

# Progressing Your Malware Analysis Skills

---



**Tyler Hudak**

INCIDENT RESPONDER

@secshoggoth



# Overview

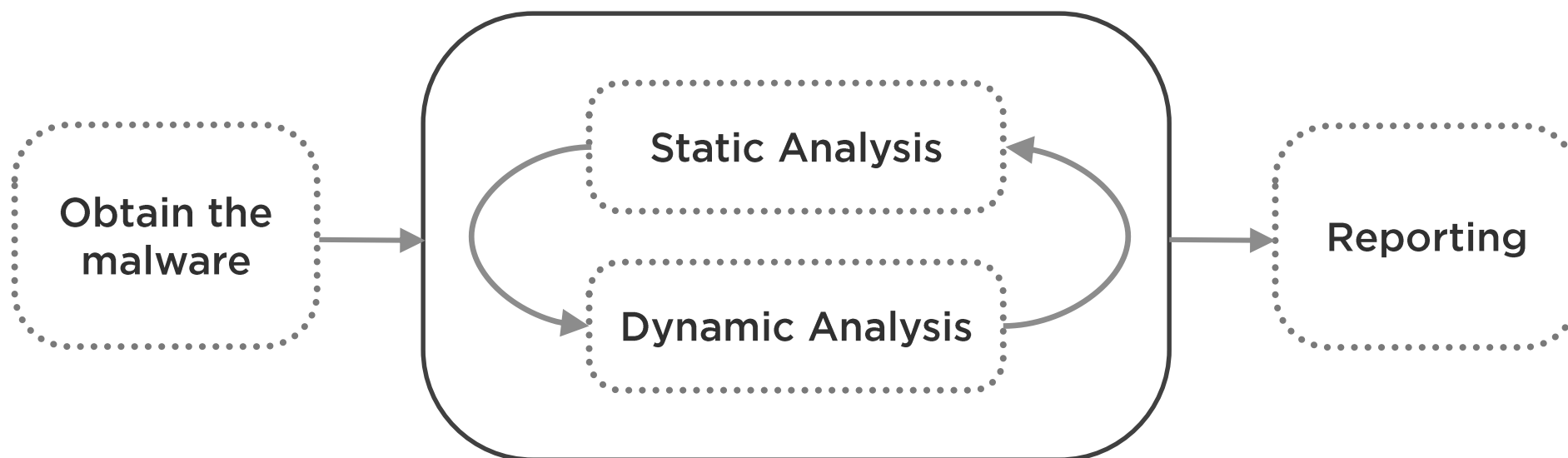


**Recap of malware analysis**

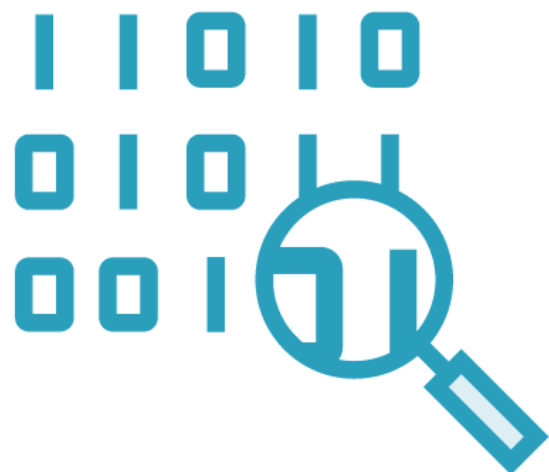
**Where to go from here?**



# Malware Analysis Process



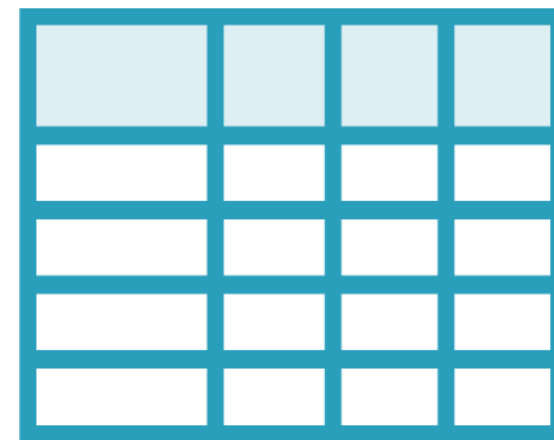
# Static Analysis



Hashing



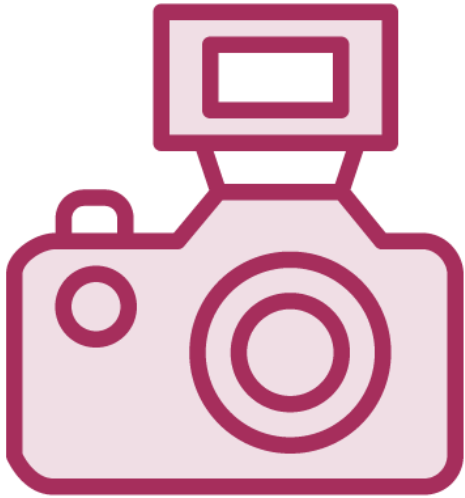
Embedded Strings



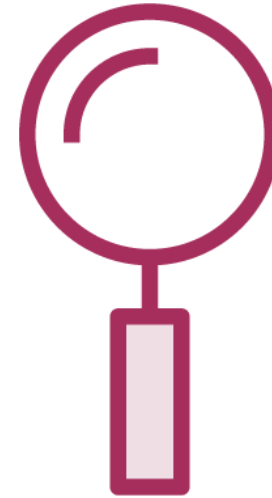
PE Header



# Dynamic Analysis

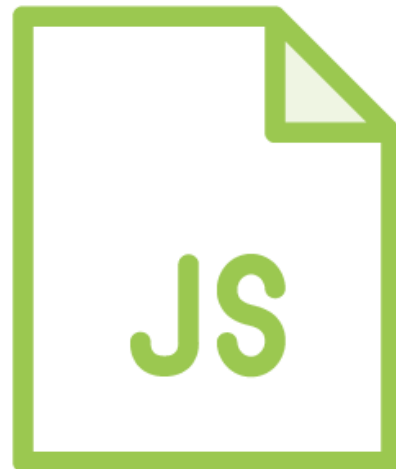


**Monitor Changes**

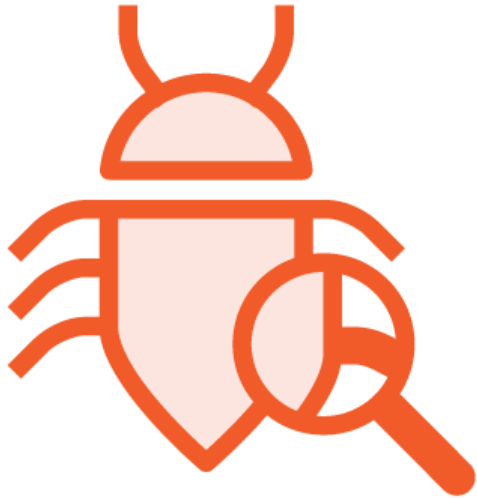


**Behavior Monitoring**

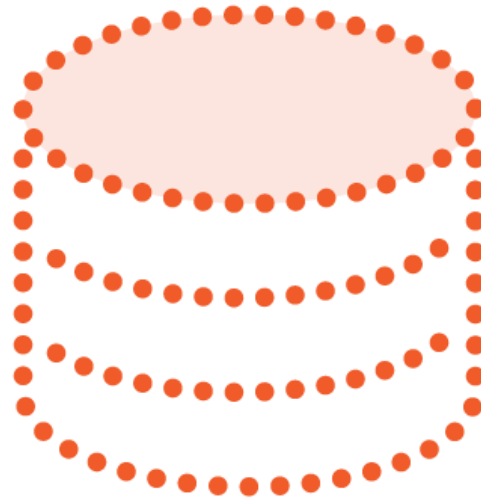
# What Next?



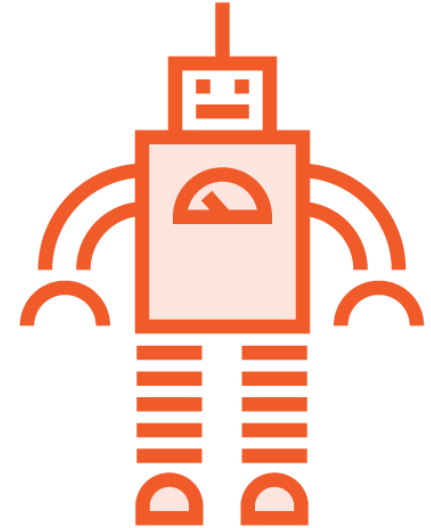
# More Techniques



**Reverse  
Engineering**



**Memory  
Analysis**



**Automation**

# Open Malware

[Home](#) [About](#) [Contact us](#)

**Warning: This site contains live malware.  
Use at your own risk.**

Please note that this site is under active development. Instability might occur.

## Search

Enter your search via MD5, SHA1, SHA256, or an antivirus name.

Search

Open Malware  
Georgia Tech Information Security Center

VirusShare.com - Because Sharing is Caring

Account: [Login](#)

[Home](#) - [About](#) - [Hashes](#) - [Support the Project](#)

Please [login](#) to search and download.

System currently contains 28,378,024 samples.

Please note that this site is constantly under construction and might be broken.

Latest sample added to the system:

MD5	a0bcc129297f7a3b68f9def239cb6801
SHA1	ea52e61cf27305bc55809c7fe5705f6557d987cc
SHA256	5564b157a9211e582d327b5aa21ac9543888e9723dca26306c00a17235a55ecb
3072:BwJ52Y7ZoH5XJawwOa+Kj4haxn9/0kqNrB1/UIKvYYzcd:BwHysw/Oj4haxnJ09Nr/9dVd	
135,979 bytes	
PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive	

<http://openmalware.org>

<http://virusshare.com>







**Safety is extremely important!**



# Summary



**Practice!**

**Use your skills!**

