

S10 L1

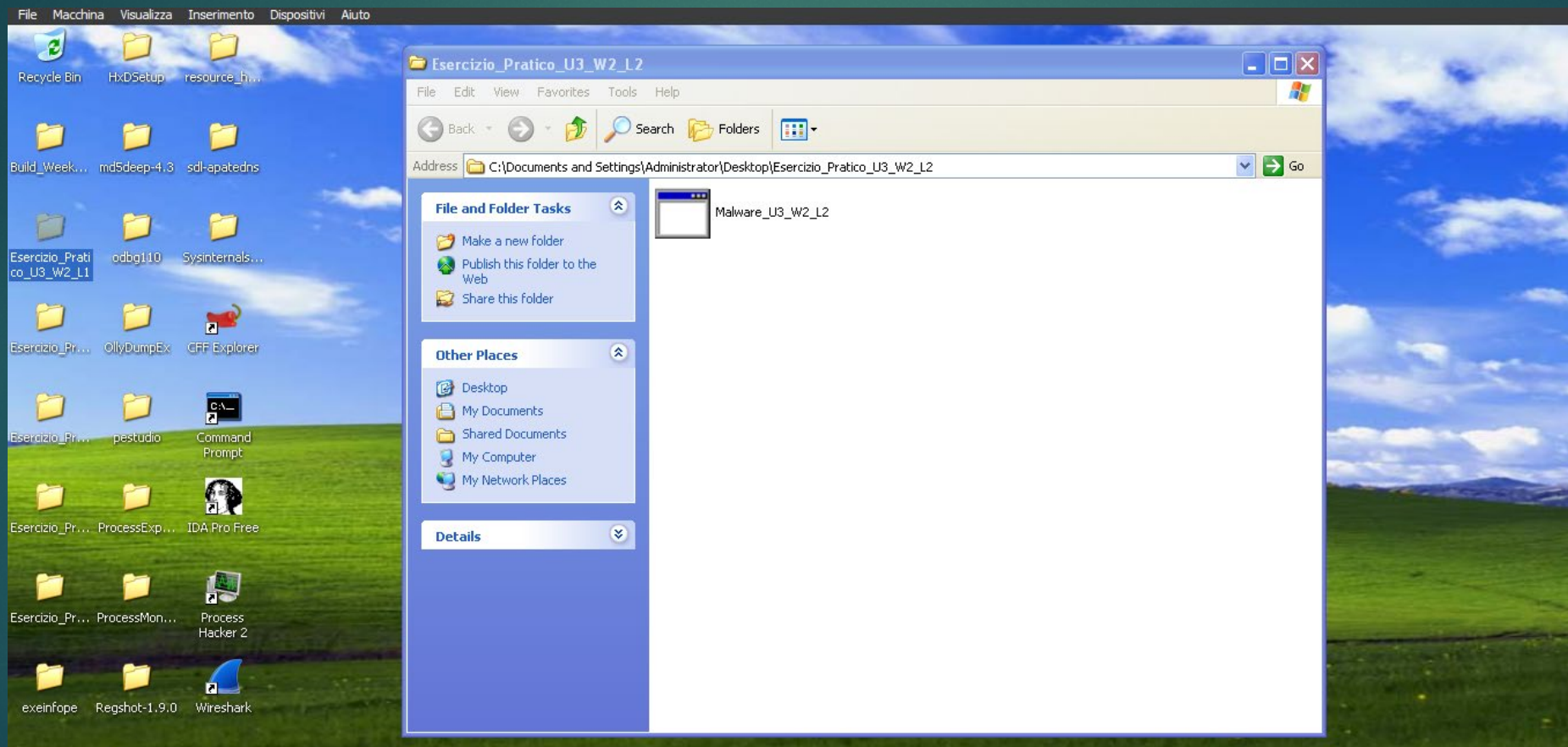
NELLA LEZIONE TEORICA DEL MATTINO, ABBIAMO VISTO COME RECUPERARE INFORMAZIONI SU UN MALWARE TRAMITE L'ANALISI STATICA BASICA. CON RIFERIMENTO AL FILE ESEGUIBILE CONTENUTO NELLA CARTELLA «ESERCIZIO_PRATICO_U3_W2_L1» PRESENTE SUL DESKTOP DELLA VOSTRA MACCHINA VIRTUALE DEDICATA ALL'ANALISI DEI MALWARE, 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

Come primo punto apriamo il seguente file **Malware_U3_W2_L2** nella cartella **Esercizio_Pratico_U3_W2_L2**



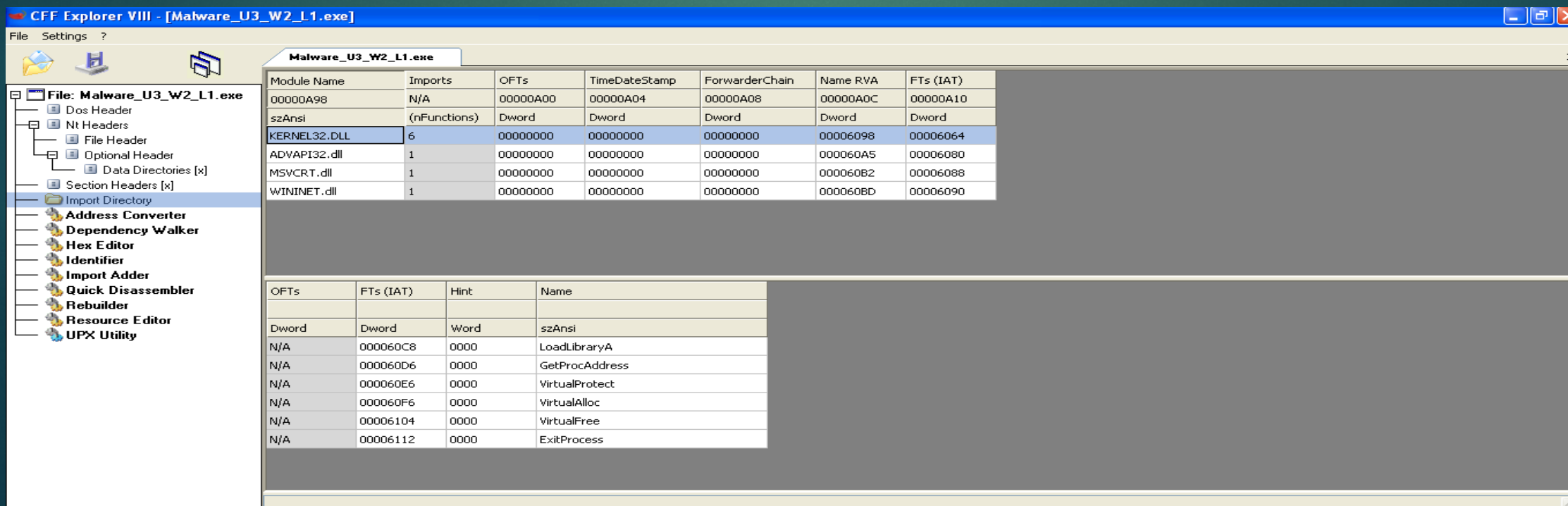
Eseguiamo il programma CFF Explorer e selezioniamo la cartella Import Directory ed all'interno di essa troveremo le seguenti librerie:

Kernel32.dll: libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

Advapi32.dll: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft

MSVCRT.dll: libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C

Wininet.dll: libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.



CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(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	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

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
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess