S10-L1

by Andreoli Michael & Hmich Otman

Referring to the executable file contained in the "Esercizio_Pratico_U3_W2_L1" folder located on the Desktop of your virtual machine dedicated to malware analysis, answer the following questions:

List the libraries imported by the malware, providing a description for each of them.

List the sections that make up the malware, providing a description for each of them.

Add a final consideration on the malware under analysis based on the information collected.

CFF Explorer

CFF Explorer is a freeware suite offering a comprehensive Portable Executable (PE) editor, CFF Explorer, alongside a process viewer. CFF Explorer itself provides in-depth analysis and modification capabilities for PE files, including support for 32-bit and 64-bit architectures. Key functionalities include:

Detailed PE Structure Exploration: Examine headers, sections, imports, exports, and resources of PE files.

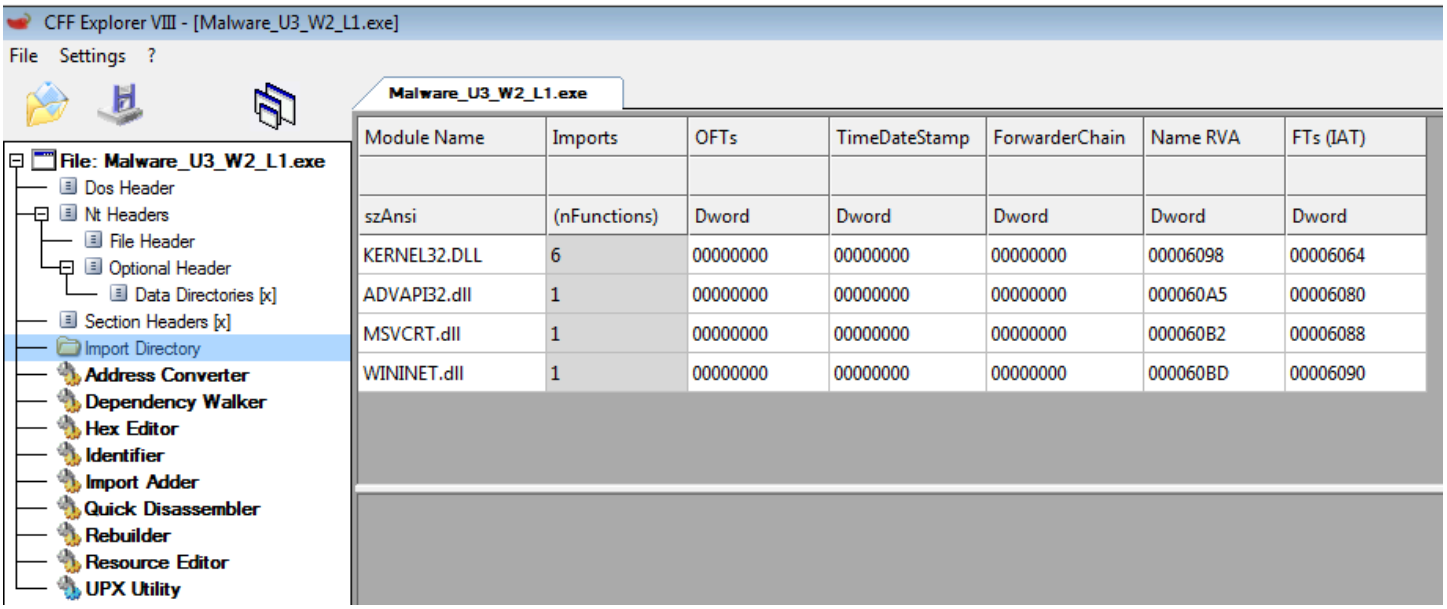
Editing and Customization: Modify metadata fields and flags, enabling customization of program behavior.

Advanced Functionality: Tools like a disassembler, hex editor, import adder, and scripting language empower advanced editing and analysis.

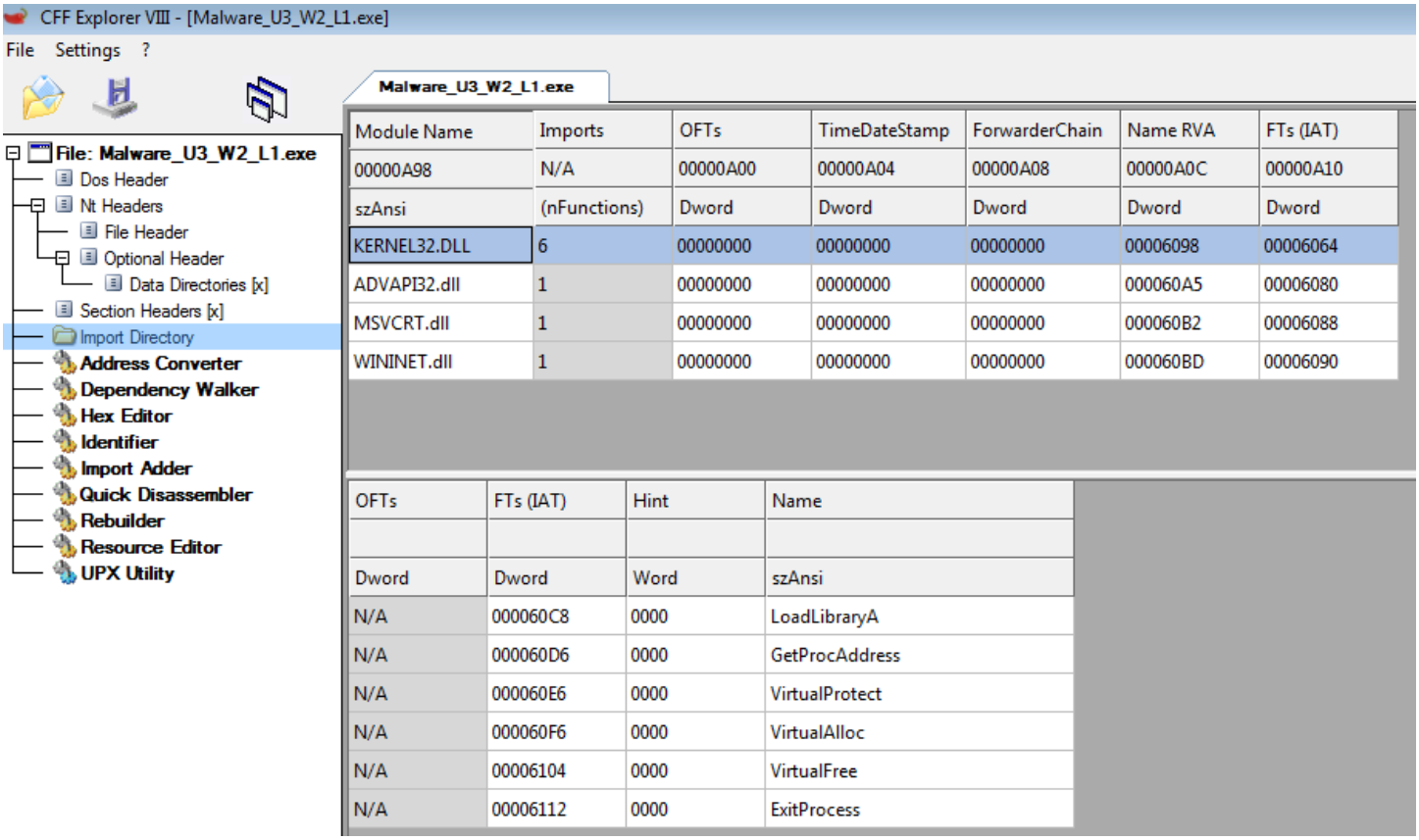
.NET Support: CFF Explorer is the first PE editor with full support for editing .NET internal structures and resources.

Overall, CFF Explorer caters to programmers and reverse engineers seeking a feature-rich solution for PE file analysis and modification.

Import Directory

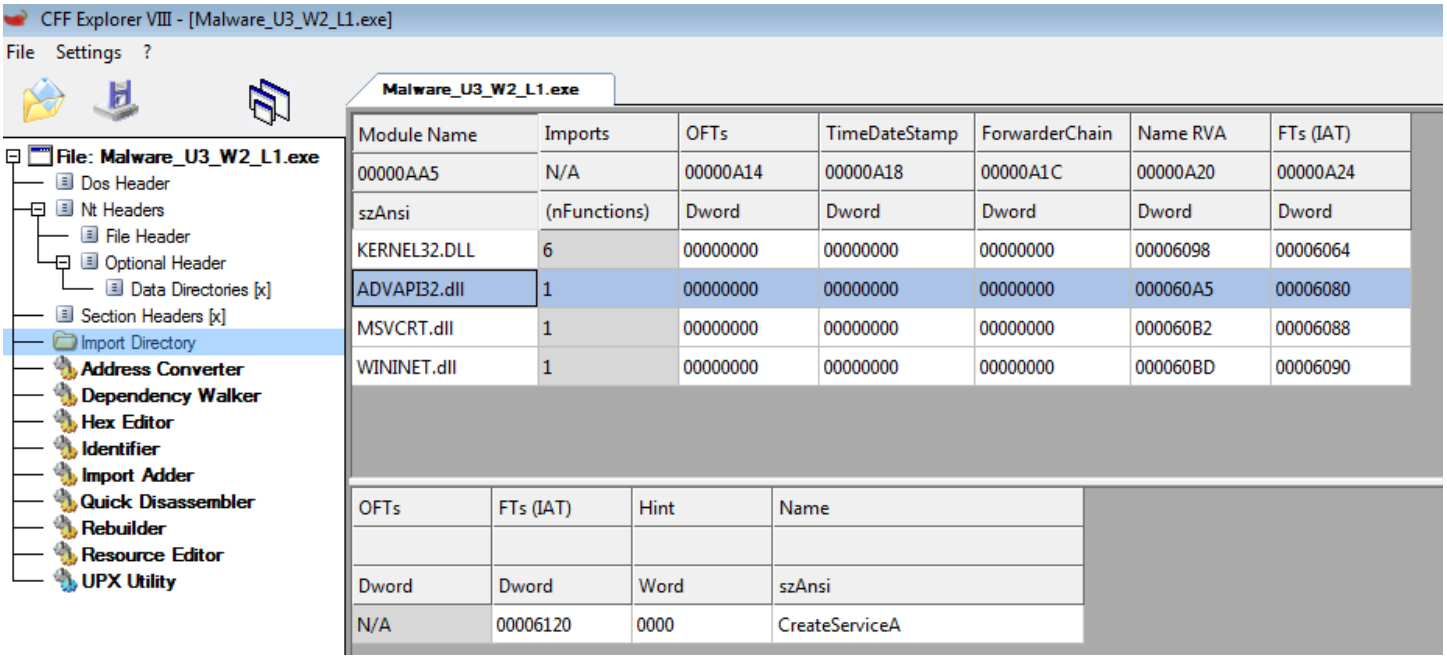


A **DLL (Dynamic Link Library)** is a toolbox for computer programs. It contains tools (functions and data) that many programs can use at once, instead of each program having its own copy. This saves space and memory. If a program needs to open a file. There's a DLL with a "file open" tool inside. Many programs can use this same tool from the DLL, instead of each writing their own version.

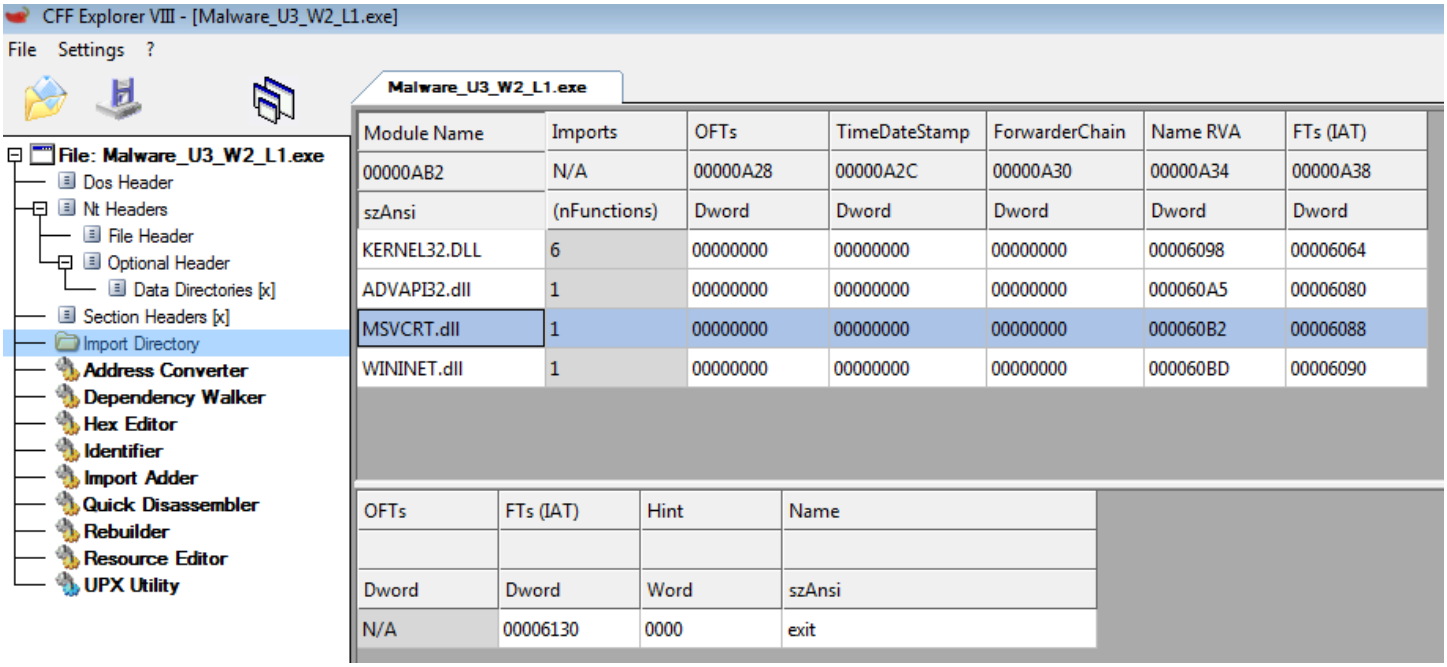


KERNEL32.DLL: A fundamental Windows library. It provides basic functions, including memory management, process management, and thread execution. It

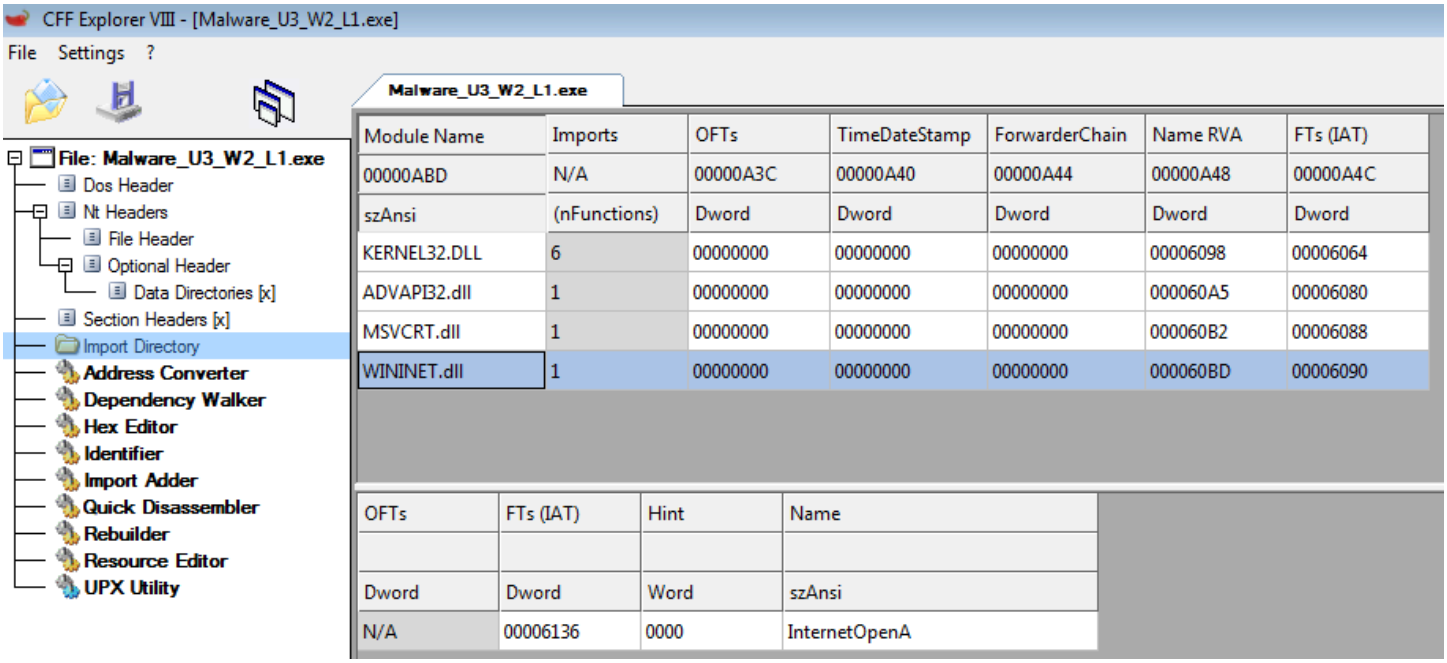
is imported by many operating system executable files.



ADVAPI32.dll: Handles user authentication, security token management, and access to the system registry. It is often imported by executable files that require elevated privileges or need to access protected resources.

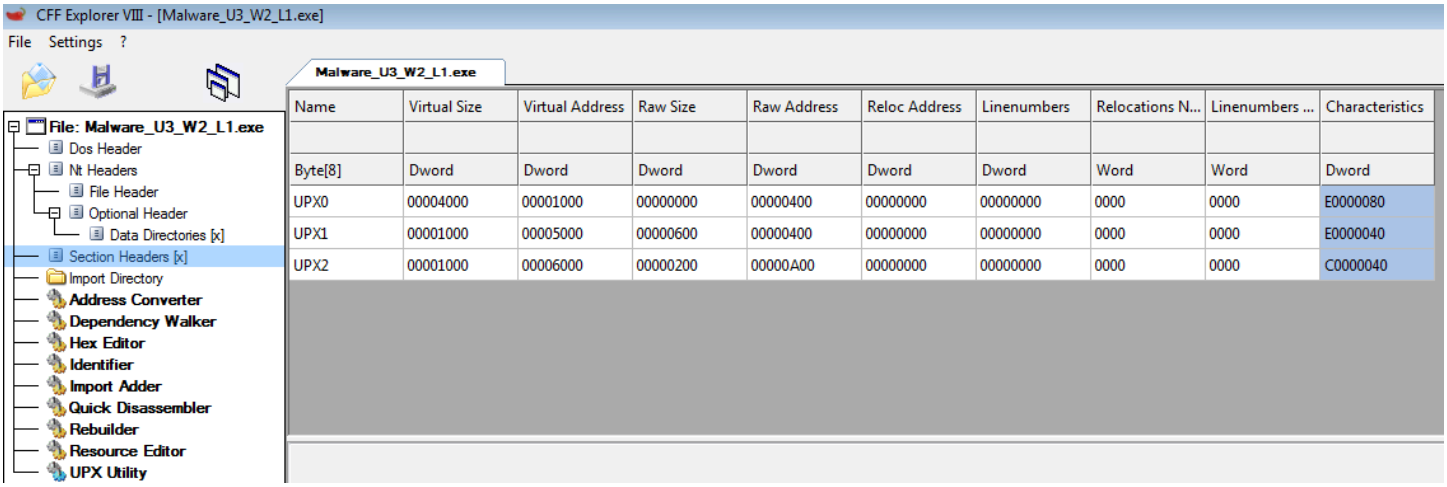


MSVCRT.dll: The standard C runtime library for Windows. It provides basic functions for input/output, string management, and mathematics. It is imported by almost all Windows executable files that use the C or C++ programming languages.

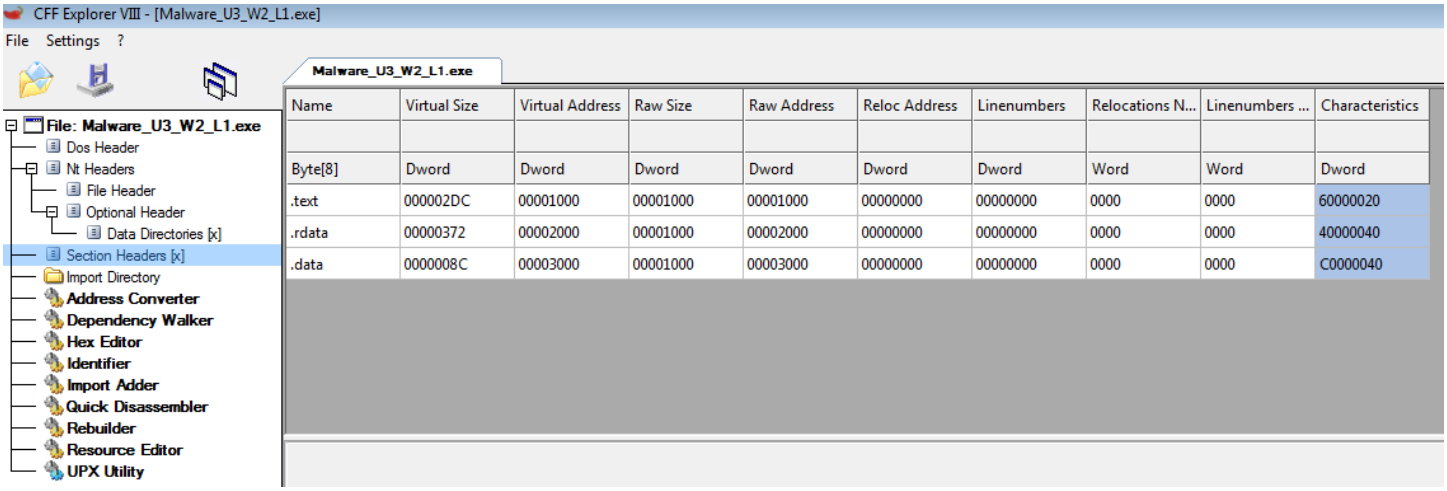


WININET.dll: Provides functions for Internet access, such as sending and receiving HTTP requests and downloading files. It is imported by executable files that need to connect to the Internet.

Section Headers



From an initial attempt to open with CFF, we were unable to retrieve the section names, so we used the UPX utility to decompress the malware and analyze it again.



Now we can see the parts of the malware, .text, .rdata, .data;

.text This is the part of the code that will be executed by the CPU.
.rdata This is the section that contains information about the imported libraries.

.data Contains the global variables that the code will act upon.

We can conclude that the malware in question could potentially be very dangerous if executed. It calls code from the most important system libraries and could thus have access to the machine's files, manage its memory, access user data, and, once the code is executed, it could also send all collected information to a potential attacker using network libraries.