



Basic Analysis Techniques

Length	Micromodule
Collection	NSA NCCP
Updated	February 21, 2023
Contributors	Josh Stroschein
Academic Levels	Undergraduate
Topics	Malware
Link	https://clark.center/details/jstroschein/01bc7fe9-db5d-4024-ac63-d126fdb2ea5c

Description

Performing malware analysis begins with basic techniques - obtaining information about the samples you are analyzing, gleaning indicators of compromise and identifying other useful information. In this course you will learn core techniques for performing basic analysis of malicious software.

Outcomes

- Describe the difference between static and dynamic analysis
- Demonstrate the ability to use hashing utilities to identify a malicious sample
- Explain general rules for analyzing malware
- Experiment with anti-virus software to create signatures based off of custom programs.
- Use string utilities on malicious samples to identify valuable data
- List the different categories of malicious software

Links

External links that are associated with this learning object

- [YouTube - Basic Analysis Techniques](#)