Magnet RESPONSE CLI Guide

The following CLI (command-line interface) parameters can be used to automate running Magnet RESPONSE from a command line:

Case setup / General options

- /accepteula
  - Indicates you accept the End User License Agreement so you aren't prompted to agree to the EULA via the GUI
- /nodiagnosticdata
  - Turns off diagnostic logging. If this switch is not present, diagnostic logging is enabled.
    Leaving this option enabled will allow diagnostic information to be gathered and sent to Magnet Forensics regarding usage of the RESPONSE program. This information is extremely helpful in the development of this tool and no identifying information or content is sent.
- /unattended
  - Disables any pop-up GUI dialogs that otherwise might be displayed in non-automated operation, and does not wait for any user input at the end of the collection (i.e. exits automatically at the end).
- /output:<output folder path>
  - Specifies the output folder to be used. **Required.**
    e.g. /output:"d:\all cases\RESPONSE_Collections"
- /caseref:<case reference>
  - The case reference for this collection. **Required.**
    e.g. /caseref:"23-123456"
- /drive:<drive letter to be scanned>
  - Allows you to specify which drive to target collection from. If this switch is not specified, then the system drive is targeted.
    e.g. /drive:D

Capture options

- /captureram
  - Enables RAM capture
- /capturepagefile
  - Enables capture of pagefile.sys file
- /capturevolatile
  - Enables volatile data capture
- /capturesystemfiles
  - Enables critical system file collection
- /captureextendedprocessinfo
  - Enables extended info capture for running processes/loaded modules
- /saveprocfiles

  - Enables saving copies of running processes/loaded modules. Must be used with /captureextendedprocessinfo switch
- /capturefiles:<comma separated keywords>
  - Enables scanning for files with filenames containing specified keywords e.g. /capturefiles:secret,badfile,.vbs,confidential
- /skipsystemfolders
  - Indicates that the Program Files/ProgramData/Windows folders should be skipped when searching for files based on filename keywords. Must be used with /capturefiles
- /maxsize:<file size in KB>
  - Indicates the maximum file size to collect from hits found using /capturefiles – any files above this size are skipped e.g. /maxsize:500
- /captureransomnotes
  - Enables the ransomware ransom note collection

Note: If none of the above switches are specified, then all options are enabled by default.

Verification

- MagnetRESPONSE <path to RESPONSE collection ZIP file>
  - Specifying only the full path to a previously collected RESPONSE ZIP file package causes RESPONSE to run a verification on that ZIP file and output a simple text file report indicating if the verification was successful. Currently, this option is not automatable – no other switches can be specified when using this option and user input is required to exit after the verification is completed.

Auto-collect options

These options can be useful if you are providing the tool to a non-technical operator to simply capture the data and bring it back to you for processing/analysis. This executable file naming method can be combined with the above CLI options, but should be used with caution (and thoroughly tested) as the below configurations will take priority over the CLI switches and the CLI switches are applied afterwards, which may result in unintended behavior.

Option 1 - Capture Everything

Rename the executable to have the text "AutoCapture" anywhere in the filename. All options will be enabled and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs from.

Option 2 - Minimal Capture

Rename the executable to have the text "AutoCaptureMinimal" anywhere in the filename. Only the "Volatile Data" and "Critical System Files" options will be enabled (no extended info saved for running processes), and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs from.