



File Formats

| | |
|-----------------|---|
| Length | Micromodule |
| Collection | NSA NCCP |
| Updated | March 9, 2019 |
| Contributors | Josh Stroschein |
| Academic Levels | Undergraduate |
| Topics | Reverse Engineering |
| Link | https://clark.center/details/jstroschein/78b6f17c-d1a2-454a-a68c-dee5c676e278 |

Description

File formats allow the organization of binary content. In the case of Windows executables (EXE) or shared libraries (DLL), this allows the operating system to parse the binary content and load into memory for execution. In this module you will learn the basics of the PE file format, what information can be gleaned from analyzing it and how a disassembly tool such as IDA Pro finds executable code for disassembly.

Notes

This work was made possible by NSA Grant for the development of cyber security curriculum.

Outcomes

- Differentiate between different PE parsing utilities to select the correct one based on desired analysis objectives
- Interpret output from PE parsing utilities to understand program behavior
- Demonstrate working knowledge of the PE file format

Files Not Included in Bundle

Download links of files associated with this object but not included in bundle

- [04 - File Formats.mp4](#)

Links

External links that are associated with this learning object

- [YouTube - File Formats](#)