Portable Executable File Format

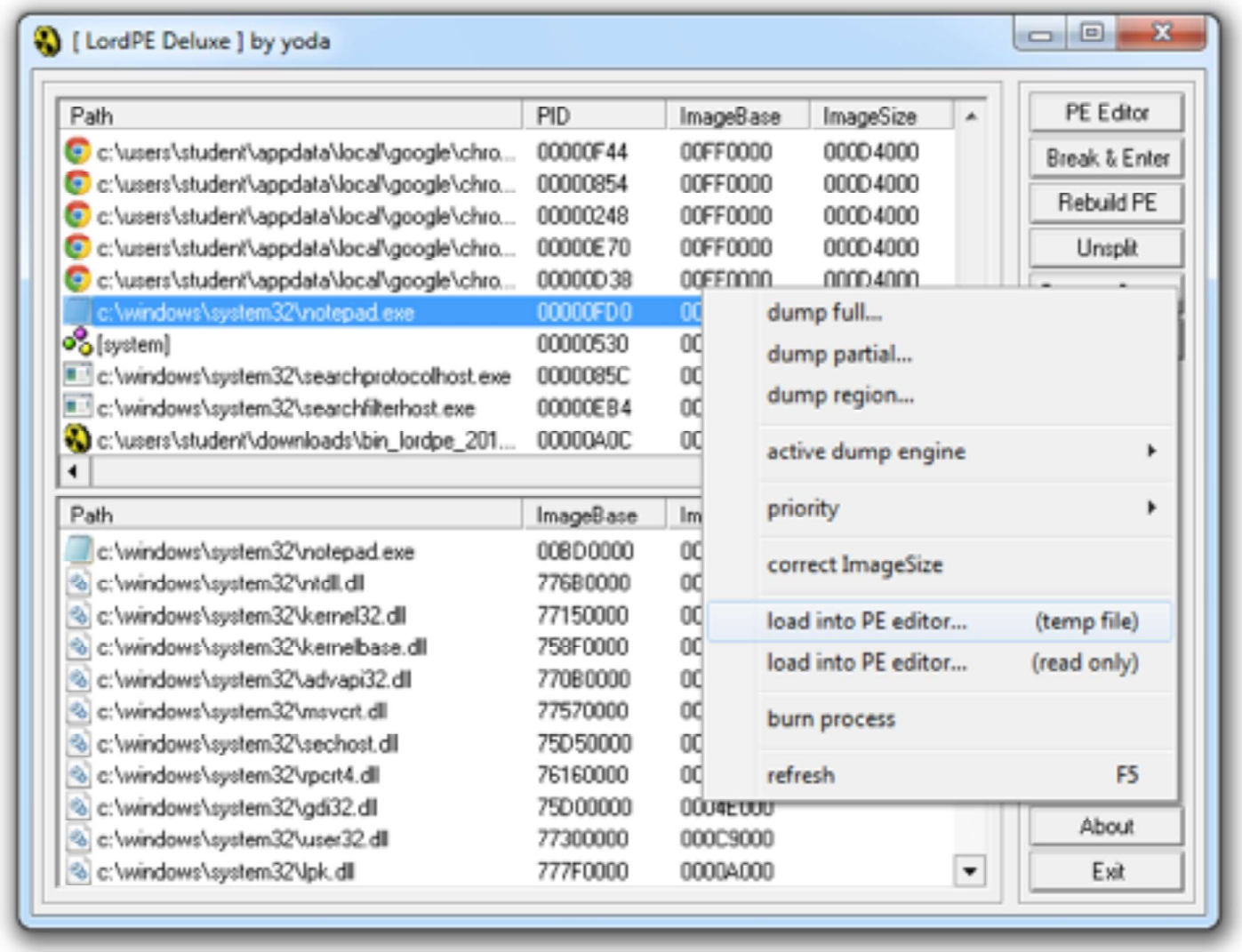
PE Files

- Used by Windows executable files, object code, and DLLs
- A data structure that contains the information necessary for Windows to load the file
- Almost every file executed on Windows is in PE format

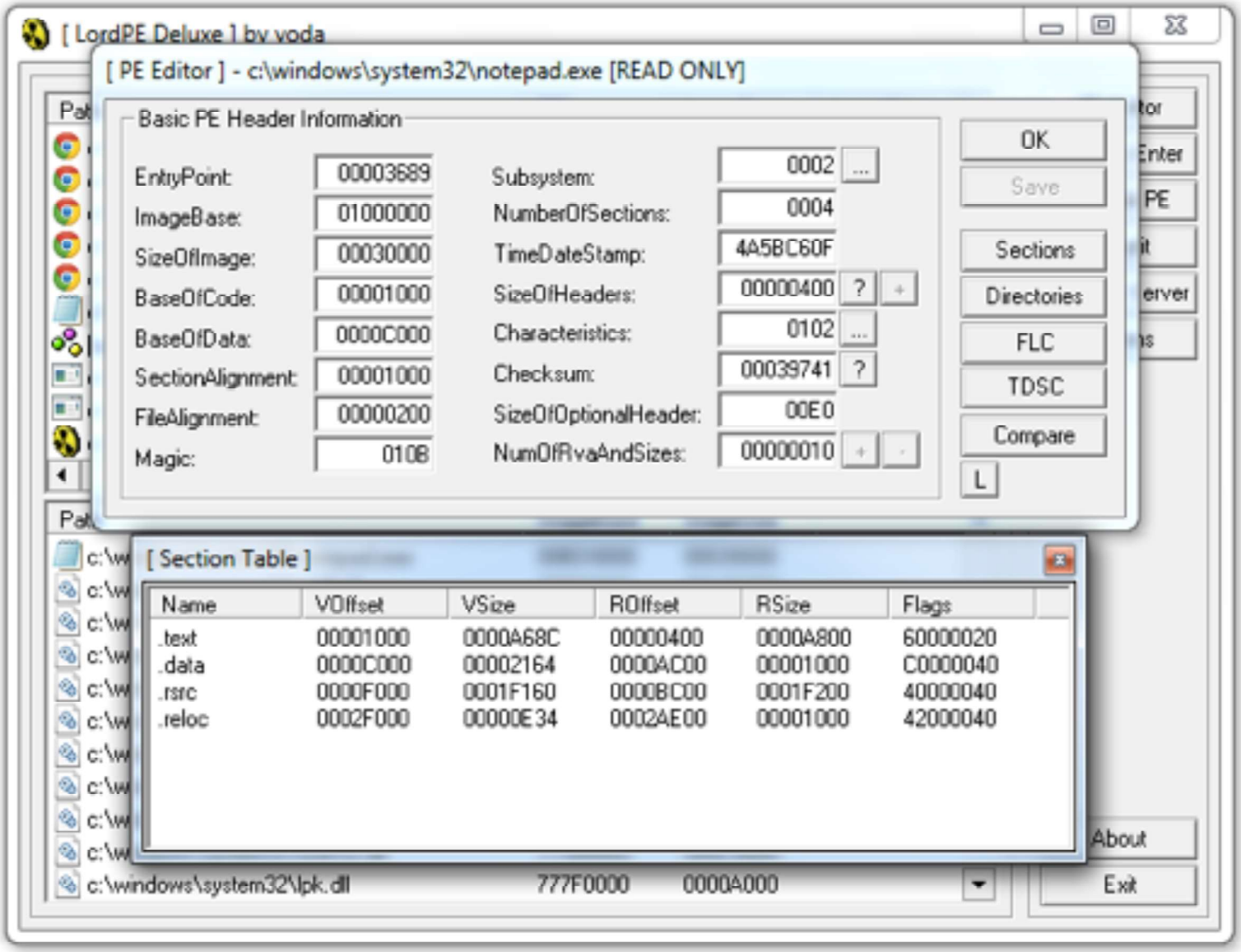
PE Header

- Information about the code
- Type of application
- Required library functions
- Space requirements

LordPE Demo


[LordPE Deluxe] by yoda
Path
PID
ImageBase
ImageSize
c:\users\student\appdata\local\google\chro... 00000F44 00FF0000 000D4000
c:\users\student\appdata\local\google\chro... 00000854 00FF0000 000D4000
c:\users\student\appdata\local\google\chro... 00000248 00FF0000 000D4000
c:\users\student\appdata\local\google\chro... 00000E70 00FF0000 000D4000
c:\users\student\appdata\local\google\chro... 00000D38 00FF0000 000D4000
c:\windows\system32\notepad.exe 00000FD0
[system] 00000530
c:\windows\system32\searchprotocolhost.exe 0000085C
c:\windows\system32\searchfilterhost.exe 00000E84
c:\users\student\downloads\bin_lordpe_201... 00000A0C
Path
ImageBase
c:\windows\system32\notepad.exe 00BD0000
c:\windows\system32\ntdll.dll 776B0000
c:\windows\system32\kernel32.dll 77150000
c:\windows\system32\kernelbase.dll 758F0000
c:\windows\system32\advapi32.dll 770B0000
c:\windows\system32\msvcrt.dll 77570000
c:\windows\system32\sechost.dll 75D50000
c:\windows\system32\rpcrt4.dll 76160000
c:\windows\system32\gdi32.dll 75D00000
c:\windows\system32\user32.dll 77300000 000C9000
c:\windows\system32\lpk.dll 777F0000 0000A000
dump full...
dump partial...
dump region...
active dump engine
priority
correct ImageSize
load into PE editor... (temp file)
load into PE editor... (read only)
burn process
refresh F5
PE Editor
Break & Enter
Rebuild PE
Unsplit
About
Exit

Main Sections



There are a lot more sections

- But the main ones are enough for now
- Link Ch 2c

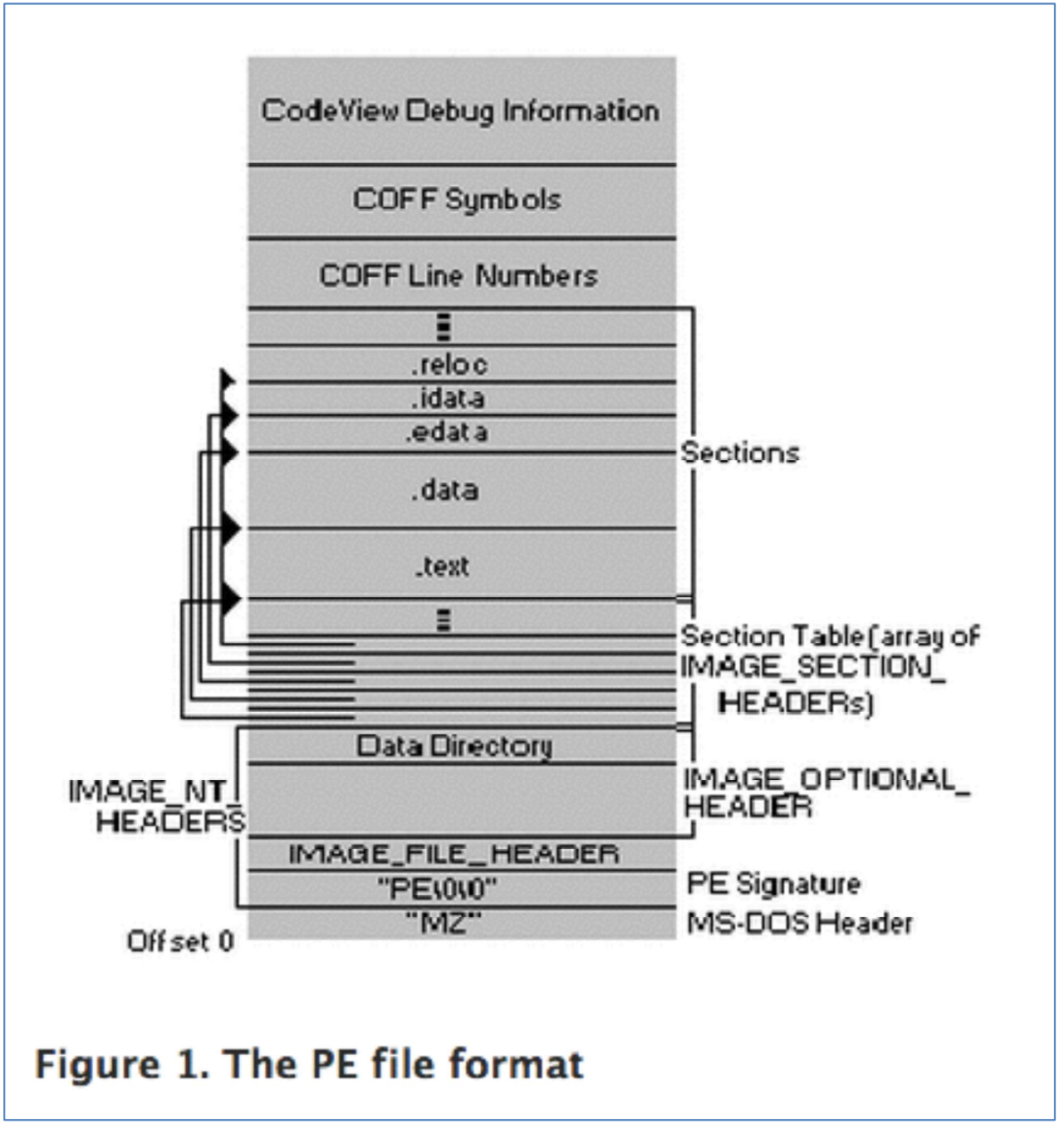


Figure 1. The PE file format

Linked Libraries and Functions

Imports

- Functions used by a program that are stored in a different program, such as library
- Connected to the main EXE by **Linking**
- Can be linked three ways
  - **Statically**
  - At **Runtime**
  - **Dynamically**

Static Linking

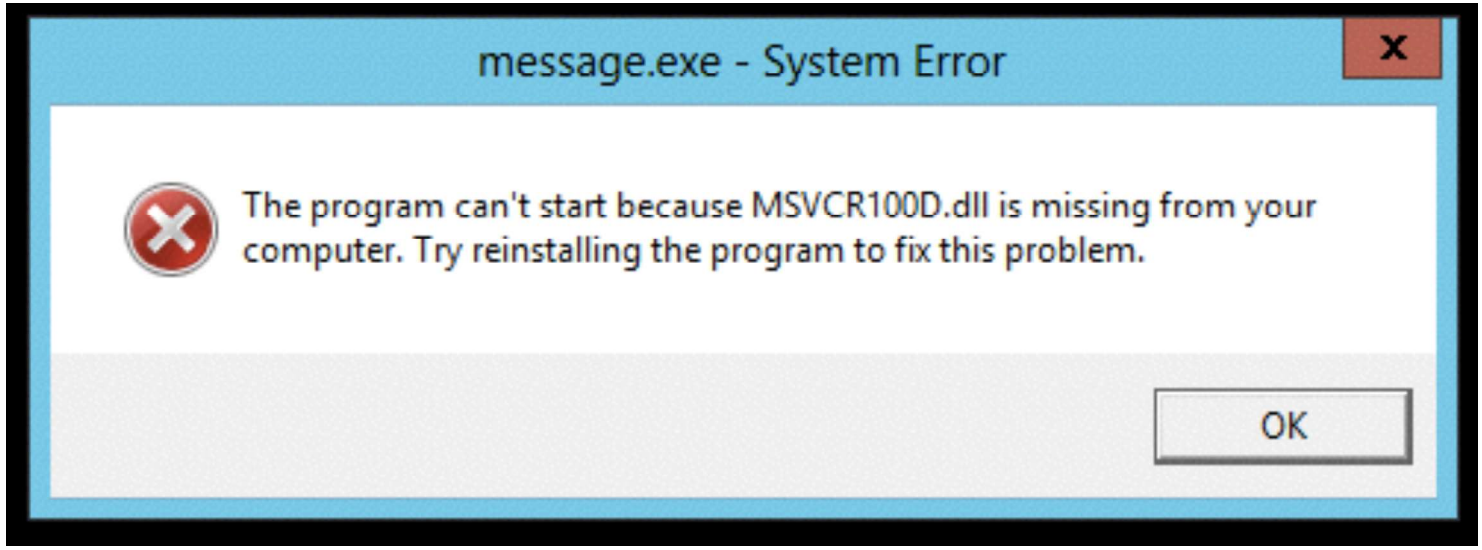
- Rarely used for Windows executables
- Common in Unix and Linux
- All code from the library is copied into the executable
- Makes executable large in size

Runtime Linking

- Unpopular in friendly programs
- Common in malware, especially packed or obfuscated malware
- Connect to libraries only when needed, not when the program starts
- Most commonly done with the **LoadLibrary** and **GetProcAddress** functions

Dynamic Linking

- Most common method
- Host OS searches for necessary libraries when the program is loaded



Clues in Libraries

- The PE header lists every library and function that will be loaded
- Their names can reveal what the program does
- **URLDownloadToFile** indicates that the program downloads something