**CFF Explorer Worksheet**

**Objective:**

This worksheet aims to introduce you to the basics of using CFF Explorer to explore and understand the structure of PE files.

**1. Getting Started with CFF Explorer**

**a. What is CFF Explorer?**

CFF Explorer is a tool used for analysing and editing Portable Executable (PE) files. It provides a user-friendly interface for viewing the internal structure of PE files, making it easier to understand how executable and libraries are constructed.

**b. Installing CFF Explorer:**

1. Visit the official website or a trusted software repository to download CFF Explorer.
2. Install the application on your computer by following the setup instructions.

**2. Exploring a PE File**

**a. Opening a File:**

1. Launch CFF Explorer.
2. Click on the **"File"** menu and select **"Open"**.
3. Browse to a PE file on your computer (e.g., notepad.exe) and open it.

**b. Exploring the PE Header:**

1. In the left-hand pane, click on **"NT Headers"**.
2. Examine the sections within the NT Headers:
   * **File Header**: Contains basic information about the file, such as machine type and the number of sections.
   * **Optional Header**: Contains crucial details about memory management, entry points, and more.

**Questions:**

* What is the **Machine** type listed under the File Header?
* What is the **Entry Point** address in the Optional Header?

**3. Inspecting the Section Headers**

**a. Viewing Sections:**

1. Click on **"Section Headers"** in the left pane.
2. Review the list of sections such as .text, .data, .rdata, etc.

**b. Understanding Section Details:**

* **.text**: Contains the executable code.
* **.data**: Contains initialized data.
* **.rdata**: Contains read-only data, such as import tables and string literals.

**Questions:**

* What is the size of the .text section?
* What is the Virtual Address (VA) of the .rdata section?

**4. Viewing the Import Table**

**a. Understanding Imports:**

1. Click on **"Import Directory"** in the left pane.
2. This section lists all the libraries (DLLs) the PE file imports functions from.

**b. Exploring Imported Functions:**

* Click on each DLL name to view the functions imported from it.

**Questions:**

* Which DLLs are imported by the file?
* Name one function that is imported from kernel32.dll.

**5. Analyzing the Export Table**

**a. What are Exports?**

1. Click on **"Export Directory"** in the left pane.
2. This section lists the functions or variables that the PE file exports for use by other modules.

**b. Viewing Exported Functions:**

These are the DLLs imported by the malware sample 1.**Questions:**

* Does the file export any functions? If yes, name one.

**6. Practical Exercise**

1. Open a new PE file (e.g., calc.exe).
2. Answer the following questions based on the file:

**Questions:**

* What is the **Subsystem** value in the Optional Header?
* How many sections are present in the file?
* Name two DLLs that this file imports from.

**7. Saving Changes**

**a. Modifying and Saving:**

1. You can make changes to certain fields in the headers (e.g., modifying section characteristics).
2. To save your changes, go to **"File" > "Save As"**, and save the modified file under a new name.

\*\*b. **Important:** Be cautious when making changes, as incorrect modifications can render the file unusable.

**Conclusion:**

This worksheet provides an introduction to using CFF Explorer for exploring PE files.