Responding at Scale with Magnet RESPONSE

Doug Metz, Security Forensics Consultant
Magnet Forensics

Who Am I

```
PS /Users/dmetz> gc ./whoami.txt


Security Forensics Consultant with Magnet Forensics.
Over 15 years in Incident Response supporting government, private sector, and academic institutions.
(former) Global Incident Response Manager for a Fortune 200 company.

HTCIA Delaware Valley-Philly Chapter
Volunteer for The Magnet Auxtera Project
PowerShell Enthusiast
ND Alumni #GoIrish

Blog:     https://bakerstreetforensics.com
GitHub:   https://github.com/dwmetz

Mastodon: https://infosec.exchange/@dwmetz
LinkedIn: https://www.linkedin.com/in/dwmetz/
Twitter:  @dwmetz
```

SEEK JUSTICE. PROTECT THE INNOCENT.

BAKER STREET FORENSICS

D . F . I . R .

WHERE IRREGULARS ARE PART OF THE GAME

HTCIA

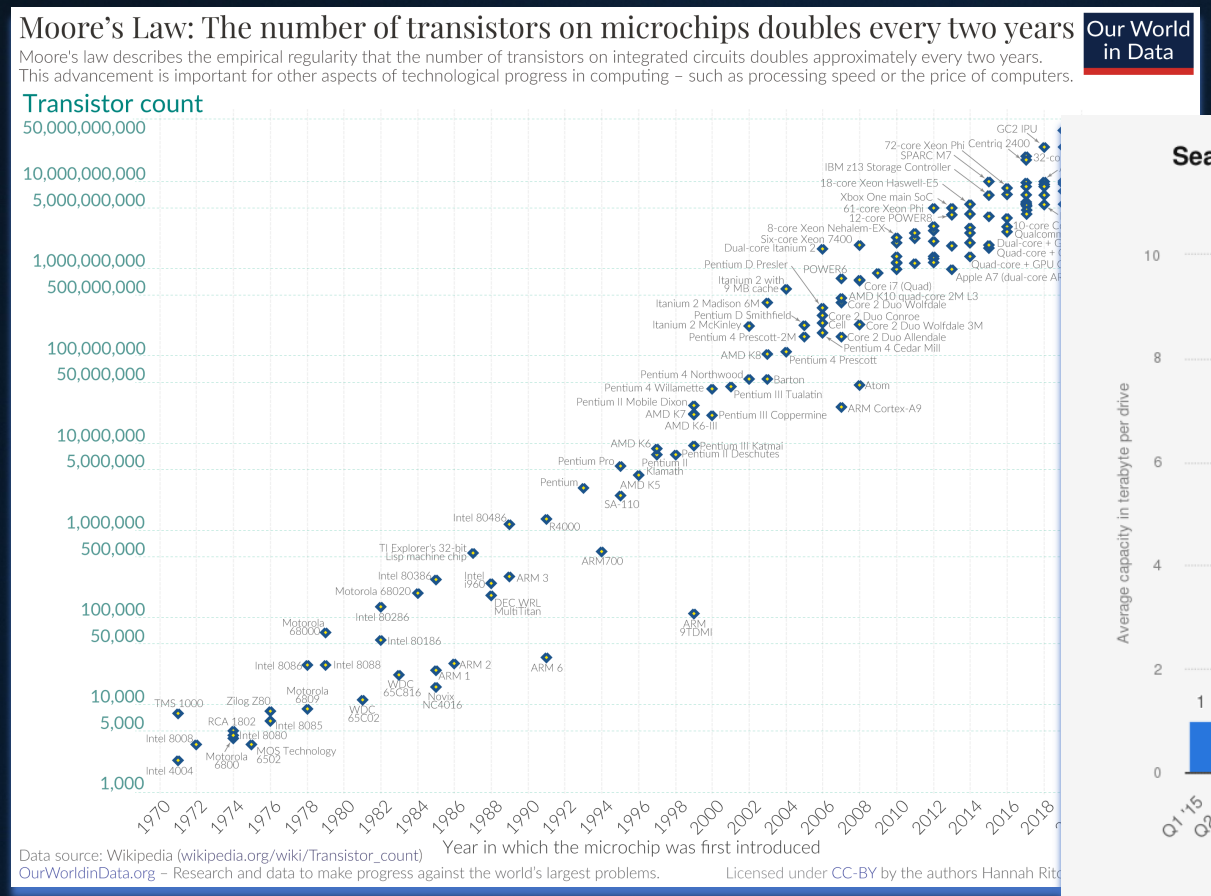
MAGNET FORENSICS®

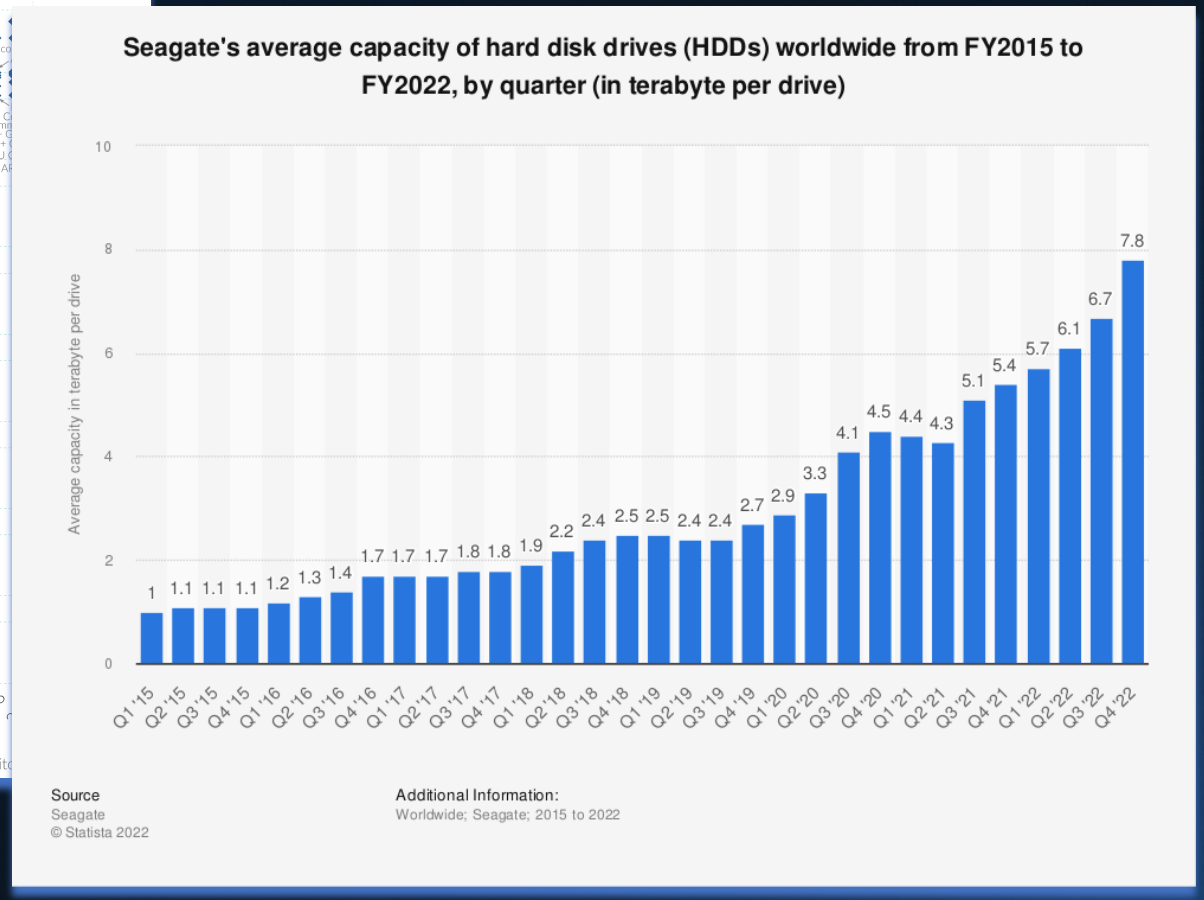
magnetforensics.com

Agenda

- Magnet RESPONSE introduction, operation and output
- Processing tips for AXIOM Cyber
- Responding at Scale with PowerShell and the RESPONSE CLI
- Turn it up to 11 with Magnet AUTOMATE

MAGNITUDES OF DATA





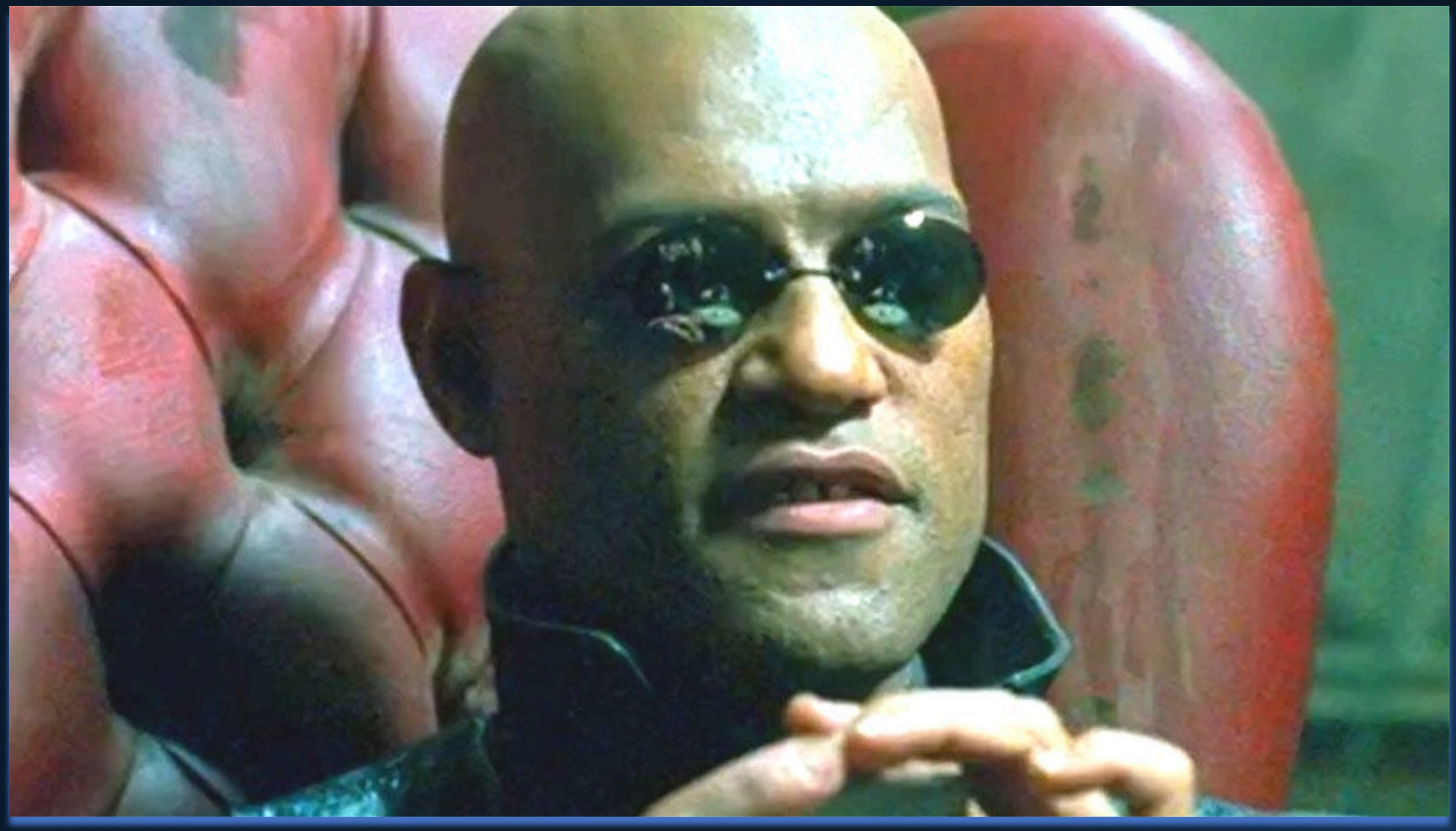
Sources:
https://en.wikipedia.org/wiki/Moore%27s_law#/
https://www.statista.com/statistics/795748/worldwide-seagate-average-hard-disk-drive-capacity/

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

What If I Told You

Less than 5% of the data is critical to 99% of the investigation?



triage noun

tri·age trē-ˈäzh ˈtrē-ˌäzh

1 **a** : the sorting of and allocation of treatment to patients and especially battle and disaster victims according to a system of priorities designed to maximize the number of survivors

b : the sorting of patients (as in an emergency room) according to the urgency of their need for care

2 : the assigning of priority order to projects on the basis of where funds and other resources can be best used, are most needed, or are most likely to achieve success

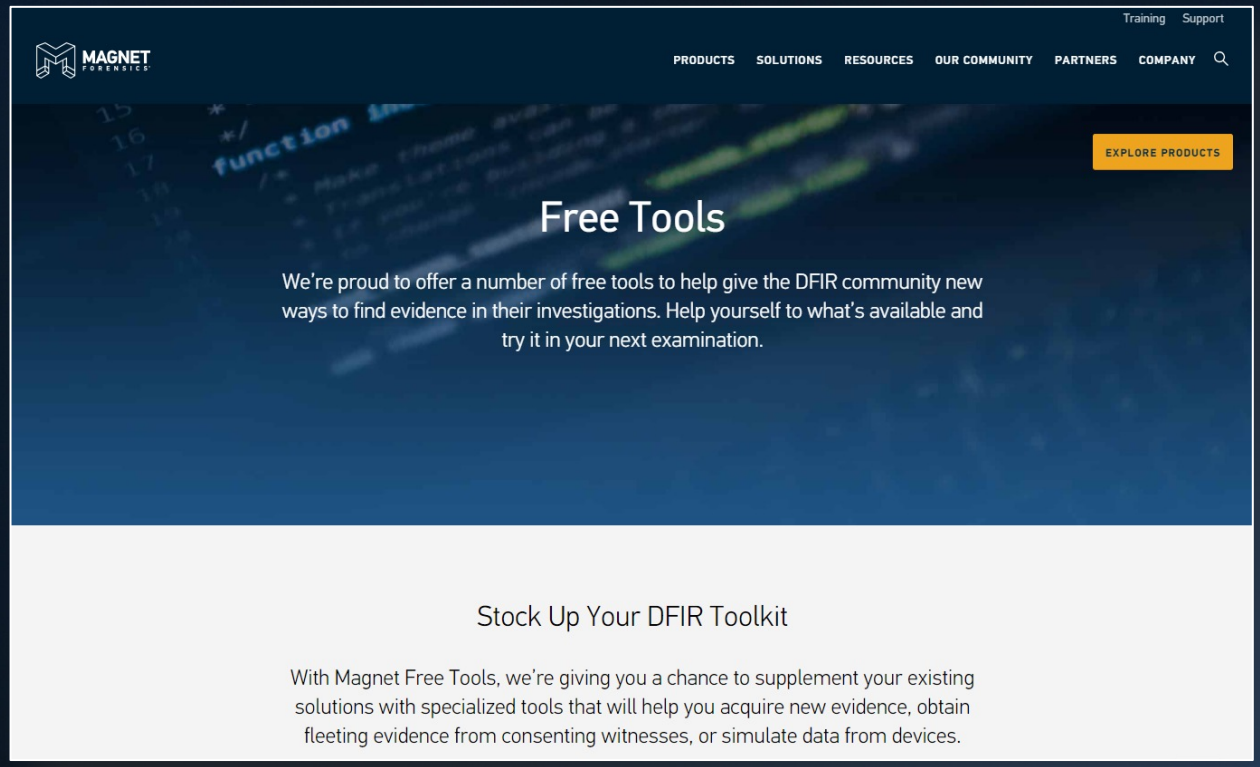
triage transitive verb

Source: https://www.merriam-webster.com/dictionary/triage

MAGNET FREE TOOLS

- Magnet RESPONSE
- Magnet DumpIt for Windows
- Magnet RAM Capture
- *…. (more)*

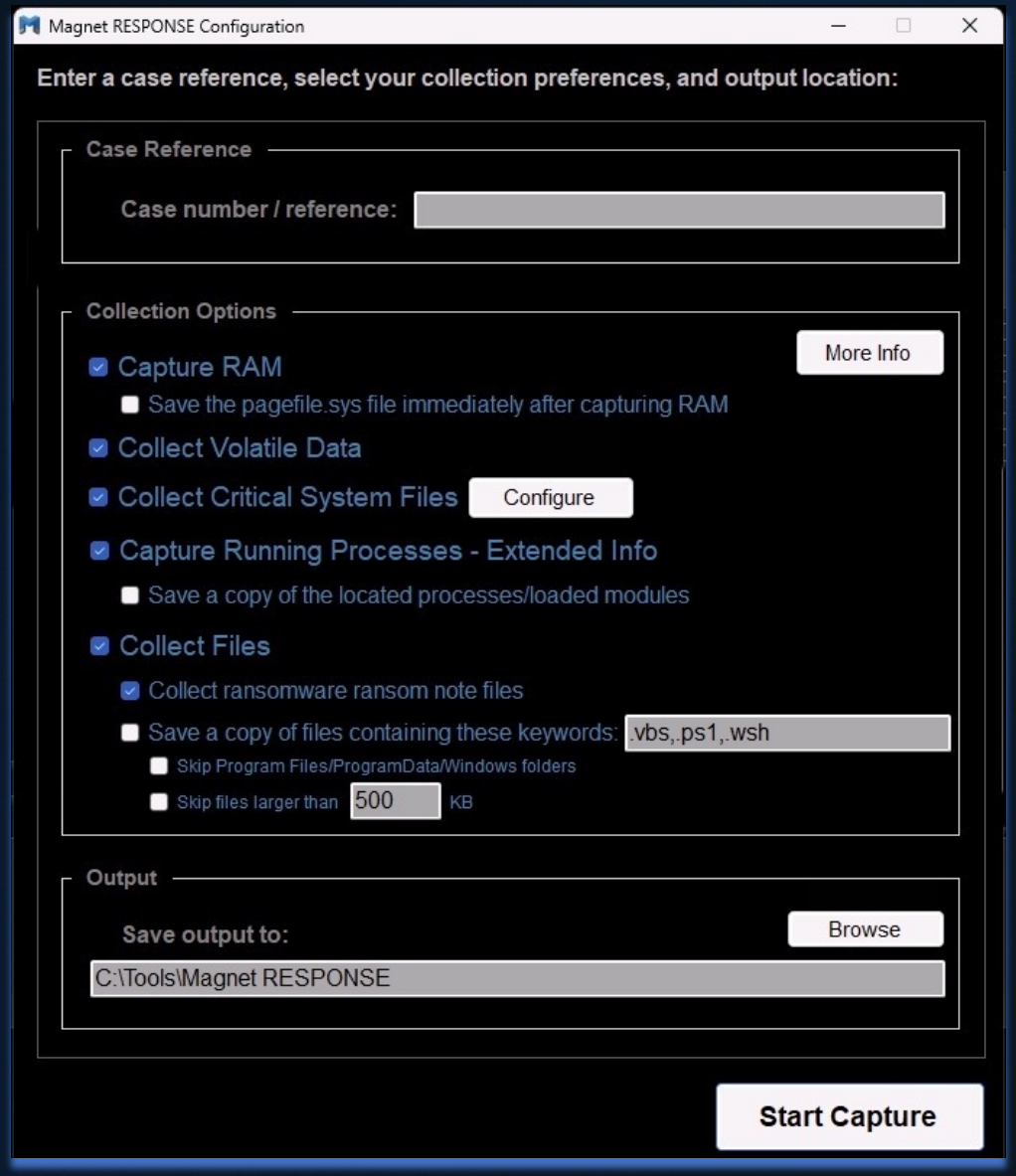
https://www.magnetforensics.com/free-tools/



MAGNET FORENSICS®

SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNET RESPONSE



Magnet RESPONSE lets investigators and non-technical users easily collect and preserve critical data relevant to incident response investigations from local endpoints.

Minimal to no training is required—it's as simple as entering a case name, selecting the collection options and then "start capture."

This makes Magnet RESPONSE useful in situations where non-technical users may need to collect and preserve data on behalf of law enforcement investigators as part of a cyber incident investigation.

https://www.magnetforensics.com/resources/magnet-response/

MAGNET RESPONSE

Auto-collect Options

These options can be useful if you are providing the tool to a non-technical operator (NTO) 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. 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.

MAGNET RESPONSE

Highlights

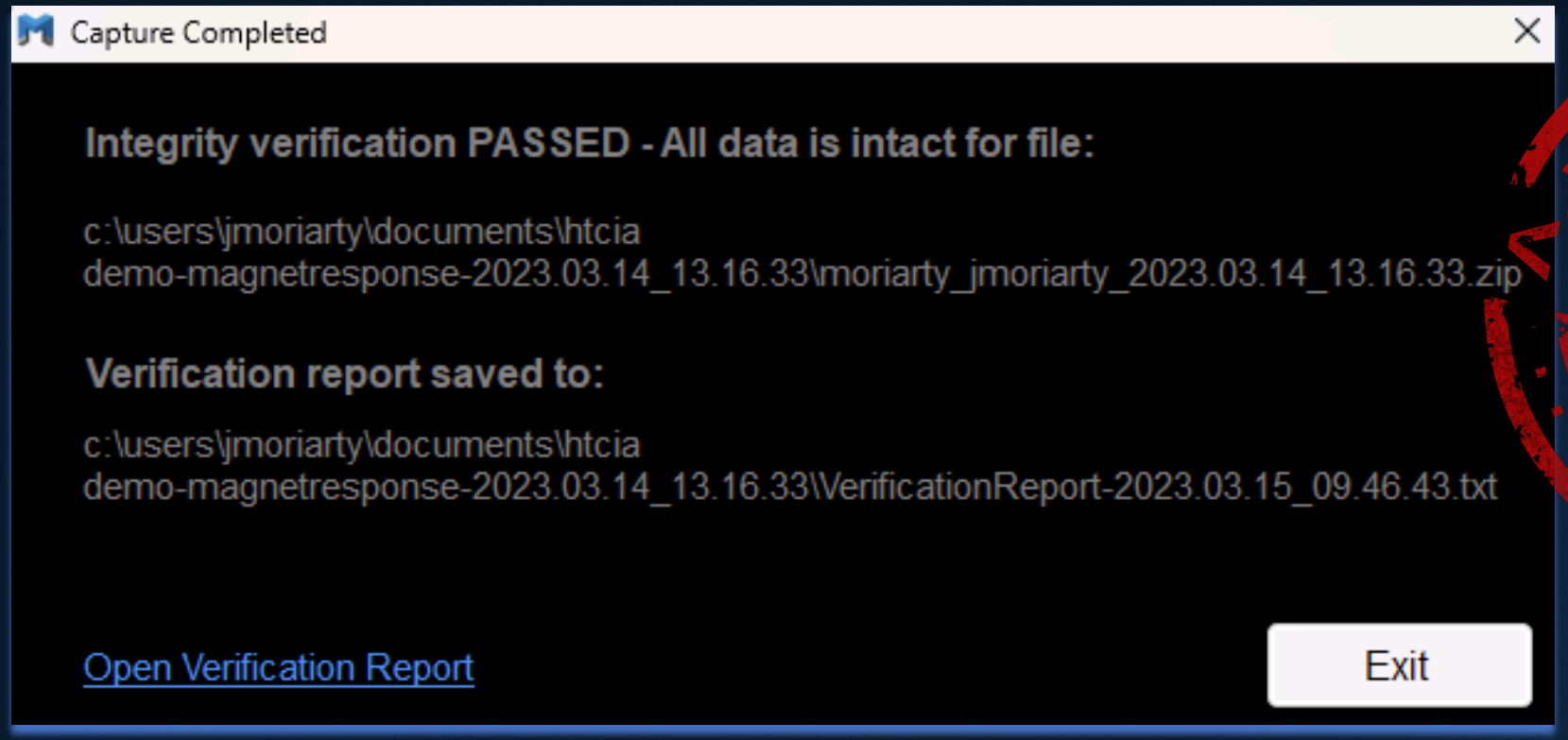
- **Easy-To-Use:** A guided two-step process and progress bar is straightforward for even non-technical users to use
- **Fast & Comprehensive**: Collect and preserve data starting with the most volatile using the built-in Comae RAM capture (MAGNET DumpIt) functionality, and volatile data and files commonly associated to cybercrime, such as Windows Event Logs, Registry Hives, Jumplist files, and many other log files in minutes
- **Portable:** It is compromised of a single executable file (less than 2MB), is easily downloaded, and can be stored and run from a USB drive
- **Collect by Keyword & Skip Large Files:** configure free-form collections using your own set of keywords with the option to limit the size of files collected to maintain speed
- **Consolidated Output:** Output is saved as a .zip file for easy delivery or processing and analysis, manually, in Magnet AXIOM Cyber and with Magnet Automate
- **Data Integrity:** An embedded hash value is provided to verify the integrity of the data

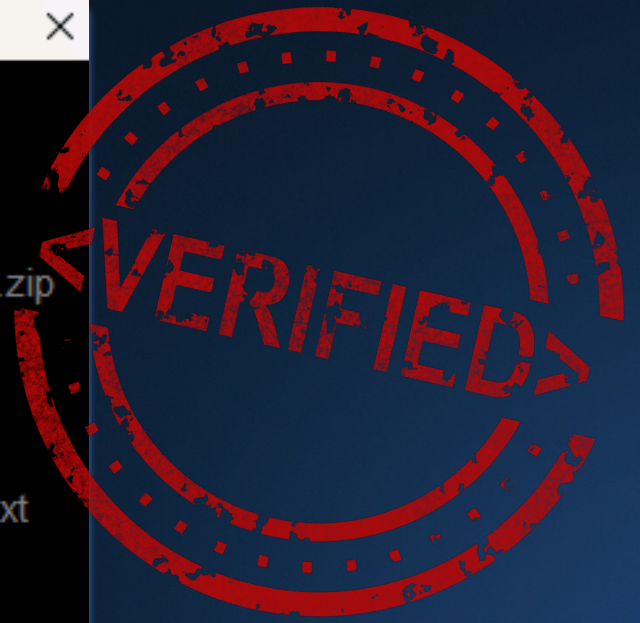
SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNET RESPONSE

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.

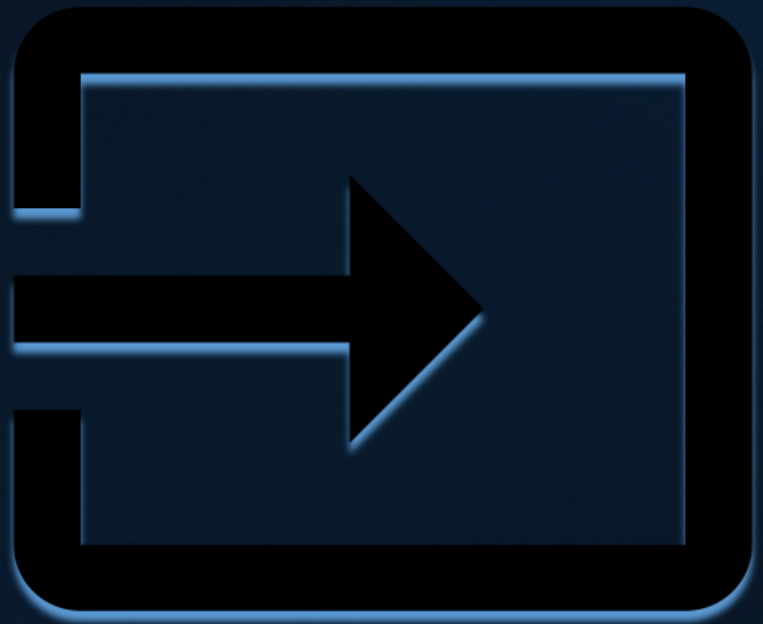


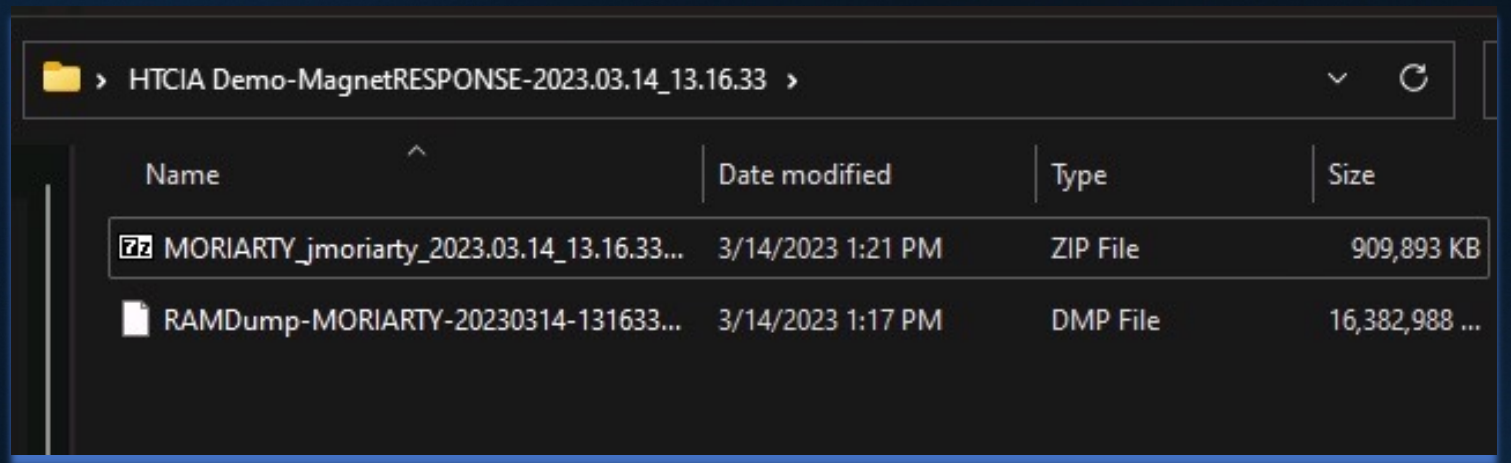


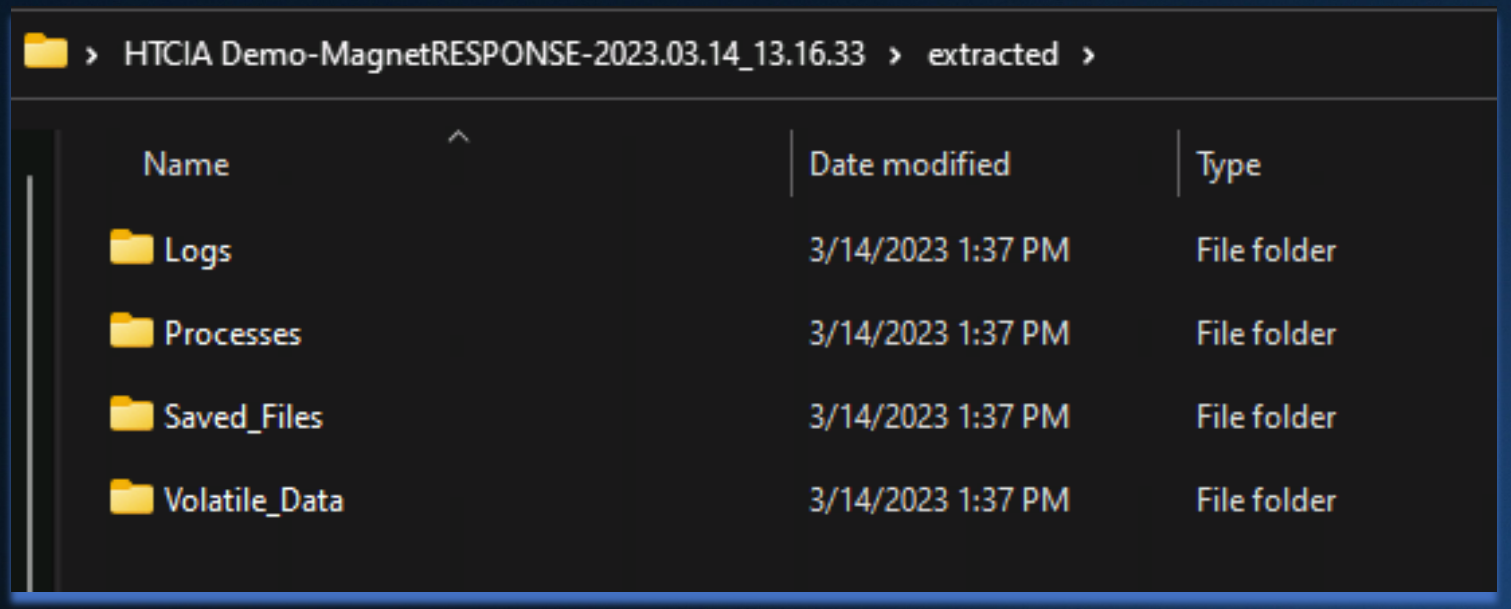
HARDWARE CHOICES

- Samsung T5 or T7

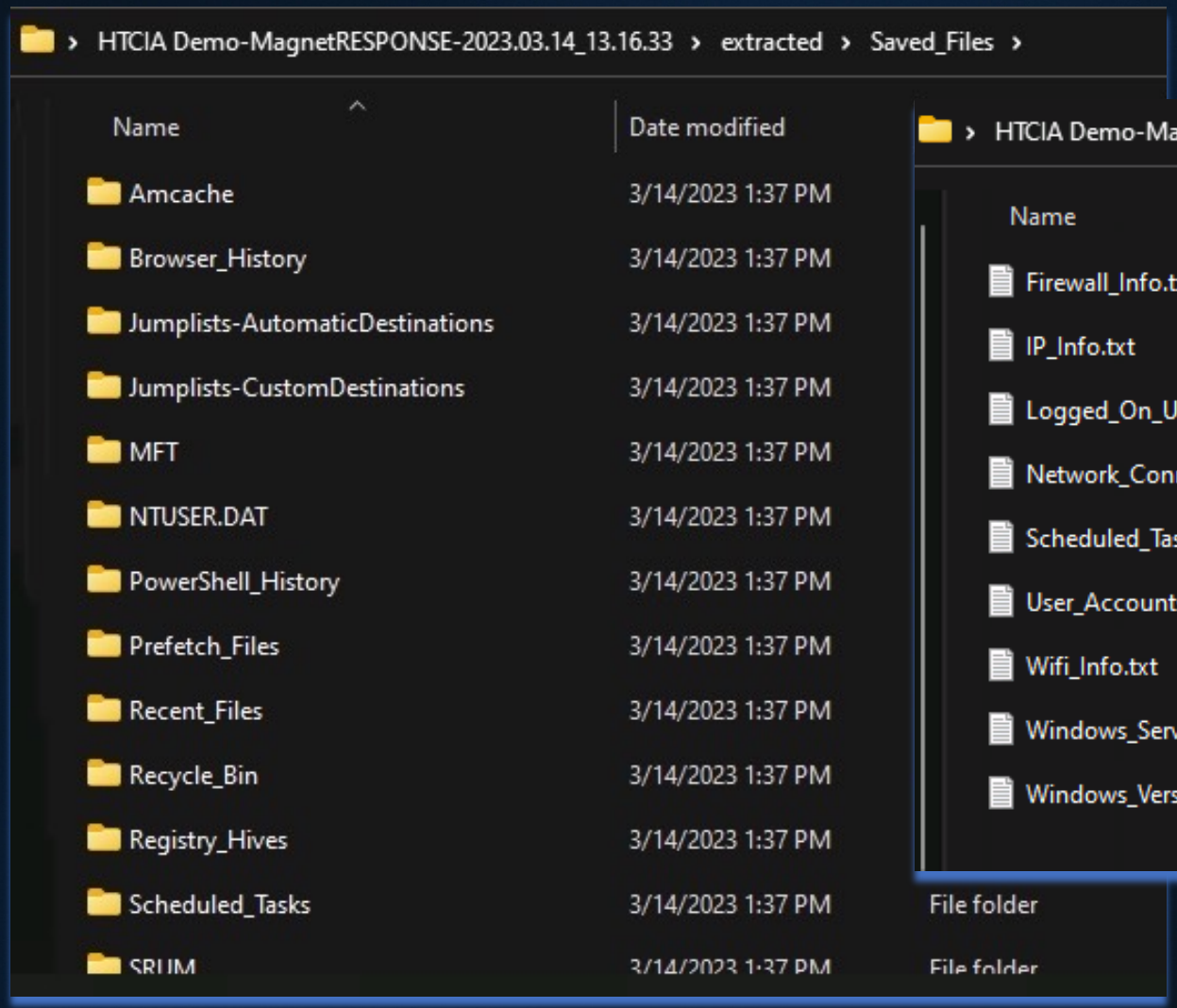
MAGNET RESPONSE: OUTPUT

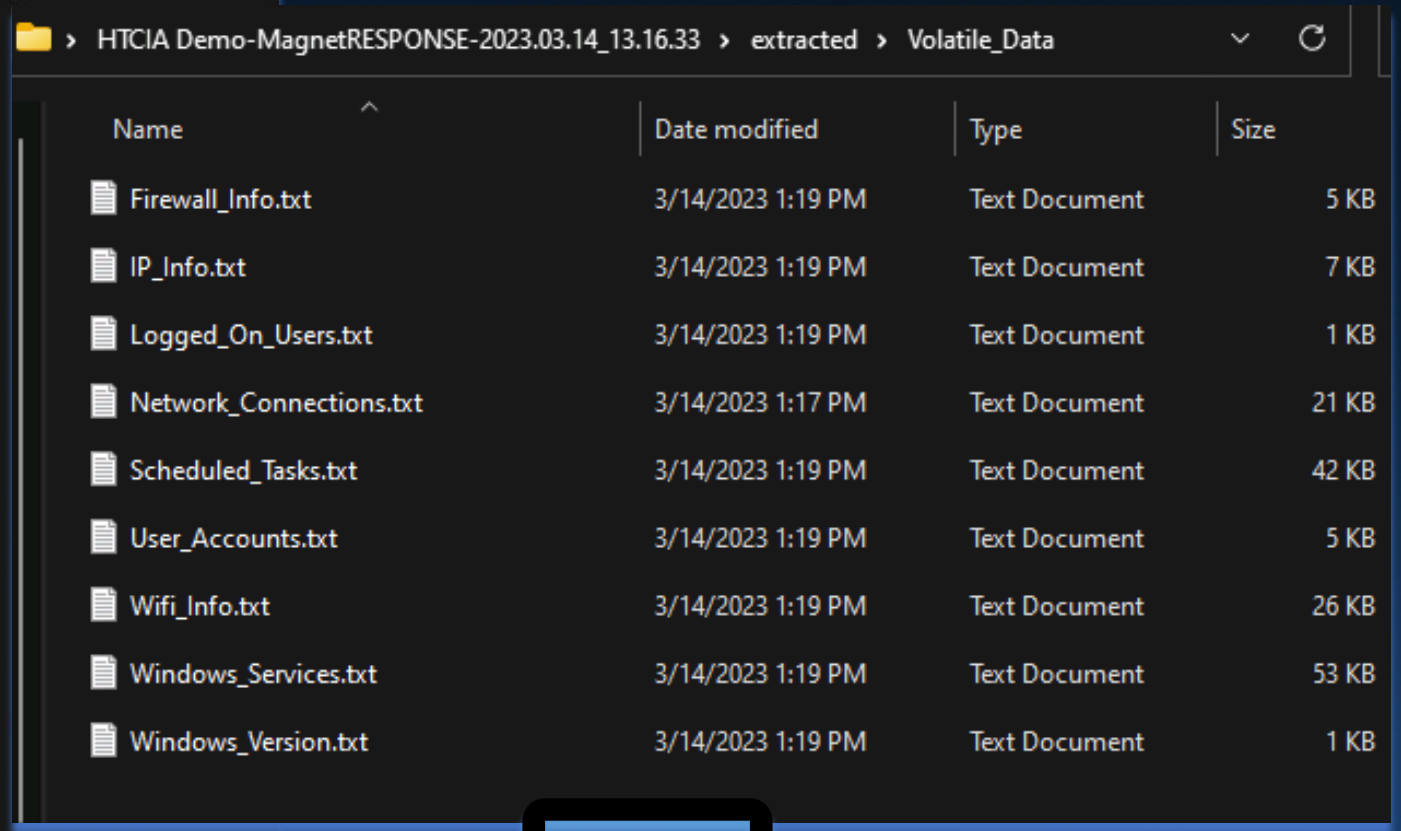


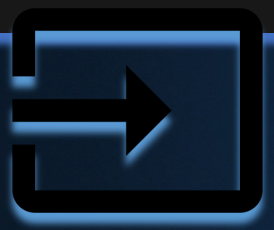




MAGNET RESPONSE: OUTPUT



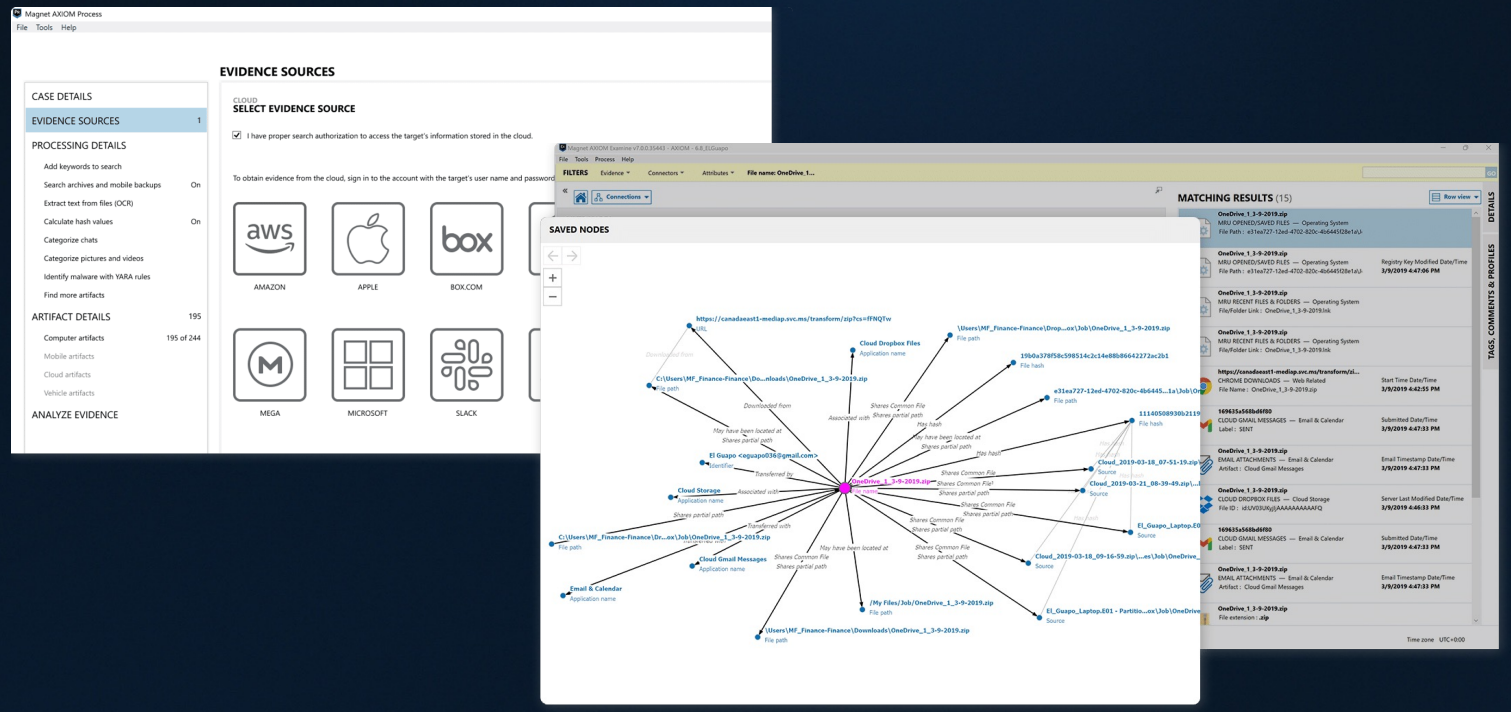




SEEK JUSTICE. PROTECT THE INNOCENT.

EVIDENCE PROCESSING TIPS

MAGNET AXIOM™ CYBER



AXIOM Cyber is a robust yet intuitive digital forensics solution that enables you to efficiently unravel and understand cyberthreats.

Remote Acquisition

Acquire From The Cloud

Examine From All Sources

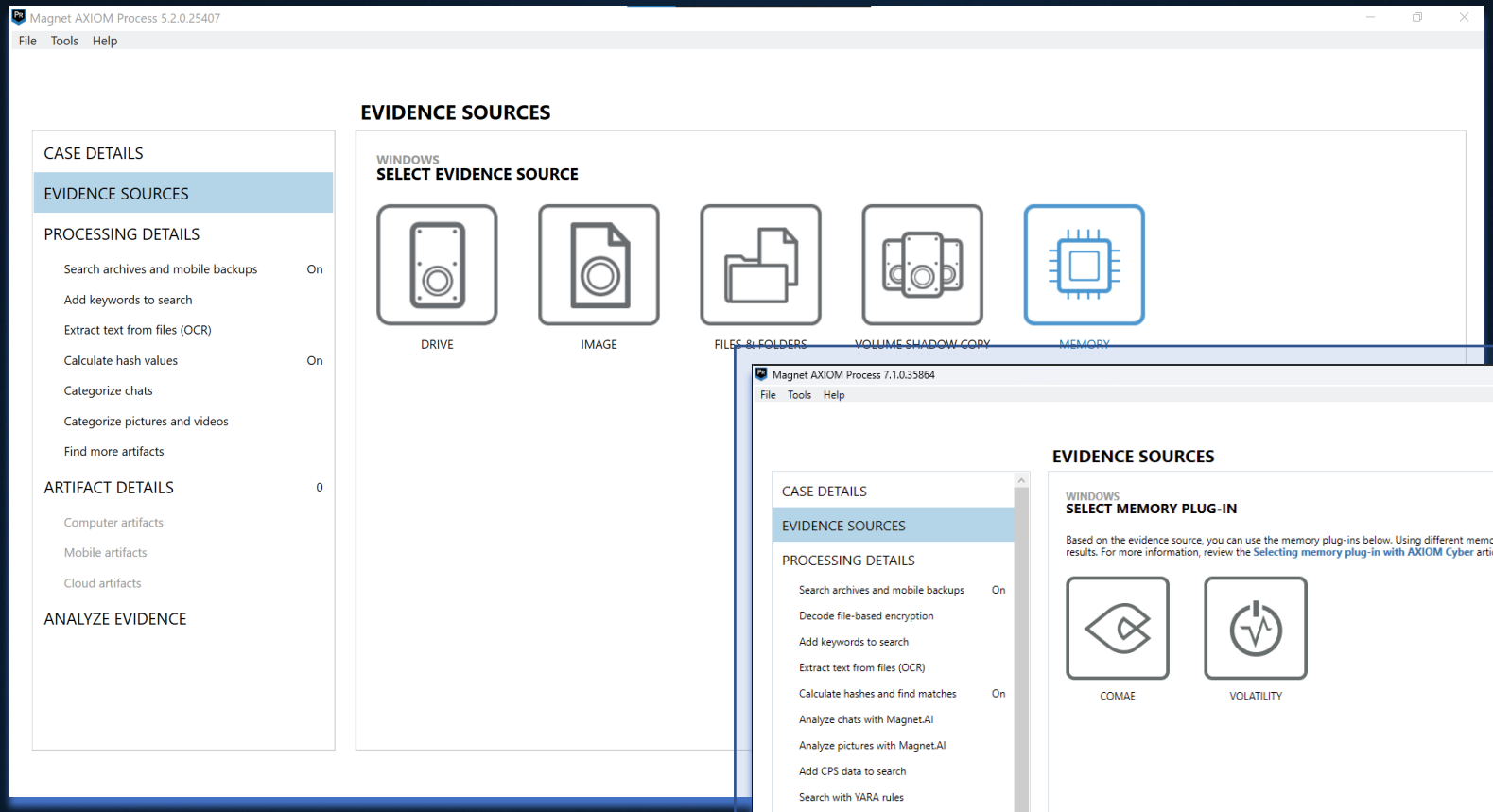
Easy Reporting

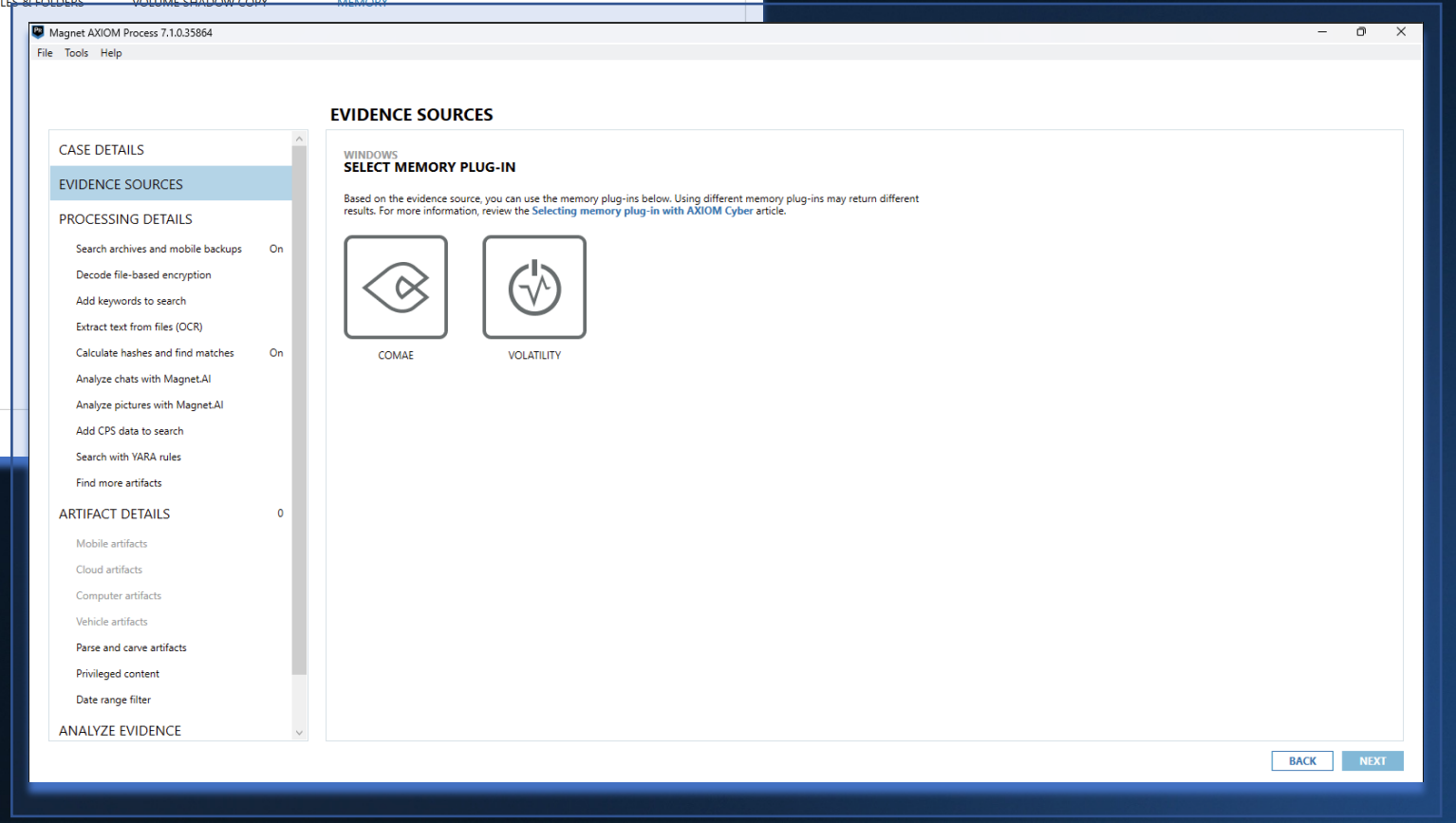
Quick Root Cause Analysis

magnetforensics.com

SEEK JUSTICE. PROTECT THE INNOCENT.

MEMORY PROCESSING

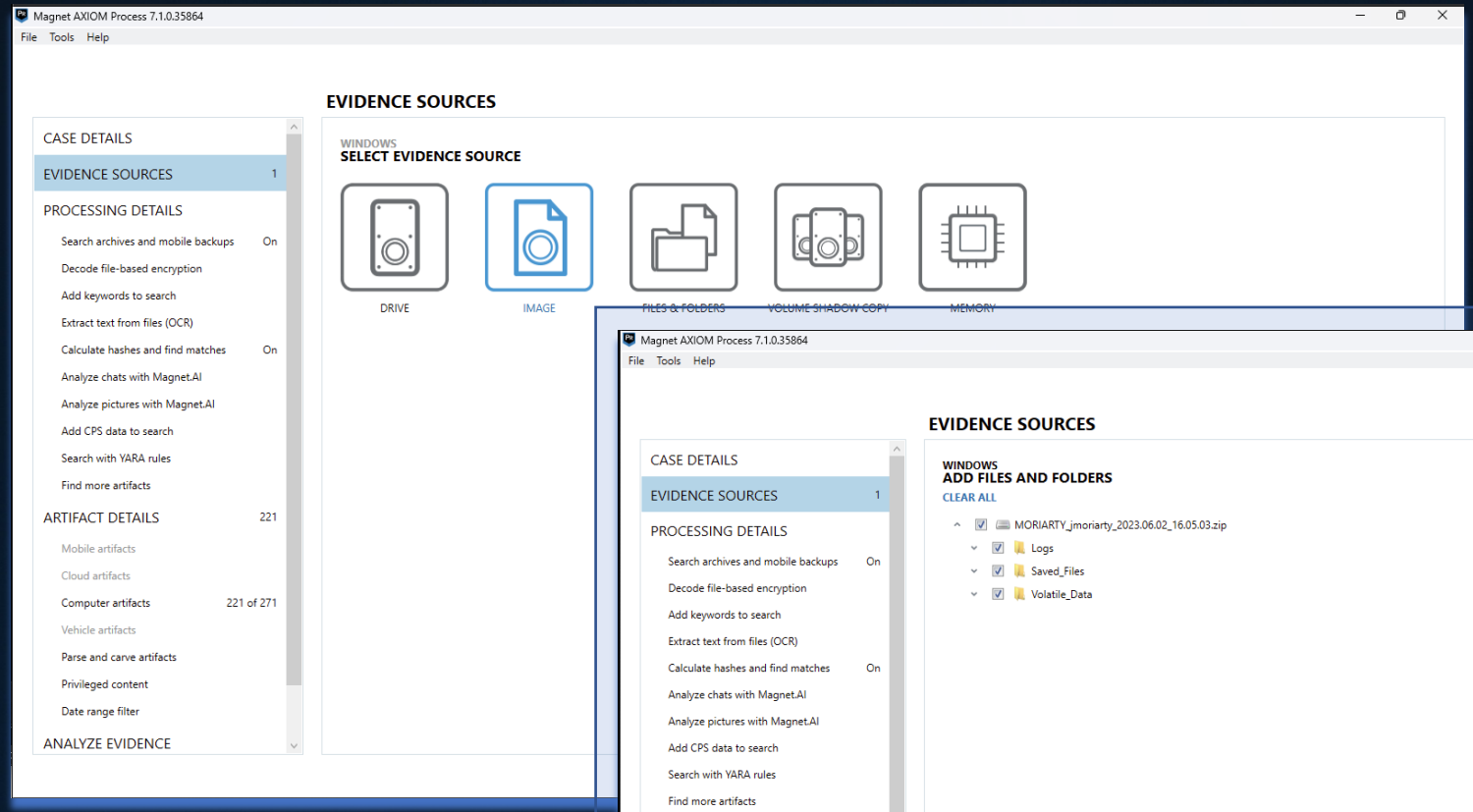


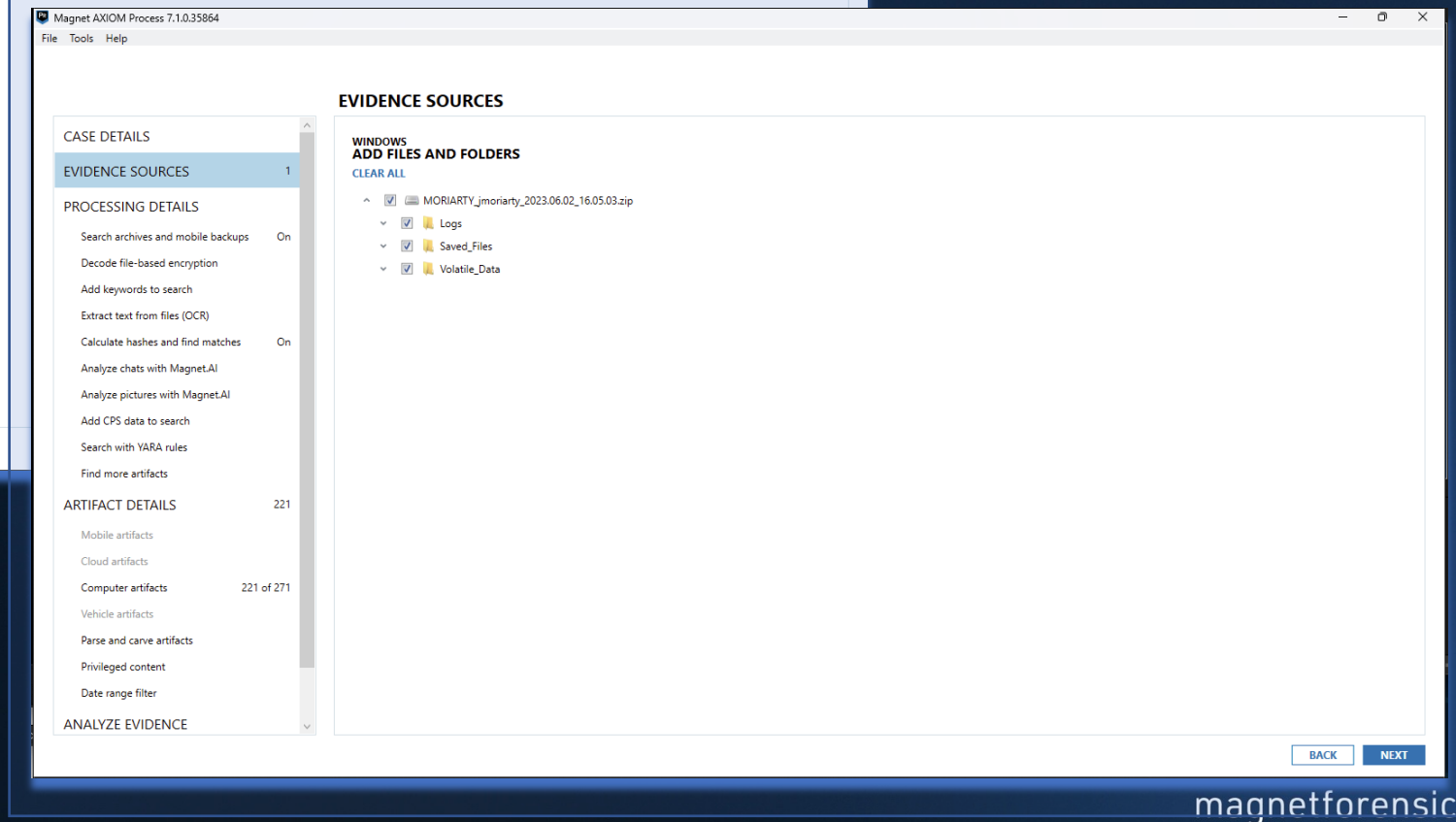


SEEK JUSTICE. PROTECT THE INNOCENT.

IMAGE PROCESSING

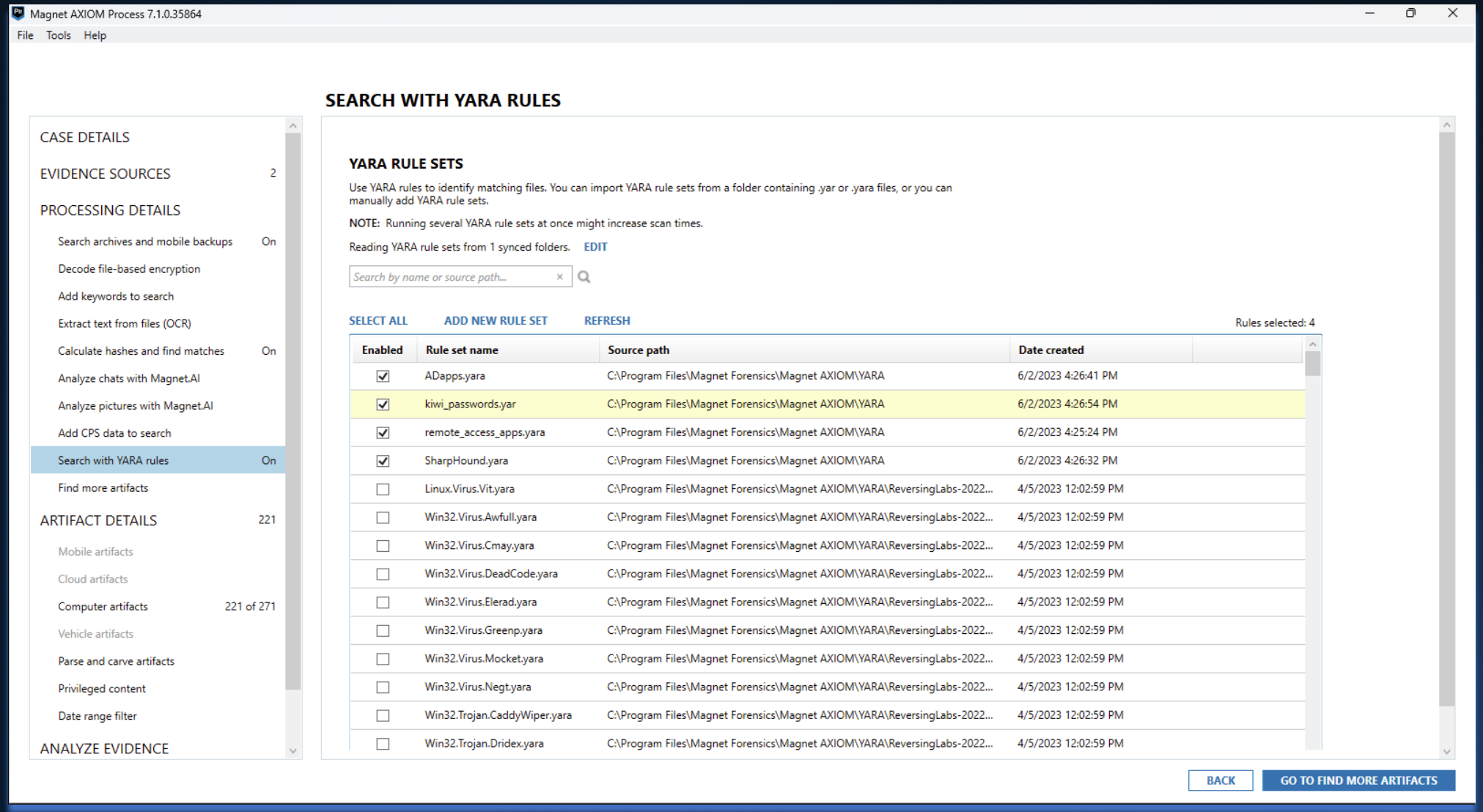
Computer > Windows > Load Evidence > IMAGE





SEEK JUSTICE. PROTECT THE INNOCENT.

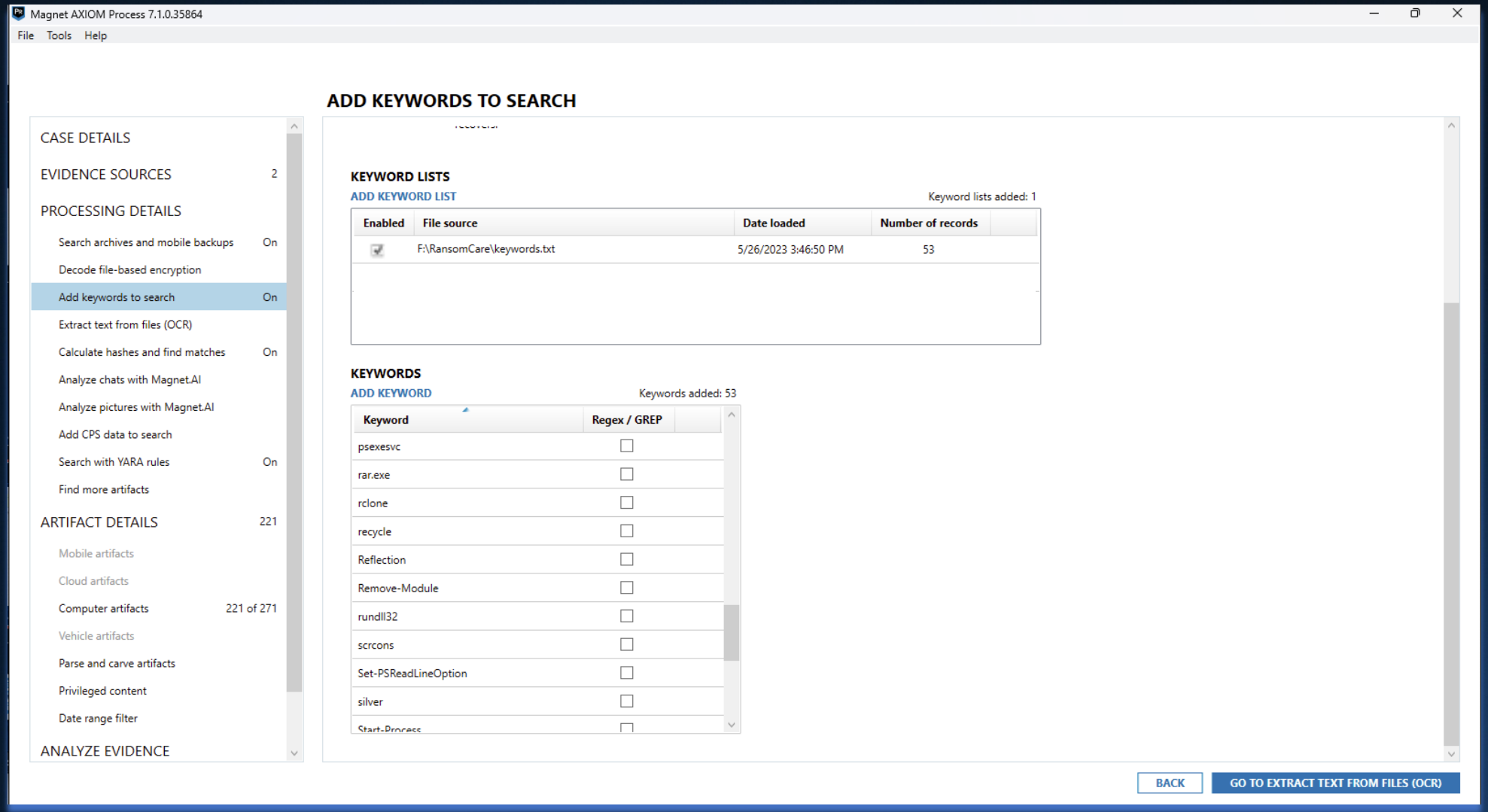
YARA



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

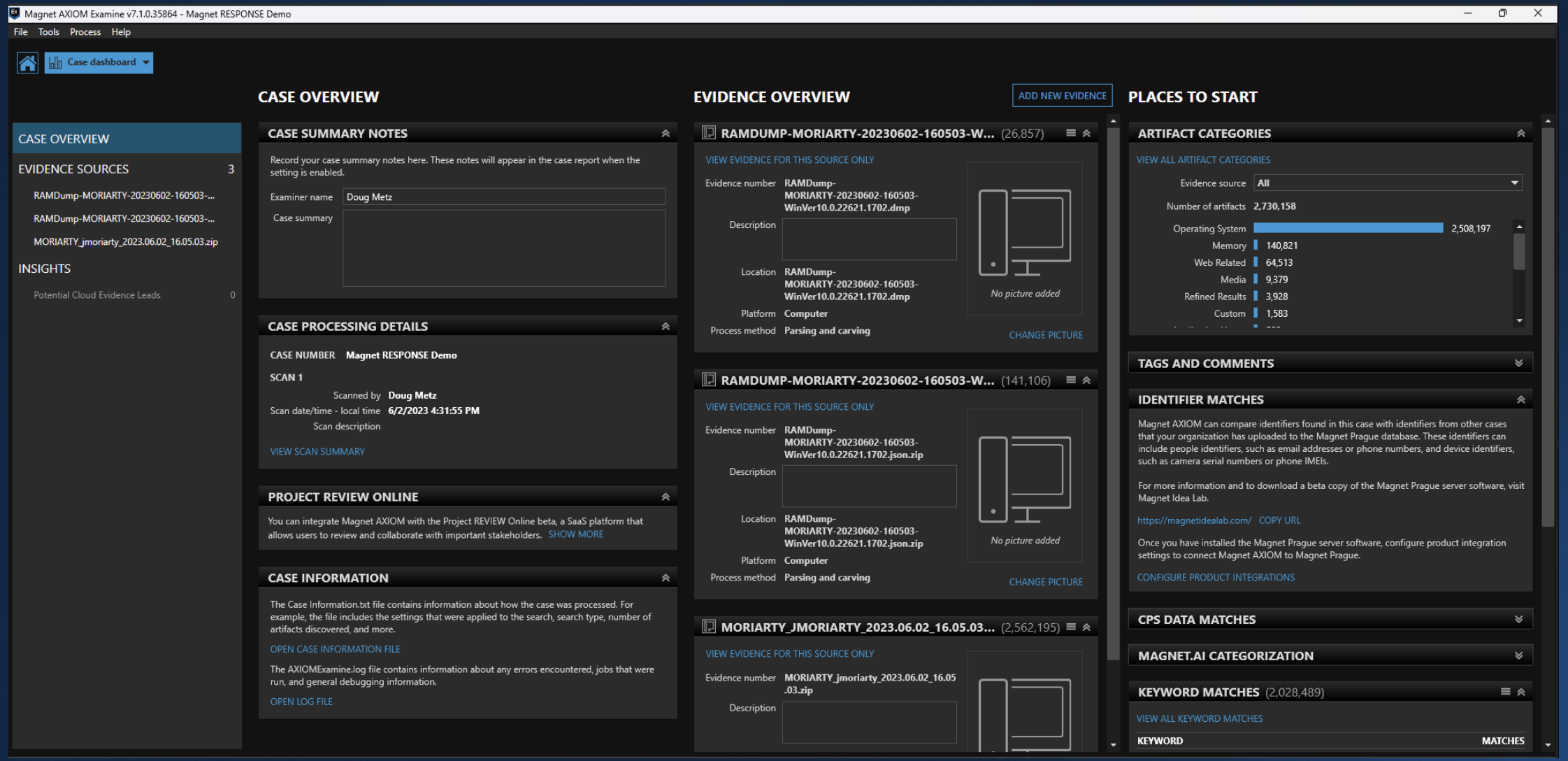
KEYWORDS



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

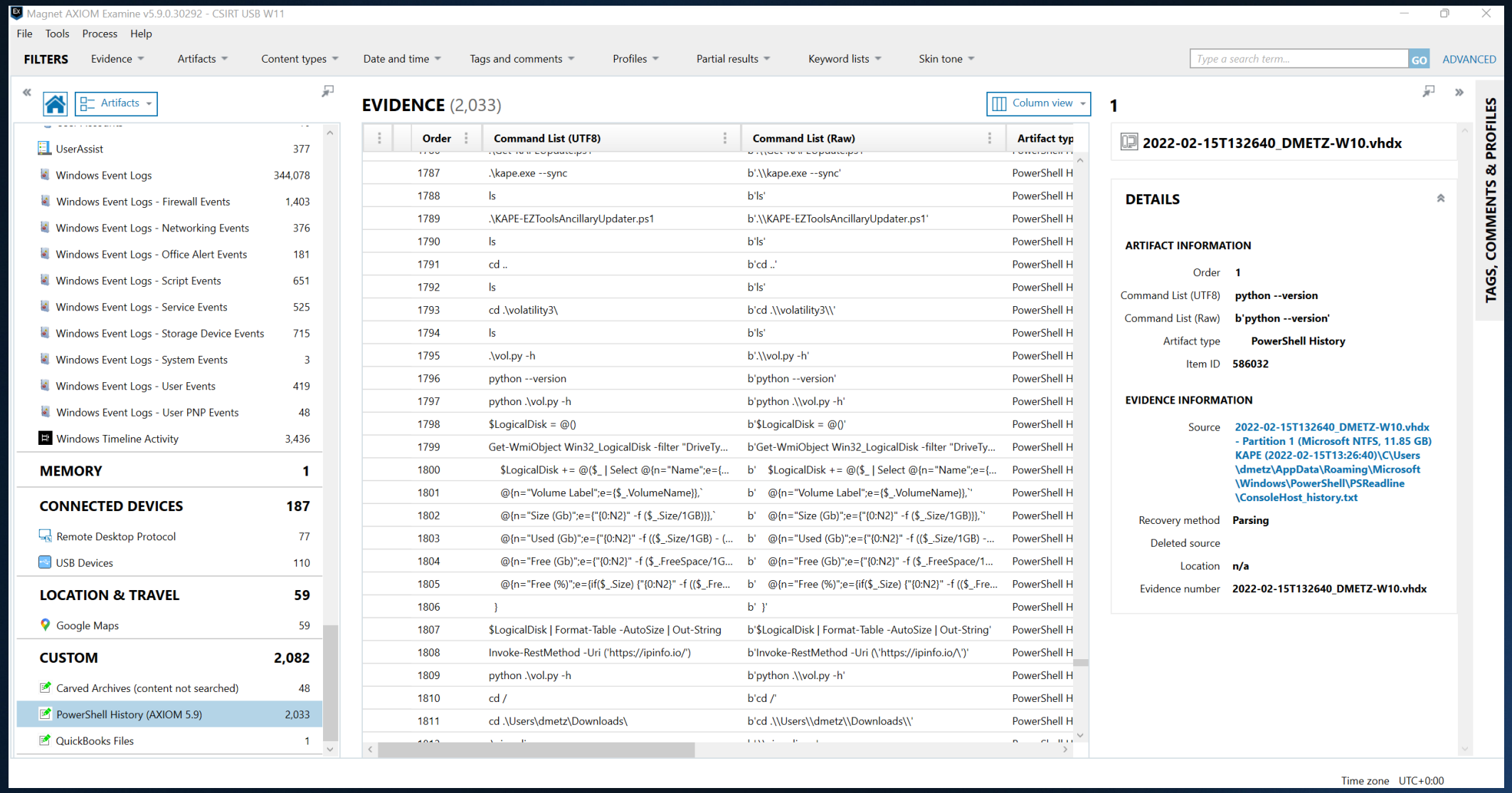
ARTIFACTS FROM RESPONSE TRIAGE



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

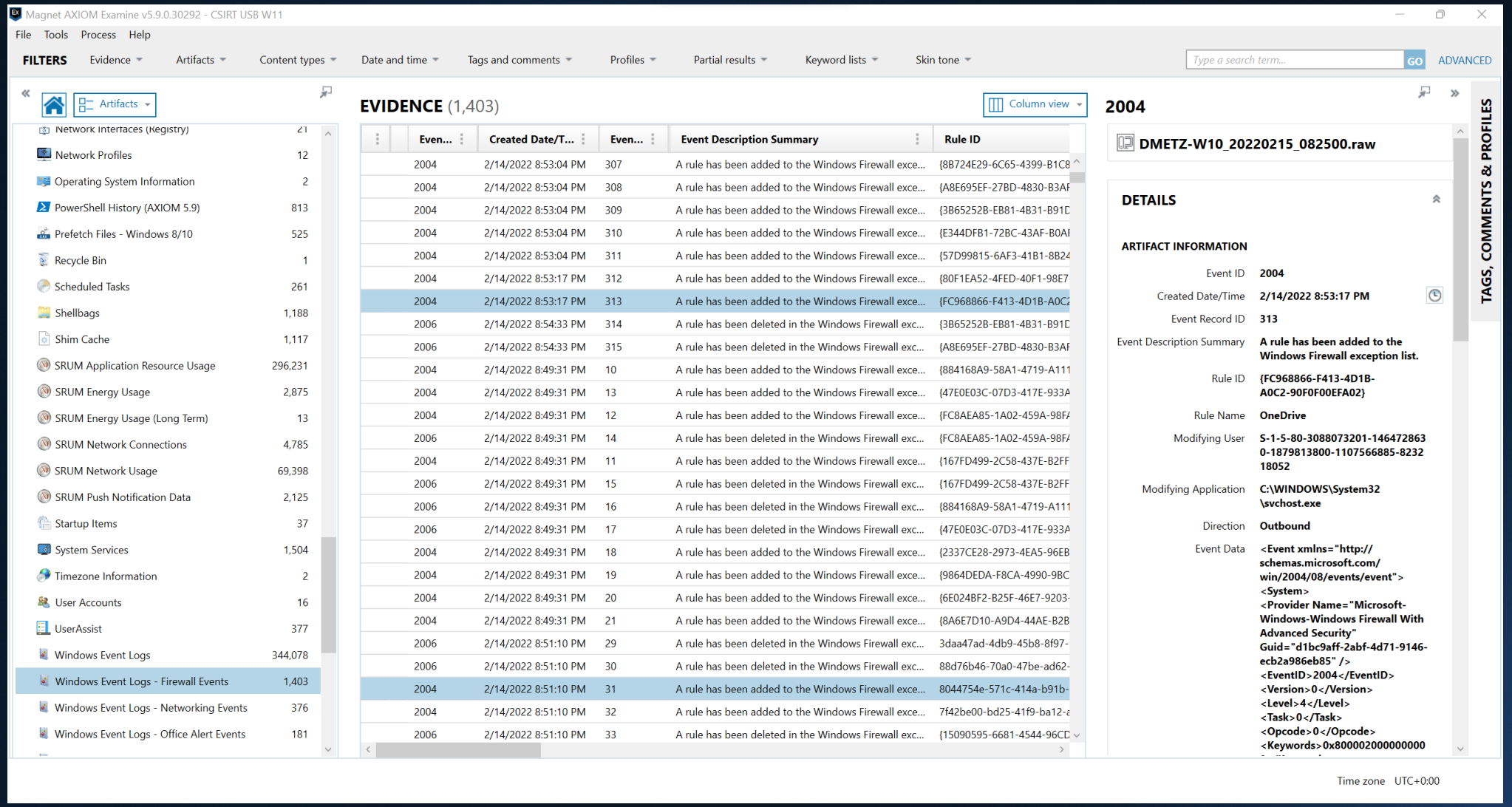
POWERSHELL HISTORY



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

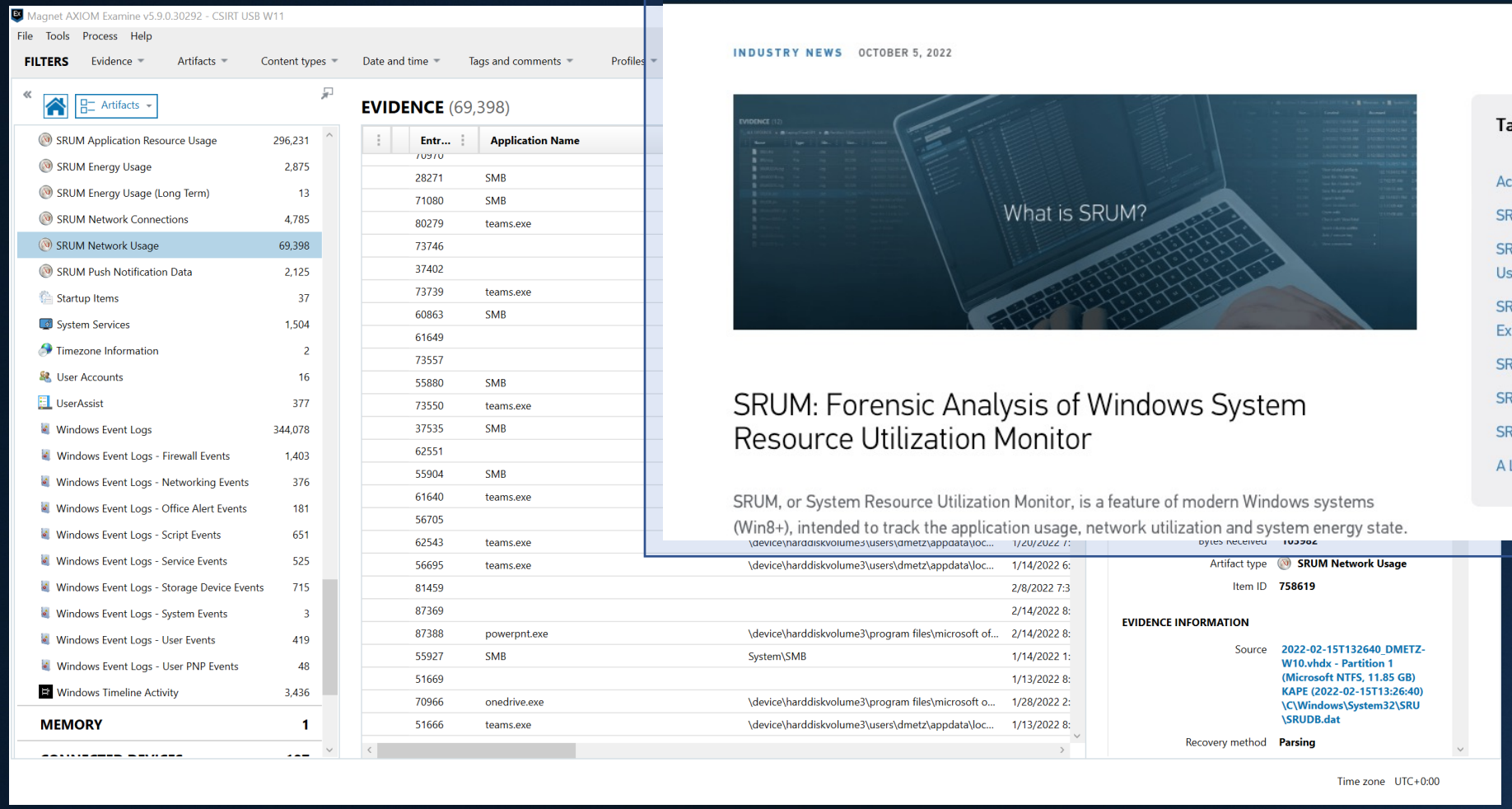
FIREWALL EVENTS



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

SYSTEM RESOURCE USAGE MONITOR (SRUM)

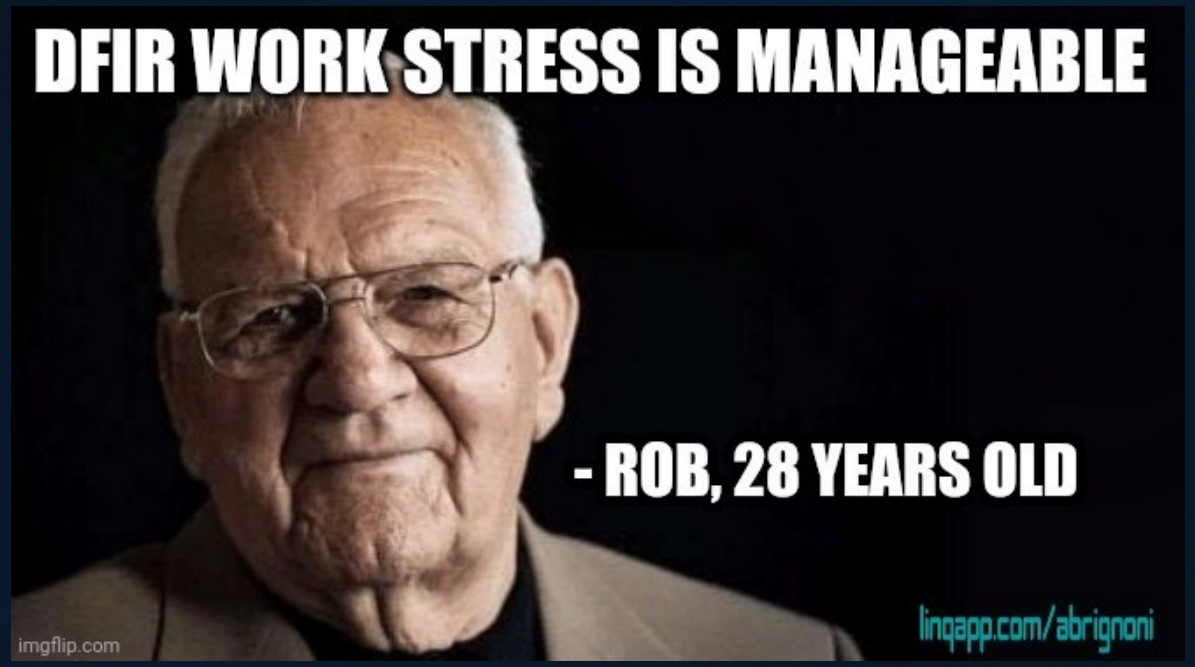


https://www.magnetforensics.com/blog/srum-forensic-analysis-of-windows-system-resource-utilization-monitor/

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

RESPONDING AT SCALE



SEEK JUSTICE. PROTECT THE INNOCENT.

RESPONDING AT SCALE WITH POWERSHELL

```
<#
.NAME Magnet RESPONSE PowerShell Enterprise
doug.metz@magnetforensics.com
ver 1.7

The script first checks if it is running with administrative permissions and exits if not.
The script will then download Magnet RESPONSE from a web server, extract it, and run with the specified options.

The $outputpath parameter can be used to write to a local directory `C:Temp`, `D:\Output` or network `\\Server\Share`.

Finally, the script removes the downloaded Magnet RESPONSE files and prints the time taken for the collection
and transfer to complete.

#>
param ([switch]$Elevated)
1 reference
function Test-Admin {
        $currentUser = New-Object Security.Principal.WindowsPrincipal $([Security.Principal.WindowsIdentity]::GetCurrent())
        $currentUser.IsInRole([Security.Principal.WindowsBuiltinRole]::Administrator)
}
if ((Test-Admin) -eq $false) {
        if ($elevated) {
        } else {
                Write-host ""
                Write-host  "Magnet RESPONSE requires Admin permissions.
Exiting.
"
}
exit
}
### VARIABLE SETUP
$caseID = "INC-8675309" # no spaces
$outputpath = "\\Server\Automate\WatchFolders\Magnet_Response" # Update to reflect output destination. C:\Temp R:\Output \\Server\Share
$server = "192.168.4.187" # "192.168.1.10" resolves to http://192.168.1.10/MagnetRESPONSE.zip
$tstamp = (Get-Date -Format "yyyyMMddHHmm")
#######
```

https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

CASE VARIABLES

```
### VARIABLE SETUP
$caseID = "demo-161" # no spaces
$outputpath = ”\\server\share" # Update to reflect output destination.
$server = "192.168.4.187" # "192.168.1.10" resolves to
http://192.168.1.10/MagnetRESPONSE.zip
```

$caseID – Name of your case or incident. (no spaces)

$outputpath – Where the collection output is sent

$server – Address for web server hosting MagnetRESPONSE.zip

https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

RESPONSE CLI 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:<keyword.csv>	- 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

COLLECTION PROFILES

```
#### Extended Process Capture
<#
$profileName = "EXTENDED PROCESS CAPTURE"
$arguments = "/capturevolatile /captureextendedprocessinfo /saveprocfiles"
#>
#### Systen Files

$profileName = "SYSTEM FILES"
$arguments = "/capturesystemfiles"
#>
#### Just RAM
<#
$profileName = "CAPTURE RAM"
$arguments = "/captureram"
#>
```

https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

RESPONSE CLI ASSEMBLED

```
MagnetRESPONSE\MagnetRESPONSE.exe /accepteula /unattended
/output:$outputpath/$caseID-$env:ComputerName-$tstamp /caseref:$caseID $arguments
```

/accepteula /unattended – general CLI requirements

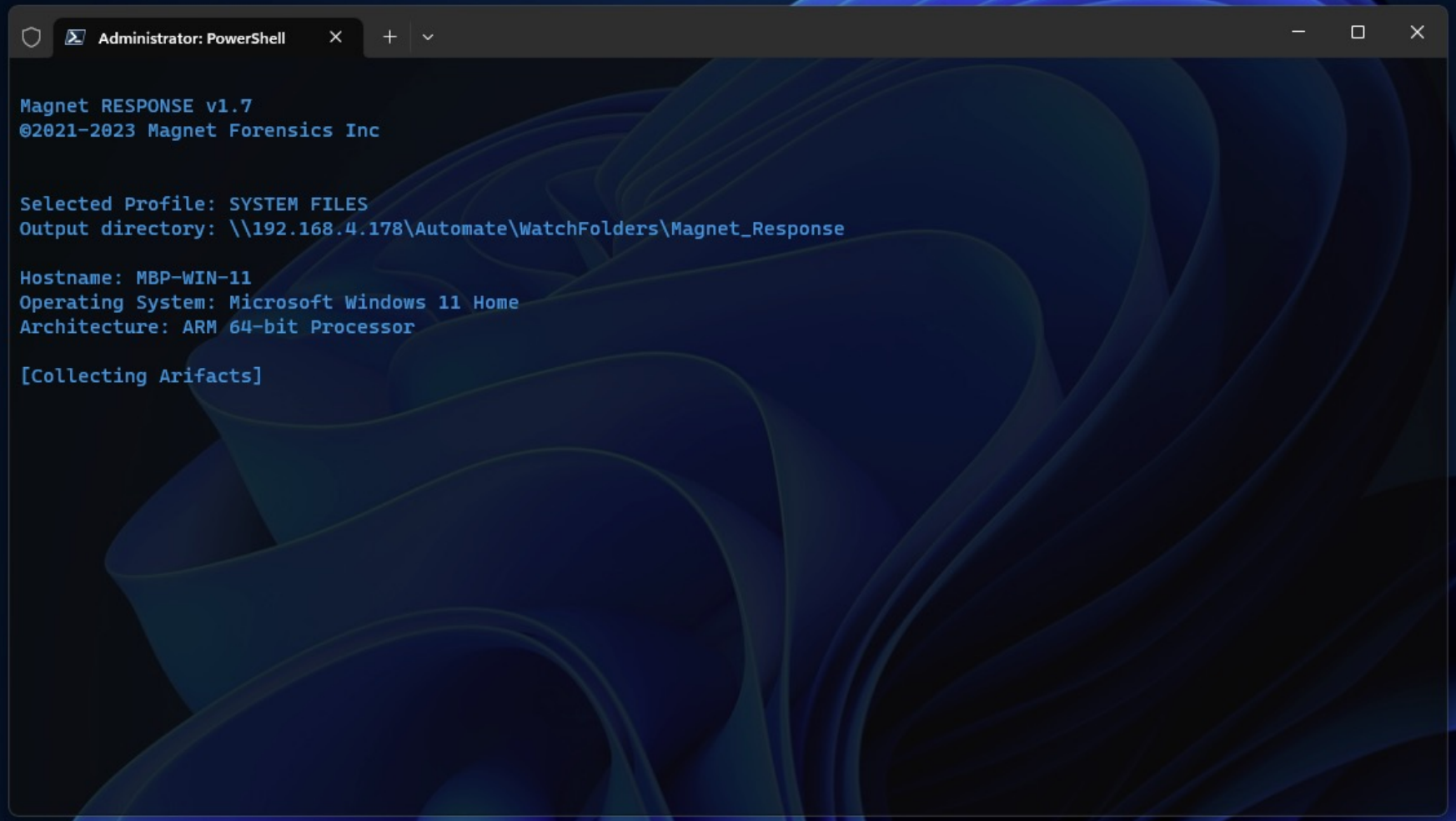
/output – server path\caseID-hostname-timestamp

/caseref:caseID – Case ID

$arguments – Specified in collection profile

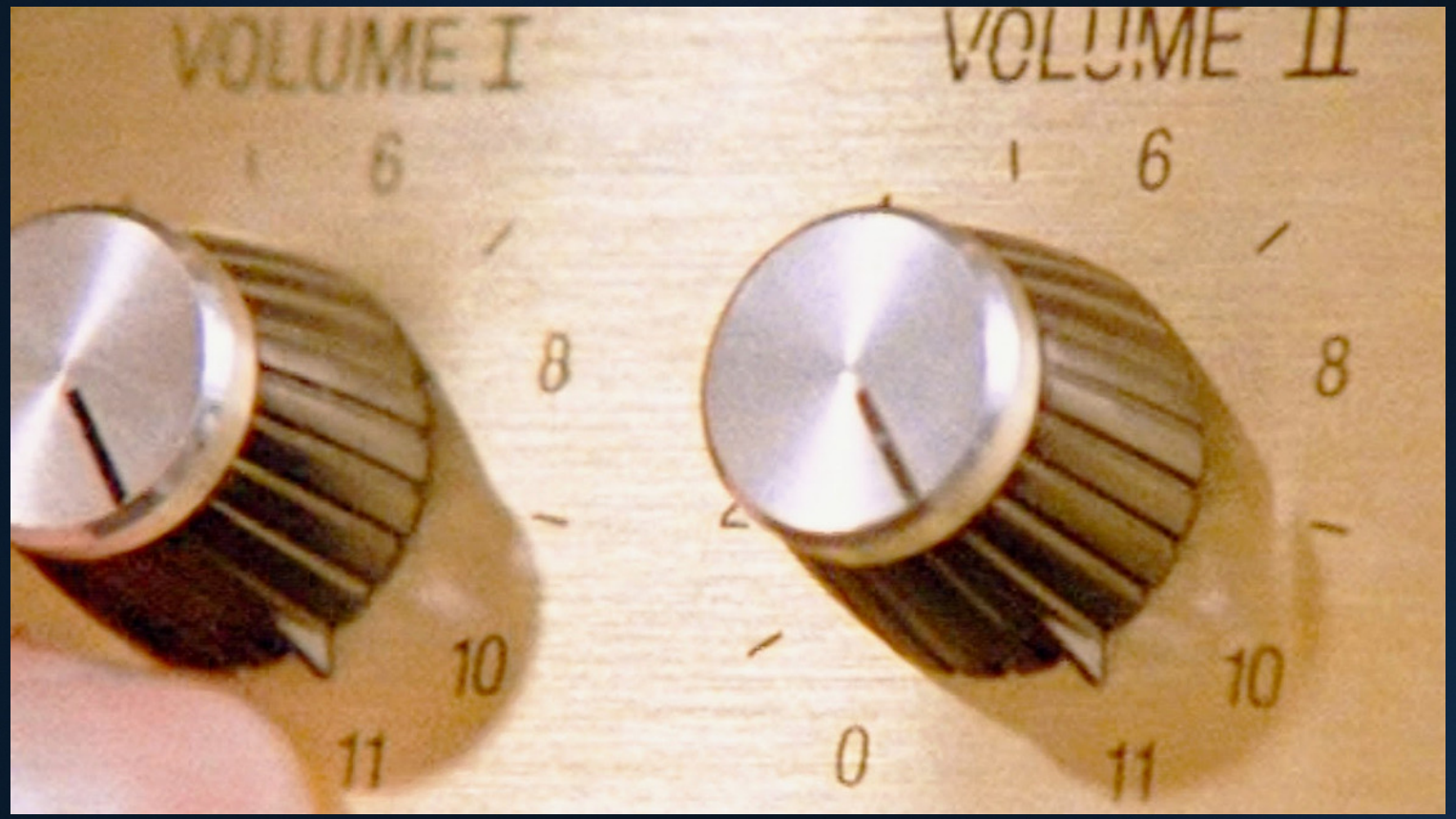
SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNET RESPONSE POWERSHELL

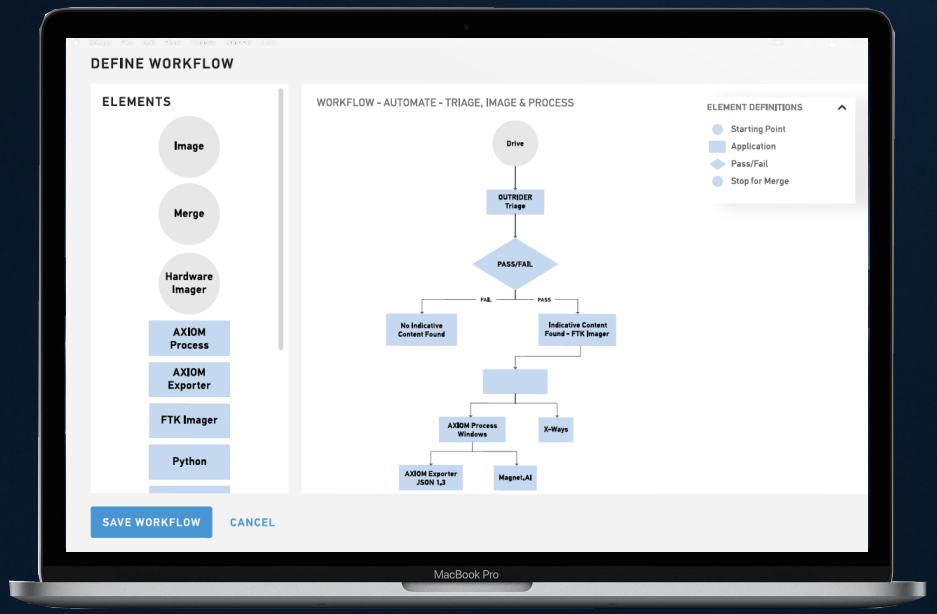


https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

TURN IT UP TO 11



MAGNET AUTOMATE



AUTOMATE increases efficiency and productivity by integrating forensic tools and tasks into automated workflows, empowering examiners to focus on what matters.

Automated Workflows

Unlimited Integrations

Faster Processing

Remote Collections

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

WATCH FOLDERS

Using a Watch Folder as the location for our collection script output means that any time a new Magnet RESPONSE collection is completed, AUTOMATE will pick up those files, create a new case, and process the acquired evidence using a repeatable and consistent methodology.

Watch folder file structure

To be able to watch a location for images, Magnet AUTOMATE needs information about how your data is structured. The first step is to provide the full path to an image. In step 2, you identify the components of the path. Here's an example of a location with each of the components identified.

D:\Storage\CASE-001\images\ICAC-Android\EVD-001

Example	Component	Description
Storage	Root	The root folder to be monitored for images. Magnet AUTOMATE looks for an exact match for this folder name and watches its subfolders for images that are added.
CASE-001	Case number variable	A variable that contains the case number. Magnet AUTOMATE uses the folder defined at this level to populate the case number on the dashboard.
EVD-001	Evidence number variable	A variable that contains the evidence number. Magnet AUTOMATE uses the folder (or file name) defined at this level to populate the evidence number on the dashboard.

Any additional folders that aren't mapped to the case and evidence number variables are treated as static folders in the path (in this example, the static folders are \images\ICAC-Android). Watch folders can have any number of static folders, but for this workflow to run, the names and structure must exactly match what you provide in this configuration.

Watch folder location

Enter the full path to the folder you want AUTOMATE to automatically monitor

\\hydepark\Automate\WatchFolders\Magnet_RESPONSE\inc-8675324-mbp-win-11-202306071504

☐ Local image mode

To avoid processing images over the network, you can turn on local image mode to copy images to the node before processing occurs.

Step 2: Map folders to the appropriate watch folder component

Identify which folders or file in the watch folder file structure represent each of the required components. You can map a folder to only one component. To change your selection, click the RESET link that appears beside a completed dropdown:

Root

Magnet_RESPONSE RESET

Case number variable

inc-8675324-mbp-win-11-202306071504 RESET

Evidence number variable

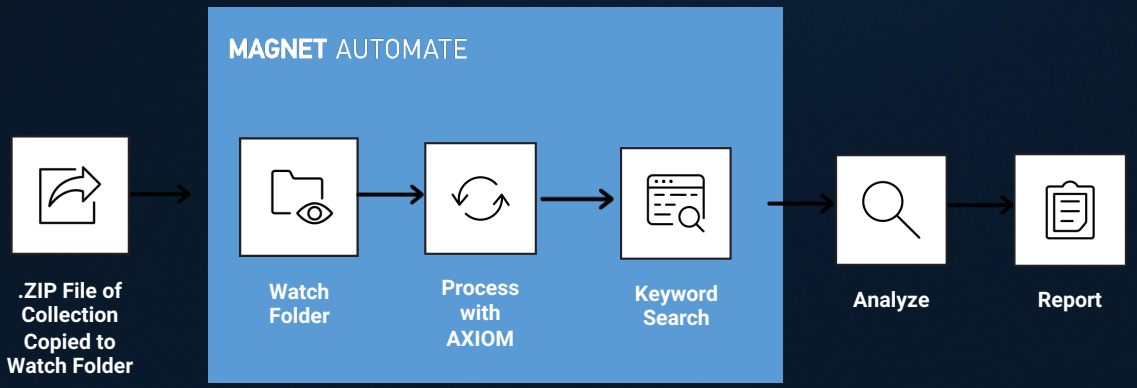
File name of forensic image RESET

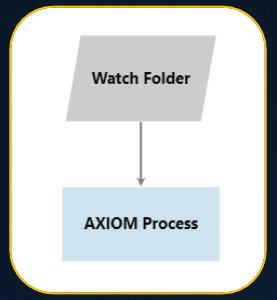
CONTINUE

SEEK JUSTICE. PROTECT THE INNOCENT.

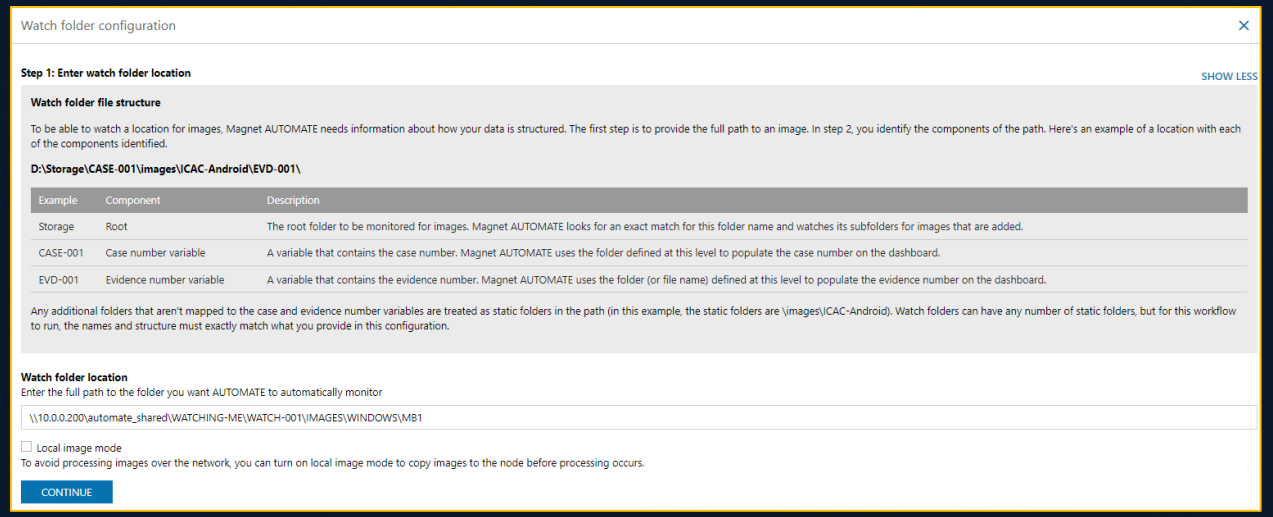
AUTOMATIC FORENSIC PROCESSING

With a Watch Folder





Workflow Builder Example

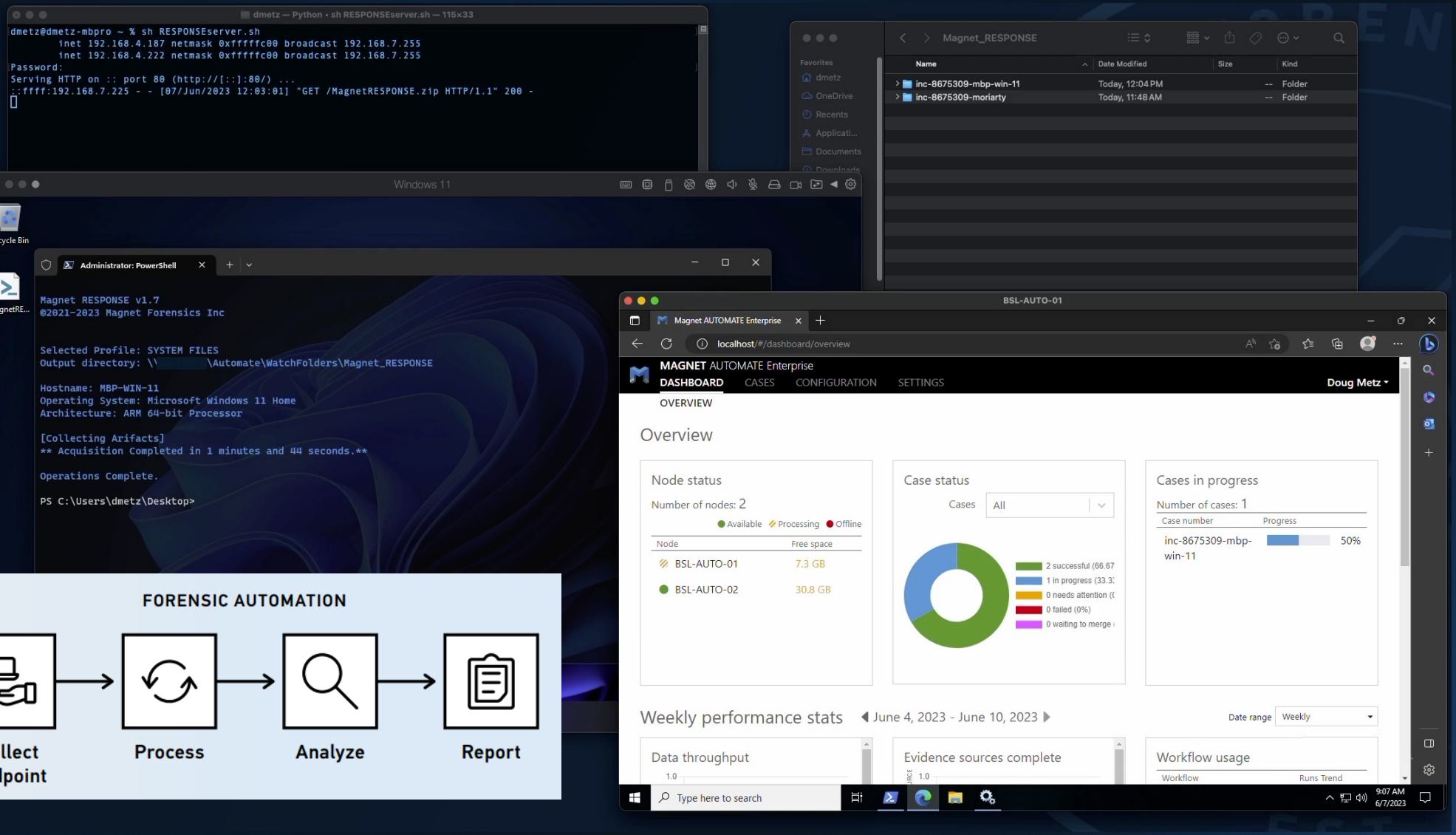


DFIR teams using AUTOMATE save time by reducing manual touchpoints and integrating their tech stack into automated workflows.

Workflows can integrate Magnet products like Axiom, as well as any 3rd party tools that have CLI options.

SEEK JUSTICE. PROTECT THE INNOCENT.

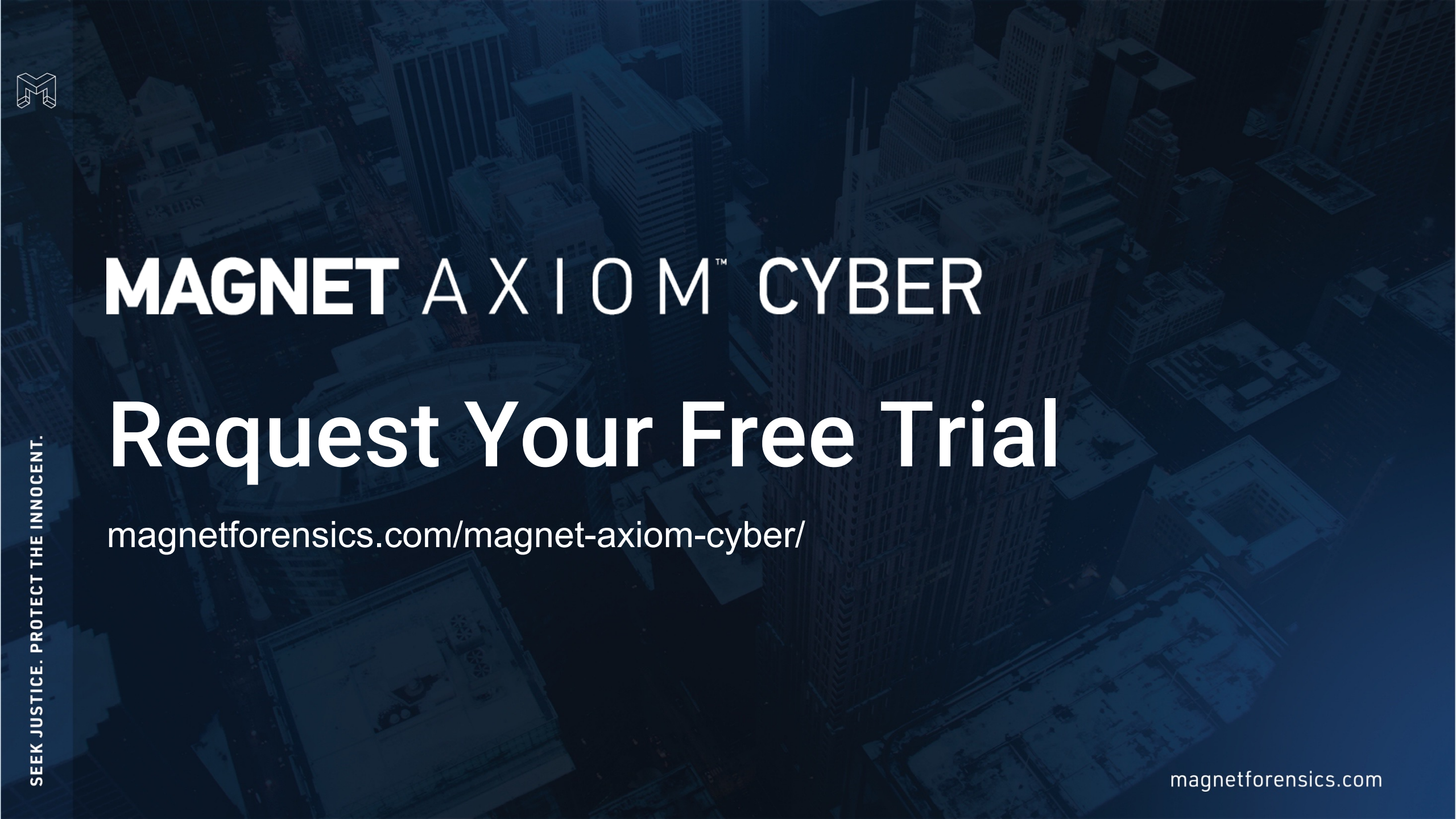
TRIAGE AUTOMATION



Triage collection to processed case in <|= 1 click

magnetforensics.com

SEEK JUSTICE. PROTECT THE INNOCENT.


MAGNET AXIOM™ CYBER
Request Your Free Trial
magnetforensics.com/magnet-axiom-cyber/
SEEK JUSTICE. PROTECT THE INNOCENT.
magnetforensics.com

THANK YOU

https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

https://github.com/dwmetz

https://bakerstreetforensics.com

doug.metz@magnetforensics.com

https://www.linkedin.com/in/dwmetz/

https://infosec.exchange/@dwmetz

~~@dwmetz~~

SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNET FORENSICS®

magnetforensics.com