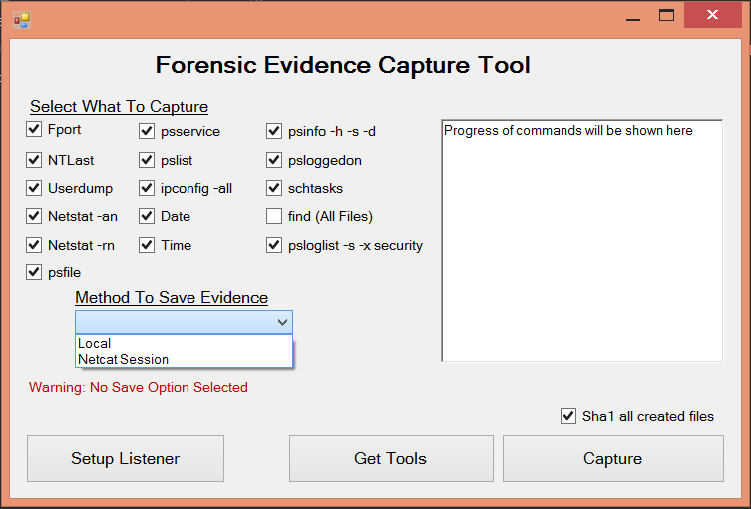
# Read Me

## Purpose

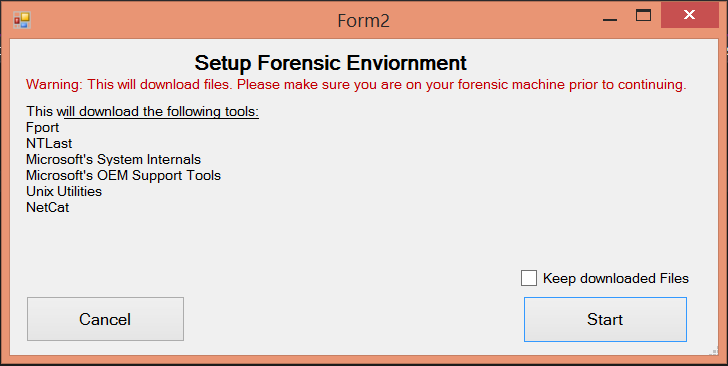
To facilitate the gathering of forensic evidence on Windows based hosts.

## Setting up

1. After starting up the executable download the tools needed for the evidence you are wanting to collect by clicking “Get Tools.”



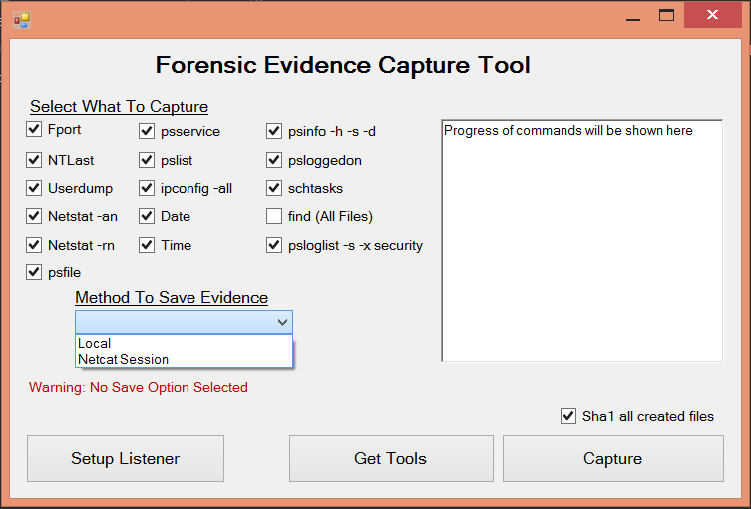
1. The “Keep downloaded tools” option will not delete the .zip files downloaded from the individual sources.
2. Click “Start”
3. Once the process is complete click “Cancel” to get back to the start screen.



## 

## Run Capture

1. Check the box next to each of the forensic reports you’d like generated.
2. Select your “Method To Save Evidence”
   1. Local - will save the generated output to this current machine.
   2. Netcat Session - Gives you the option to enter in an IP Address and Port number of the Netcat session running on your Forensic workstation.
3. Click “Capture” to generate the reports.



## 

## Setup Netcat Listener on Forensic workstation

1. This will download and run Netcat on your Forensic workstation.
2. Enter in the port you would like Netcat to listen on (ie. 6565)
3. Click “Start Listener” to run the listener.
4. Once your commands have been run on the victim machine the output is generated in one file. To separate the commands into individual files and create a Sha1 hash of each file (if the option is checked), click the “Parse” button. This will save the individual files to “/Evidence/” folder.

