



# The Windows API

Length	Micromodule
Collection	NSA NCCP
Updated	March 9, 2019
Contributors	Josh Stroschein
Academic Levels	Undergraduate
Topics	Operating Systems Security
Link	<a href="https://clark.center/details/jstroschein/cd415875-4de1-4e91-922a-92cea32aac71">https://clark.center/details/jstroschein/cd415875-4de1-4e91-922a-92cea32aac71</a>

## Description

The Windows API allows developers to create applications designed to run within the Windows operating system that take advantage of all of the features Windows has to offer. For the reverse engineer, if you are analyzing windows binaries (malicious or benign) begins with understanding how the Windows API is used and how you can determine program behavior from the use of these APIs. In this module, you will learn about the Windows API, how programs use it and where to find information about it.

## Notes

Please note that the lab files contain malicious software - please handle in a safe manner and only analyze in a proper environment. This work was made possible by NSA Grant for the development of cyber security curriculum.

## Outcomes

- Use Dependency Walker to identify import and API usage (Windows API) of sample program
- Identify commonly used libraries and APIs
- Demonstrate the ability to evaluate the use of the Windows API to assess potential program functionality

## Files Not Included in Bundle

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

- [07 - Windows API.mp4](#)

## Links

External links that are associated with this learning object

- [YouTube - Windows API](#)