## Dynamic Analysis Process

Dynamic Analysis is reviewing the executable while it is running the code.

### Stage 1: Switch the Virtual Machine to an isolated network

In Hyper-V, switch the Virtual Machine to an internal-only network.

Graphical user interface, text, application, email

Description automatically generated

Create an export or snapshot of the VM to allow rollback, Right-click on the VM and select Checkpoint.

A picture containing graphical user interface

Description automatically generated

### Stage 2: Running the tools

On the VM, run the tool ProcMon, disable the capture and clear it.

Graphical user interface, text, application

Description automatically generated

Start FakeNet; this will create a fake network to trick the malware and document calls

A screenshot of a computer

Description automatically generated with medium confidence

Run RegShot, update the scan to "C:\" and set the output path. Click on 1st shot to capture the first snap, this process will take a few minutes

Graphical user interface, application

Description automatically generated

Start the ProcMon capture

Graphical user interface, text

Description automatically generated

Execute the Malware and leave it running for 5 minutes. You will start to see traffic in FakeNet, ProcMon and other signs on the system, like popups etc.

Graphical user interface, text

Description automatically generated

Stop the ProcMon capture

Graphical user interface, text, application

Description automatically generated

Using RegShot capture, the 2nd capture

Graphical user interface, application

Description automatically generated

### Stage 3: Review the results

In RegShot, select compare and show output

Graphical user interface, application

Description automatically generated

In the output, you will notice a registry written in this example showing a persistence registry key.

Text

Description automatically generated with low confidence

This also matches the registry key found in the user's hive.

Graphical user interface, text, application

Description automatically generated

In ProcMon, perform a filtered view and review the results

Add the following filters:

* ProcessNameis: malware-name
* Operation is:
  + WriteFile
  + SetDispositionInformationFile
  + RegSetValue
  + ProcessCreate

Graphical user interface

Description automatically generated

Save the output for ProcMon and RegShot

Open the PCAP file created in FakeNet using WireShark to view any HTTP or network requests

Graphical user interface, text, application

Description automatically generated

In this case, no network traffic was recorded.

### Stage 4: Resetting VM

Once the review has been completed. The VM will need to be reset. In Hyper-V right, click on the VM and select revert to reset the VM.

Graphical user interface, application, Word

Description automatically generated