

**Find the Portable Executable (PE)  
Information of a Malware  
Executable File using PE Explorer**

***ILABS***  
***CEH PRACTICAL***



**The Portable Executable (PE) format is the executable file format used on Windows OSes that stores the information a Windows system requires to manage the executable code. The PE stores metadata about the program, which helps find additional file details. For instance, the Windows binary is in PE format that consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, linked files, and strings, menus, and symbols.**



## Aim

PE Explorer lets you open, view, and edit a variety of different 32-bit Windows executable file types (also called PE files) ranging from common such as EXE, DLL, and ActiveX Controls to less familiar types such as SCR (Screensavers), CPL (Control Panel Applets), SYS, MSSTYLES, BPL, DPL, and more (including executable files that run on MS Windows Mobile platform).

Here, we will use the PE Explorer tool to view the PE information of a malware executable file.



## Other PE Extraction tools

- ✓ Portable Executable Scanner (pescan) (<https://tzworks.net>)
- ✓ Resource Hacker (<http://www.angusj.com>)
- ✓ PEView (<https://www.aldeid.com>)

DEMO



THANKS