Magnet RESPONSE Quick Start Guide

RESPONSE is an evidence collection and preservation tool, targeted towards Incident Response cases and the data that is relevant to those investigations. It's designed to be portable (runs from a USB drive), simple/easy-to-use and fast, with low/no training required to operate the tool, while still targeting a comprehensive set of files and data that is relevant to IR investigations. Please send any feedback/issues/requests to us, we'd love to hear from you. Thanks for your support!

To conduct a RESPONSE capture, start the tool and enter a case reference/number, select your capture options, and an output location.

The output will be saved to a standard ZIP file, and if RAM is selected for capture, it is saved separately to a .bin (raw dump) file. File integrity data is saved within the ZIP file that can be used to verify that the ZIP contents have not been altered/corrupted. A file within the ZIP contains the hash value for the captured RAM if any verification needs to be done on that file.

Saved files & RAM can be processed/analyzed in a forensics tool like Magnet AXIOM/AXIOM Cyber (add the ZIP file as a Computer/Windows image, and the RAM as a Memory Image).

Verifying a capture package

To verify the ZIP, simply drag and drop it on to the RESPONSE executable. RESPONSE will launch as normal and go directly into a verification process, providing a message at the end indicating if the verification was successful. A text file containing details of the verification is saved to the same folder.

Capture options explained

Capture RAM – Captures all RAM memory to a .dmp (Microsoft crash dump format) file, leveraging the **DumpIt** RAM capture tool. If the **DumpIt** tool fails, the **Magnet RAM Capture** tool is automatically run as a fall-back measure.

Capture pagefile.sys – Captures the pagefile.sys file, immediately after RAM is captured (if enabled).

Collect Volatile Data – Saves the following items:

- Network connections
- Running processes (basic list)

- Logged-on users
- Scheduled tasks
- IP config info
- Firewall info
- Wi-Fi info
- Windows services
- Local users accounts
- Windows version details

Data is saved to individual text files to enable quick review.

Collect Critical System Files – Collects the following files/locations:

- Amcache data
- AnyDesk Logs
- Chrome Browser History
- Edge Browser History
- Firefox Browser History
- Firewall Logs
- Jumplist files
- LogMeIn Logs
- Master File Table ($MFT)
- NTUSER.DAT files
- PowerShell history
- Prefetch files
- Program Compatibility Assistant files
- Recent Link files
- Recycle Bin
- Registry Hives
- Scheduled Tasks
- SRUM data
- TeamViewer Logs
- UsrClass.dat files
- Windows Event Logs
- Windows Timeline data

Capture Running Processes - Extended Info – This option collects more data about running processes (and loaded modules in memory), saving hash values, metadata, and an entropy value from identified files which can be used to enable post-collection lookups/enrichment in another tool.

If this item is not checked, but "Volatile Data" is, a more basic list of running processes will still be captured.

Sub-option: Save copy of located processes/loaded modules – If this option is checked along with the **Capture Running Processes – Extended Info** option, copies of the located running processes/loaded modules (EXE’s/DLL’s) will be saved to the output ZIP file for analysis on another system.

Collect Files – Collect ransomware ransom note files – This option attempts to locate and save ransomware ransom note files based on file names/keywords that are known to be used by ransomware.

Collect Files – Save a copy of files containing these keywords – This option attempts to locate and save copies of files based on user-specified keywords/file extensions. Some file extensions are pre-populated for the collection of script files commonly seen used by malware.
If a file named "collectkeywords.txt" is present in the same folder as the RESPONSE executable, it will be loaded and the contents (one keyword per line) are leveraged as keywords for file collection, instead of the default keywords.
There is a sub-option that will direct RESPONSE to skip the Program Files / ProgramData / Windows folders to reduce noise / number of files collected, and another sub-option that allows you to specify a maximum file size – any files larger than this size will not be collected.

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.

Option 1 - Capture Everything

Rename the executable to have the text "AutoCapture" (no quotes) 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" (no quotes) 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.