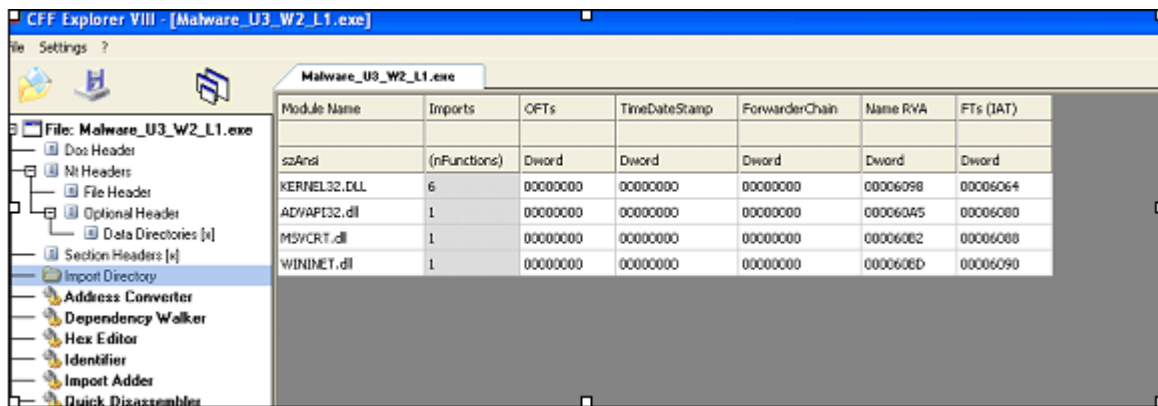


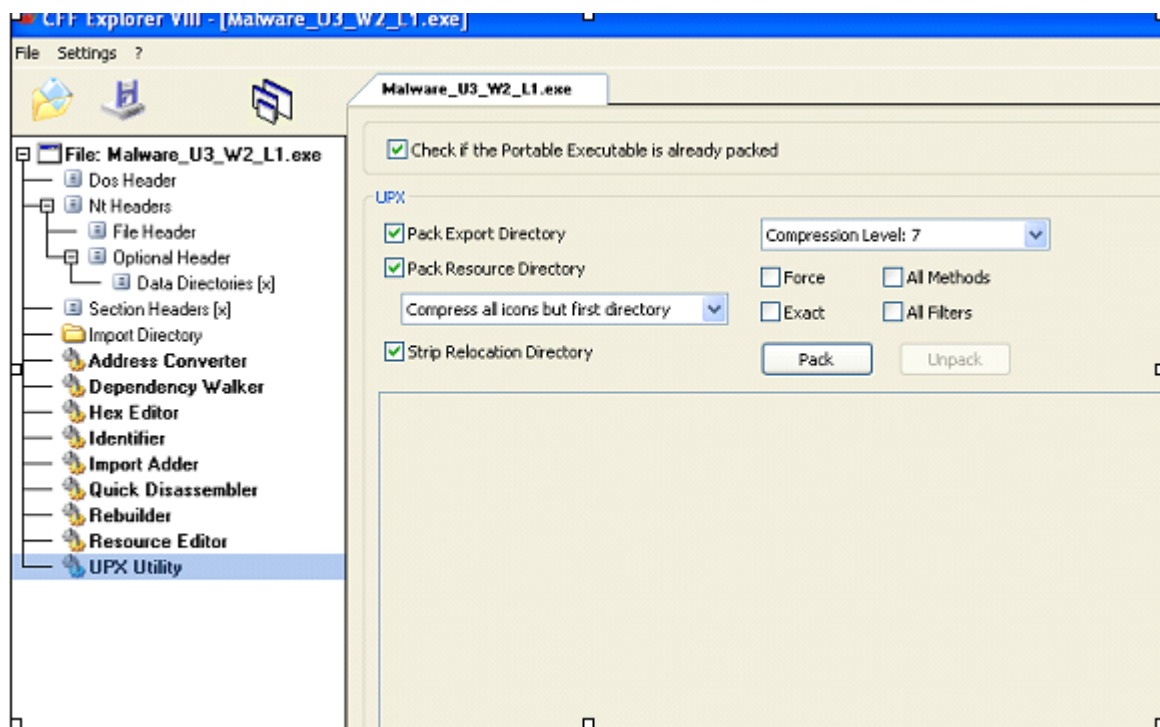
## Esercizio S10e01

1. Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse:

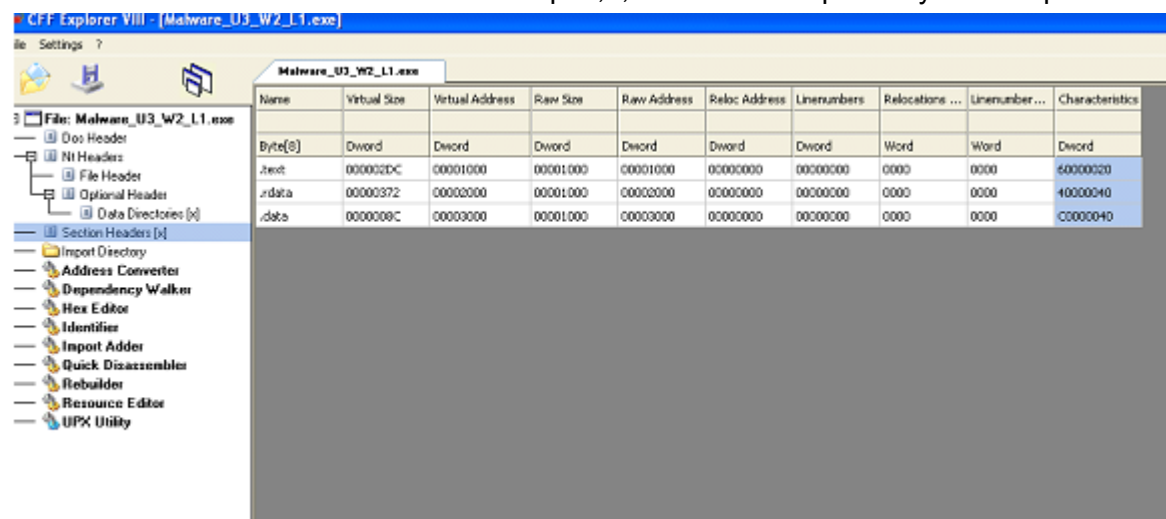


Module Name	Imports	OFFs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAndI	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006080
WININET.dll	1	00000000	00000000	00000000	000060ED	00006090

- **KERNEL32.DLL**: libreria usata per le funzioni principali per interagire con il sistema operativo. Un malware potrebbe sfruttare tale libreria per manipolare i file e per accedere alla gestione della memoria
- **ADVAPI32.dll**: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft, tramite la quale un malware potrebbe creare nuovi account utente, accedere al registro di sistema e crittografare o decrittografare dati sensibili;
- **MSVCRT.dll**: libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C. Tramite questa libreria un malware potrebbe sfruttare delle vulnerabilità presenti o per eseguire codice malevolo;
- **WININET.dll**: libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come http, FTP, NTP. Un malware potrebbe sfruttare tale libreria per comunicare con server remoti, scaricare e caricare file, inviare dati sensibili



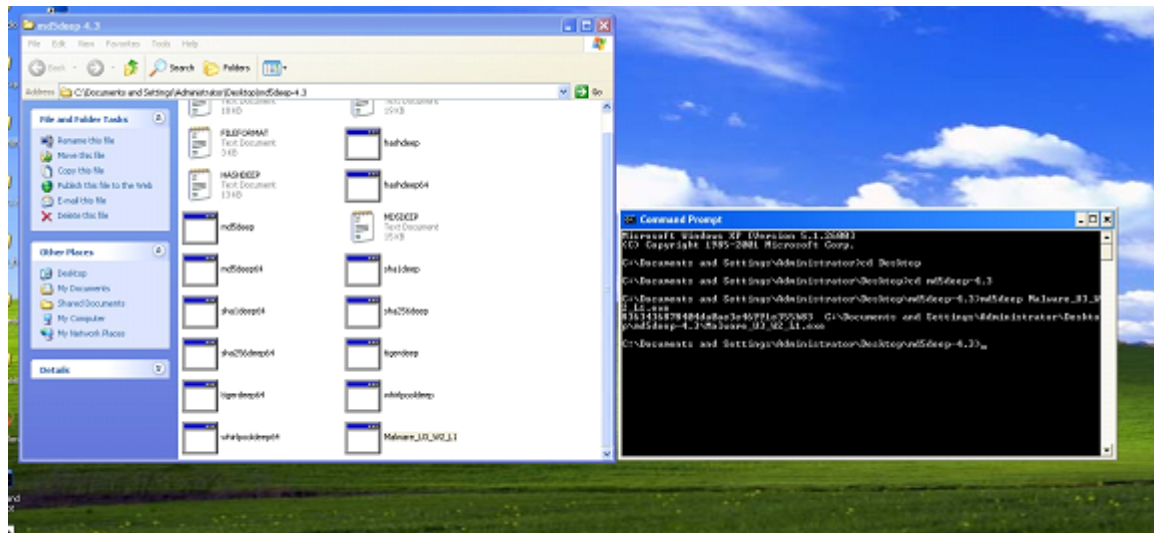
1. Adesso andremo a estrarre le sezioni Upx0,1,2 attraverso l'upx Utility con "Unpack"



- **.text**: Questa sezione contiene le istruzioni, ovvero le righe di codice che la CPU eseguirà quando il software viene avviato. È la sezione principale di un file eseguibile, poiché contiene il codice effettivo che viene eseguito per far funzionare il programma. Tutte le altre sezioni contengono dati o informazioni di supporto per questa sezione.
- **.rdata**: Questa sezione contiene informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile. Qui vengono memorizzate le informazioni sui moduli esterni che l'eseguibile utilizza, come librerie di sistema o librerie condivise, e le funzioni che vengono importate o esportate per l'utilizzo all'interno del programma.

- **.data:** Questa sezione contiene dati e variabili globali del programma eseguibile. Le variabili definite in questa sezione sono accessibili da qualsiasi parte del programma, poiché sono globalmente dichiarate.

Di seguito da Terminale tramite md5deep siamo andati a prendere l'Hash del malware.



Una volta recuperato l'Hash l'ho inserito su VIRUSTOTAL e l'analisi ci segna che 57 verifiche su 72 hanno identificato il malware come tipo Trojan, facendoci capire che la natura maligna del file.

