreviazione di **Advanced Windows 32-bit Application Programming Interface**, fornisce funzioni di alto livello per il sistema. Gestisce aspetti come la sicurezza (controllo degli accessi, crittografia), il registro di sistema e la gestione degli utenti.
- **KERNEL32.dll**: Altra libreria fondamentale, a volte chiamata anche "il cuore" di Windows. Fornisce l'accesso alle **funzioni di base del kernel** del sistema operativo. Si occupa di aspetti critici come la gestione della memoria, la creazione e la terminazione dei processi e dei thread, e la sincronizzazione.
- **GDI32.dll**: Sta per **Graphics Device Interface**. Si occupa del disegno sullo schermo. Gestisce le funzioni grafiche di base come il disegno di linee, cerchi, rettangoli, e la gestione di font e colori, rendendo possibile la visualizzazione di un'interfaccia grafica.
- **USER32.dll**: È la libreria che gestisce l'**interazione con l'utente**. Si occupa della creazione e della gestione delle finestre, dell'elaborazione degli input da tastiera e mouse e della gestione dei messaggi tra le finestre.

In sintesi, ogni DLL in questa lista ha un ruolo specifico ma tutte collaborano per far funzionare correttamente Windows e le applicazioni che usi ogni giorno. Sono il motore che sta dietro l'interfaccia e i processi che diamo per scontati.

Spiegazione delle sezioni tramite ai:

Sezioni

Ecco una spiegazione di queste sezioni comuni:

- **.text**: Questa è la sezione più importante e contiene il **codice eseguibile** del programma. Qui si trovano le istruzioni che il processore deve eseguire per far funzionare l'applicazione. È spesso la sezione più grande e viene caricata in memoria per l'esecuzione.

- **.data:** Contiene le **variabili globali e statiche** del programma che sono state inizializzate con un valore. Queste variabili occupano spazio nella memoria prima ancora che il programma inizi a funzionare.
- **.rsrc:** Abbreviazione di **risorse**. Questa sezione memorizza tutte le risorse che non sono codice o dati, come le icone, le immagini, i menu, le stringhe di testo e le informazioni sulla versione del file. Windows usa queste risorse per costruire l'interfaccia grafica del programma.
- **.idata:** Sta per **dati di importazione**. Questa sezione elenca tutte le funzioni che il programma ha bisogno di importare da altre librerie esterne (come le DLL che abbiamo visto prima, tipo KERNEL32.dll o USER32.dll). Senza questa sezione, il programma non saprebbe quali funzioni usare e da dove prenderle.

Alcune sezioni vengono ripetute, come nel nostro caso in cui .text e .rsrc compaiono due volte. Questo può succedere se un file include più sezioni dello stesso tipo, magari per questioni di allineamento della memoria o per specifici scopi del compilatore.
