

# Detecting Malware

---



## **Dale Meredith**

MCT | CEI | CEH | MCSA | MCSE  
Cyber Security Expert

[dalemeredith.com](http://dalemeredith.com) | [Twitter: @dalemeredith](https://twitter.com/dalemeredith) | [Linkedin: dalemeredith](https://www.linkedin.com/in/dalemeredith)

Be prepared, work hard, and hope for a little luck. Recognize that the harder you work and the better prepared you are, the more luck you might have.

**Ed Bradley**

# Investigating Malware

---



**Malware spreads from one system to another with ease and stealth**

<https://t.me/learningnets>

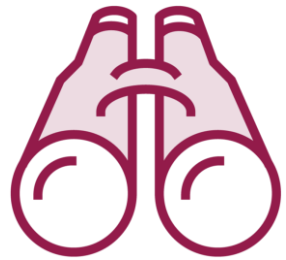


**Malware analysis is a process to determine it's origin, functionality, and potential impact**

# Malware Analysis Objectives



**Determine the malicious intent of the malware and exactly what happened**



**Identify indicators of the compromise and the exploited vulnerabilities**



**Determine the complexity level of an intruder and catch the perpetrator responsible**



**Find signatures for host and network-based intrusion detection systems**



**List the indicators of compromise for different machines and different malware programs**



## Sheep Dip

**Isolate the sheep-dipped computer from other computers on the network to block any malware from entering the system**

### Sheep-dipping tasks:

- Run user, group permission, and process monitors
- Run port and network monitors
- Run device driver and file monitors
- Run registry and kernel monitors



**Install your virtualization**

**Quarantine the network**

**Disable shared folders**

**Copy malware over**



**Before launching..**

# Types of Malware Analysis



## **Static**

**Also known as code analysis**

**Fingerprint**

- Comparing hashes**
- File dependencies**

# Types of Malware Analysis

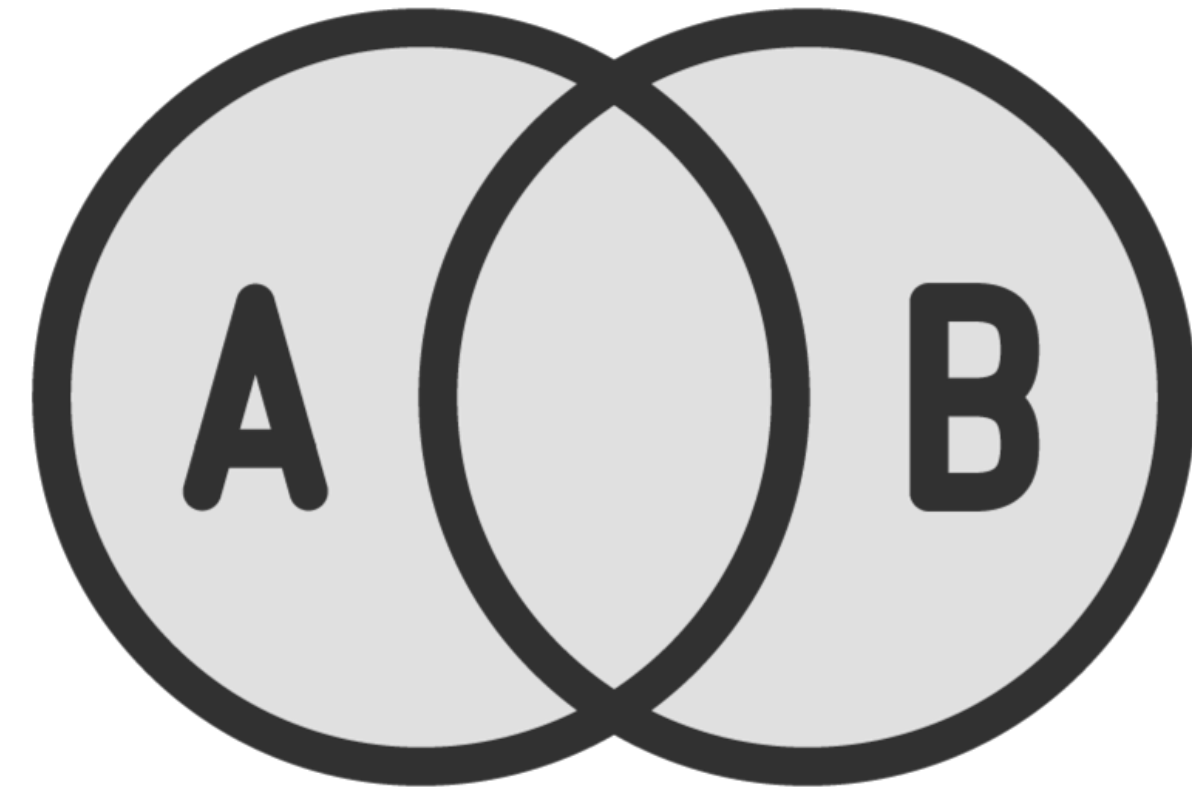


## Static

Also known as code analysis

Fingerprint

- Comparing hashes
- File dependencies



## Dynamic

Also known as behavioral analysis

Baseline of system

Host integrity monitor

Ports, processes, registry,  
and services



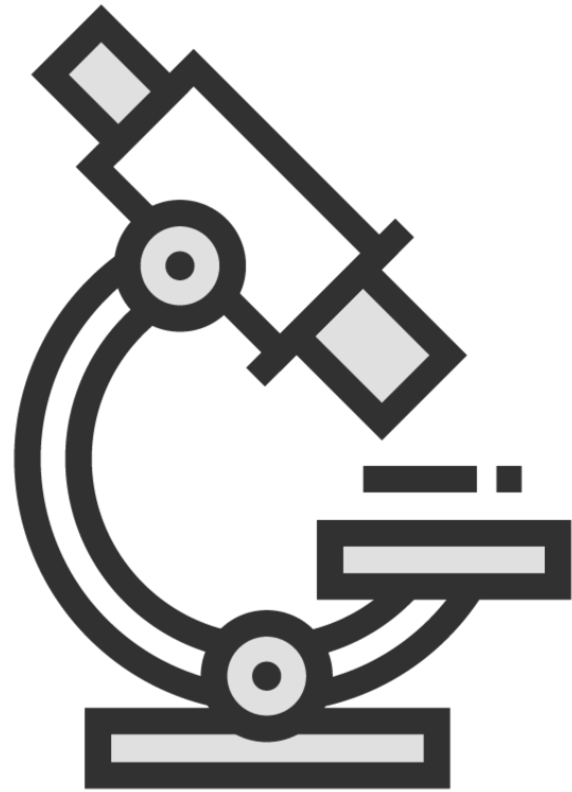
## The Goal:

**Run a service as a system account**

**Watch which programs get placed inside your start-up**

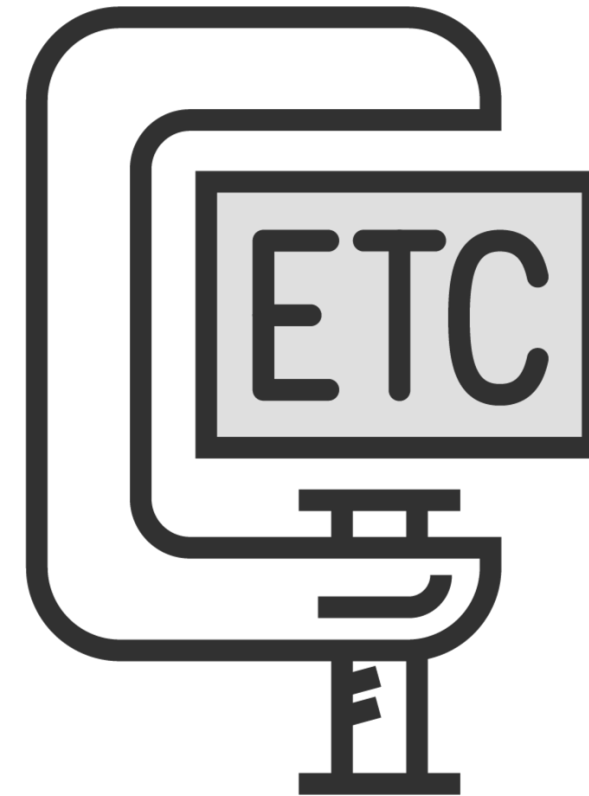
**Monitor your registry**

# Fire It Up



**BinText**

Collect string values inside binaries



**UPX**

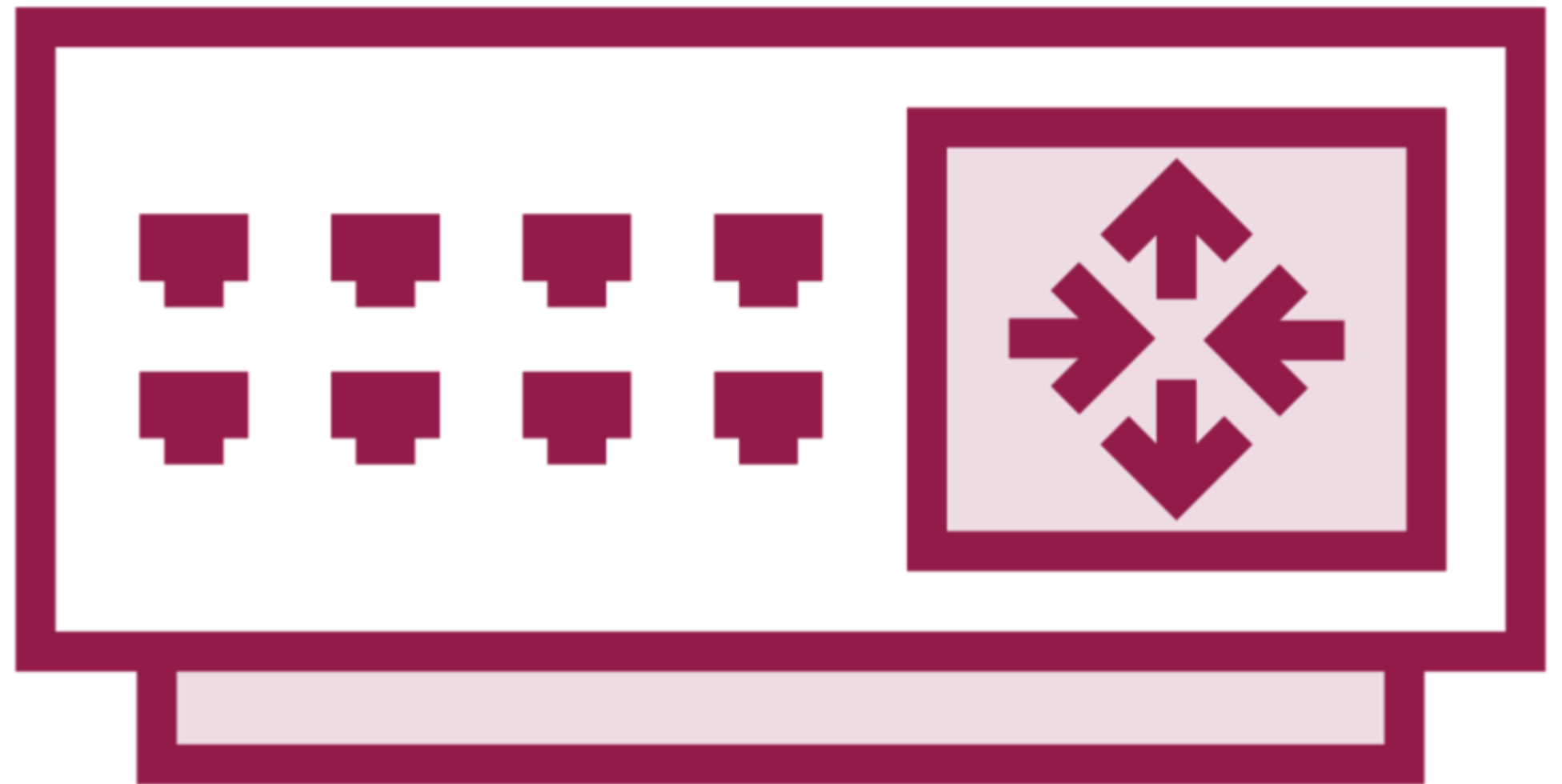
Collect compression methods

# Investigation Continues

---

**Monitor your ports**

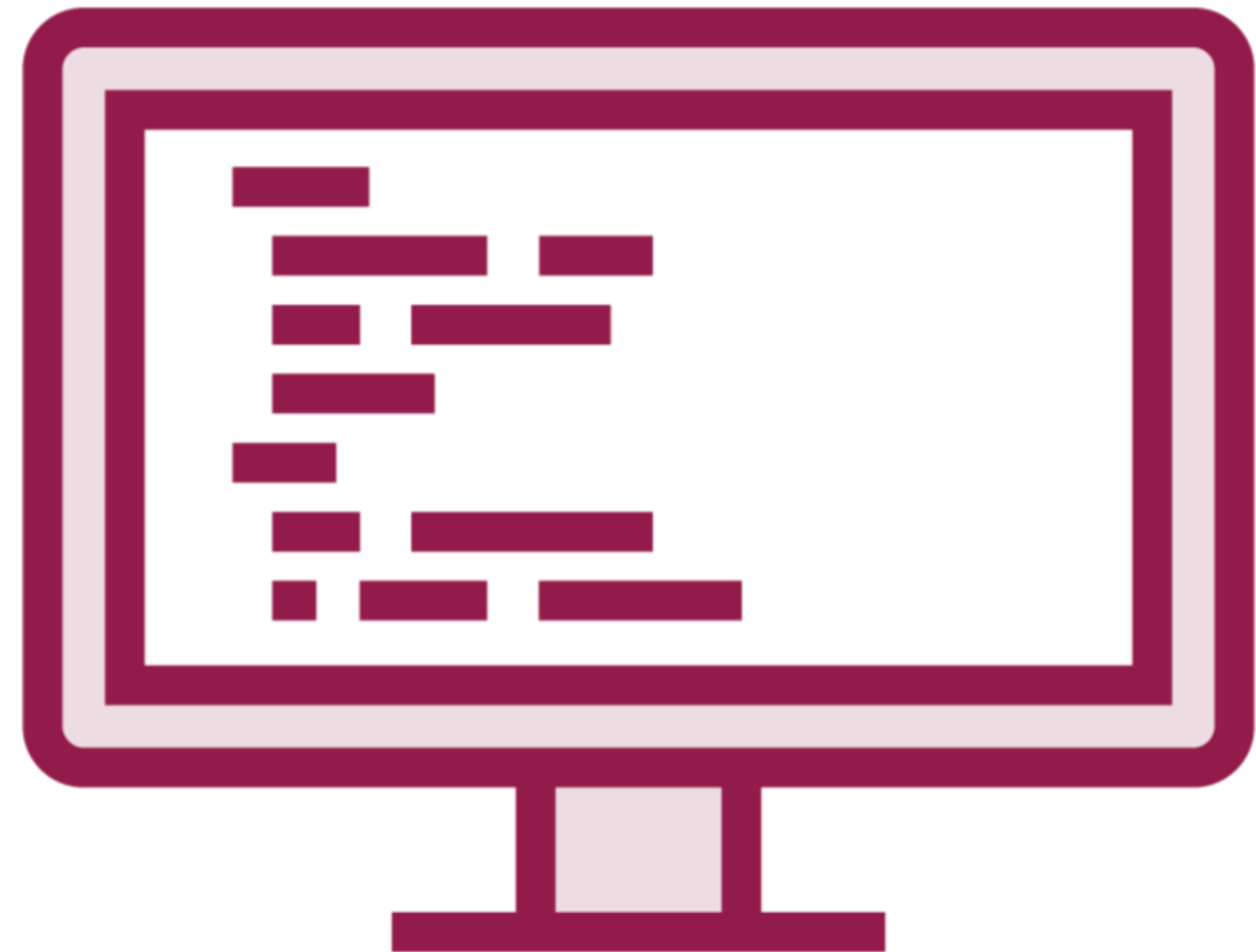
**Sysinternals:**  
Process explorer  
and/or process  
monitor



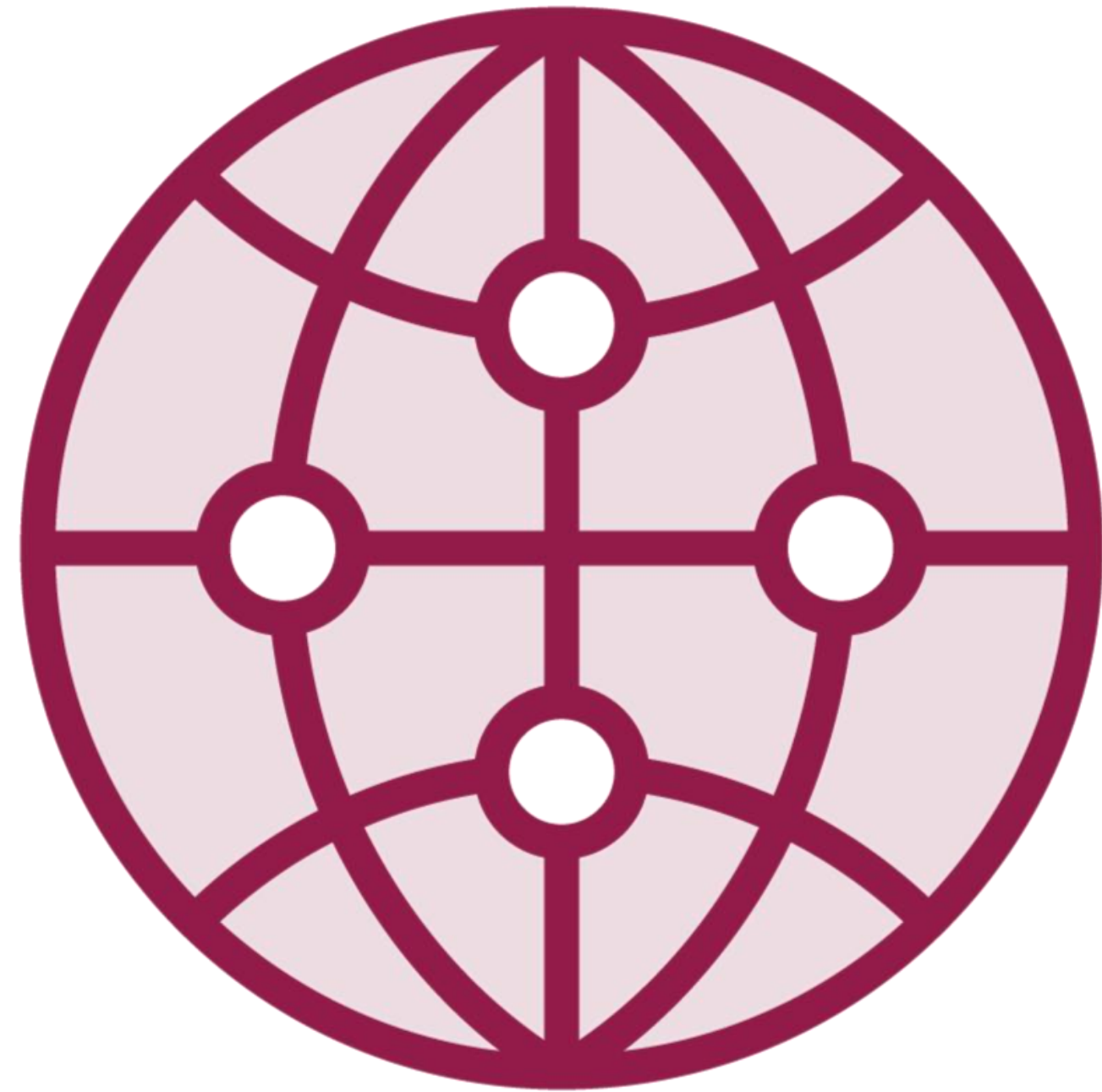
**Look for installation  
instructions**

**Look for installation  
locations**

**IDA Pro**



**Online Malware Testing**  
**-VirusTotal**



Demo



**Autoruns**

**Virus Total**

# Investigation Still Continues

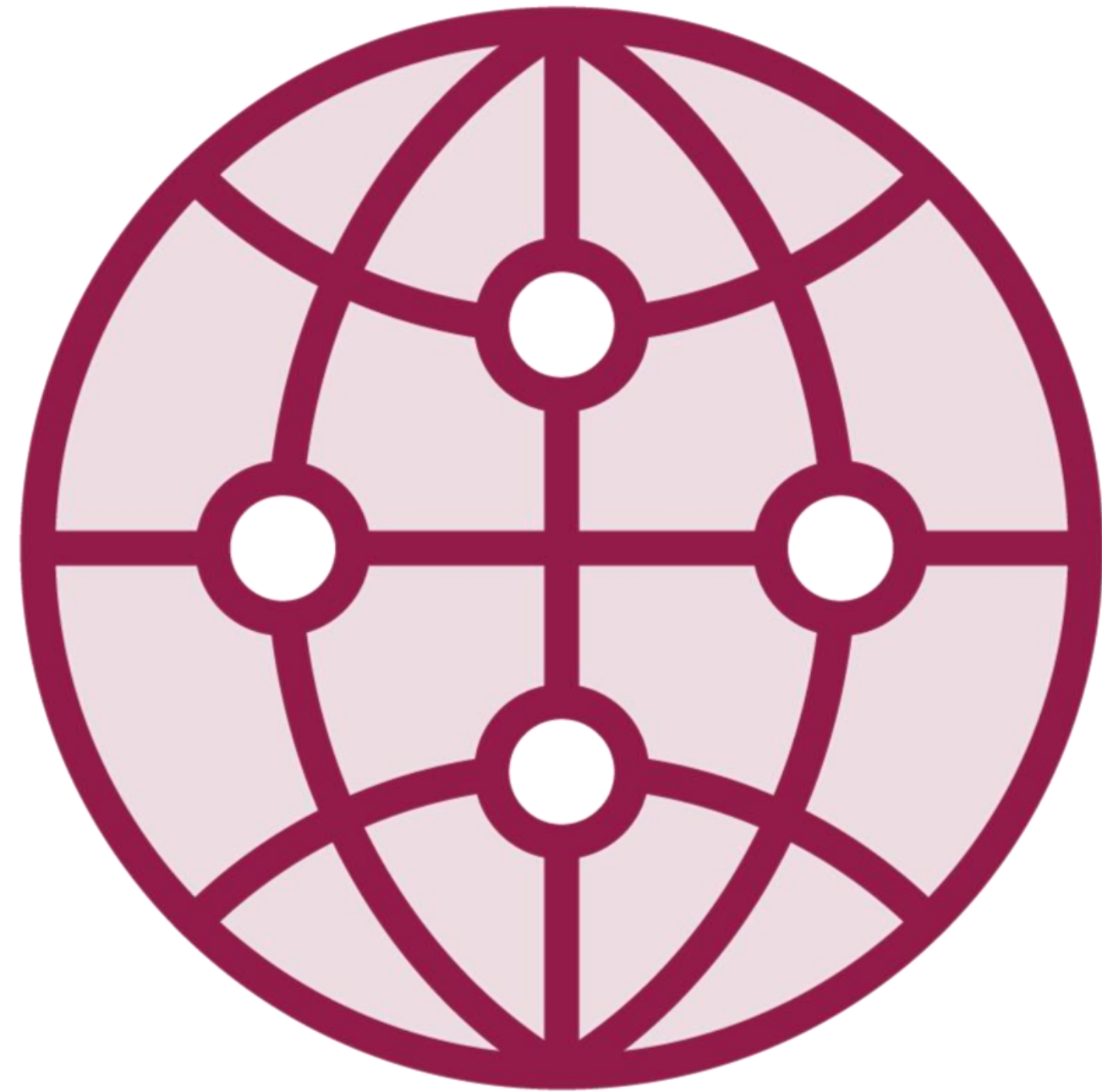
---

## Online Malware Testing

-VirusTotal

-Microsoft Security  
Intelligence

-Avast – online scanner





# Common Questions



**What is the intention of the malware**



**Who are the perpetrators, and how good are they**



**How did it get through**



**How do we abolish the malware**



**What is its impact on the business**



**How long has the system been infected**

What are the preventive measures?

# Key Guidelines for Malware Analysis



**Pay attention to essential features**



**Try different tools and approaches**



**Identify, understand, and deploy prevention techniques**

# The Creation Process

---



Que the lightning and evil laugh as creation is easier than you think

Some are more in-depth and require unique tools

Easy shamasy:

- JPS Virus Maker
- IWMT



Demo



**JPS Virus Maker**

**Internet Worm Maker Thingy**



# Tools

---

Tools to Be  
Familiar  
With



# Holy Arsenal Batman!

**TCPView**

**AutoRuns**

**DriverView**

**System File Checker (SFC)**

# Demo



**TCPView**

**DriverView**

**System File Checker (SFC)**

# Learning Check

---

# Learning Check



**Sheep dipped**



**Static**



**Online Malware Analysis**



**TCPView**



**Dynamic**



Up Next:

Deploying Countermeasure for Malware

---