



# 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



BAKER STREET FORENSICS

D . F . I . R .

WHERE IRREGULARS ARE PART OF  
THE GAME



HTCIA





# 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

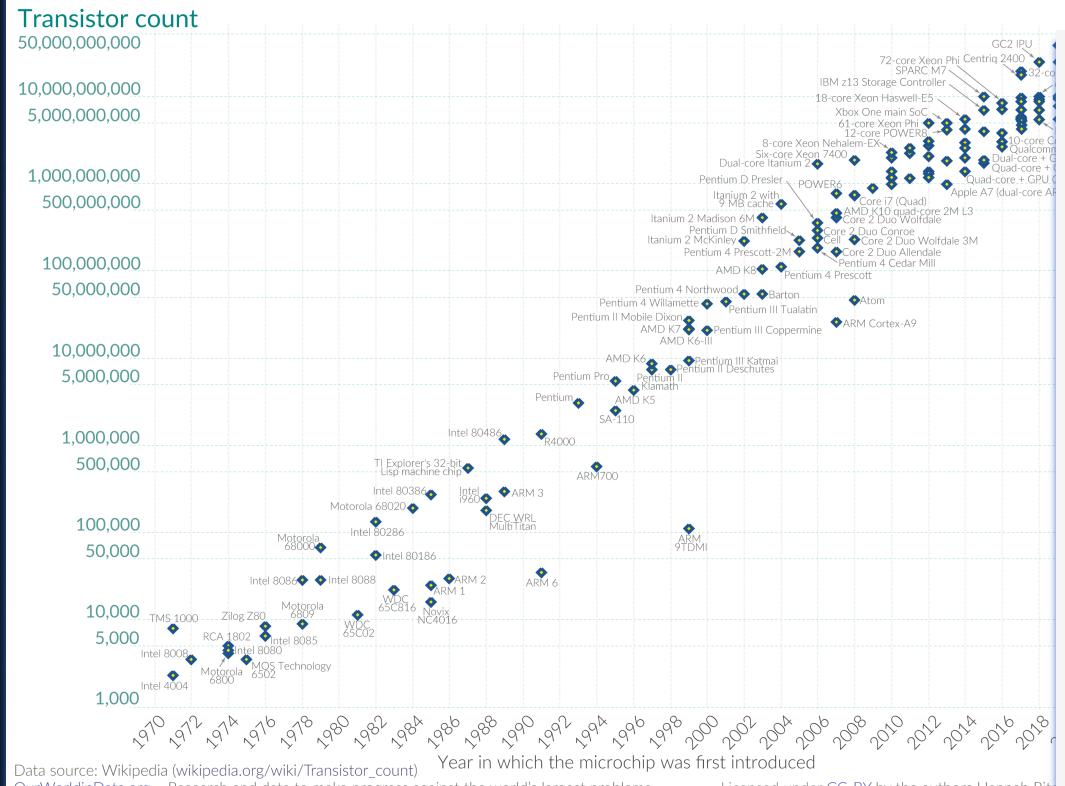


# MAGNITUDES OF DATA

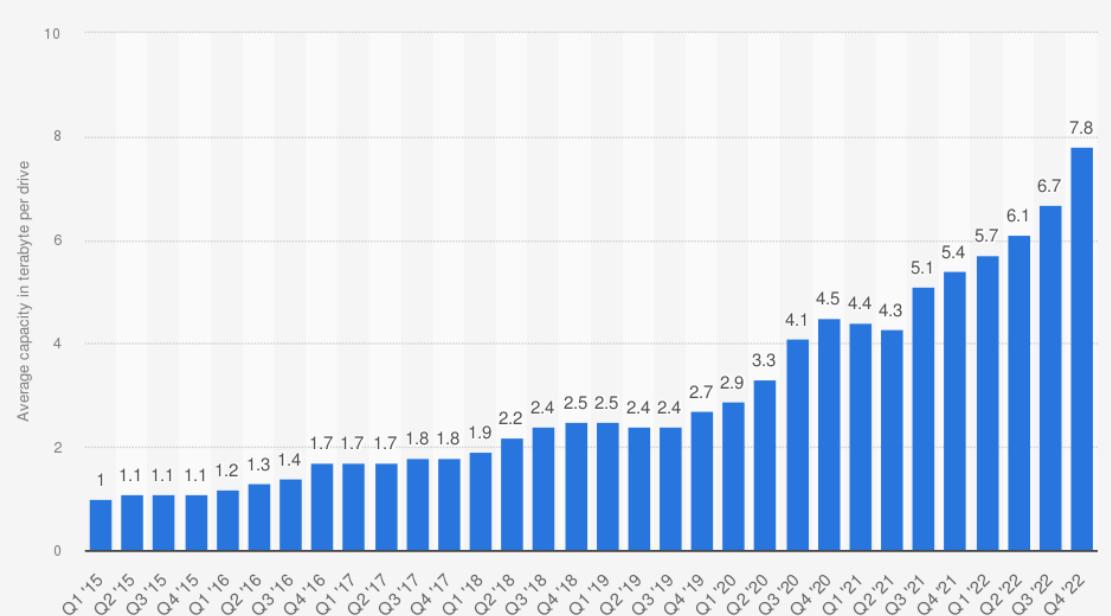
**Moore's Law:** The number of transistors on microchips doubles every two years

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.

Our World  
in Data



**Seagate's average capacity of hard disk drives (HDDs) worldwide from FY2015 to FY2022, by quarter (in terabyte per drive)**



Source  
Seagate  
© Statista 2022

Additional Information:  
Worldwide; Seagate; 2015 to 2022

## Sources:

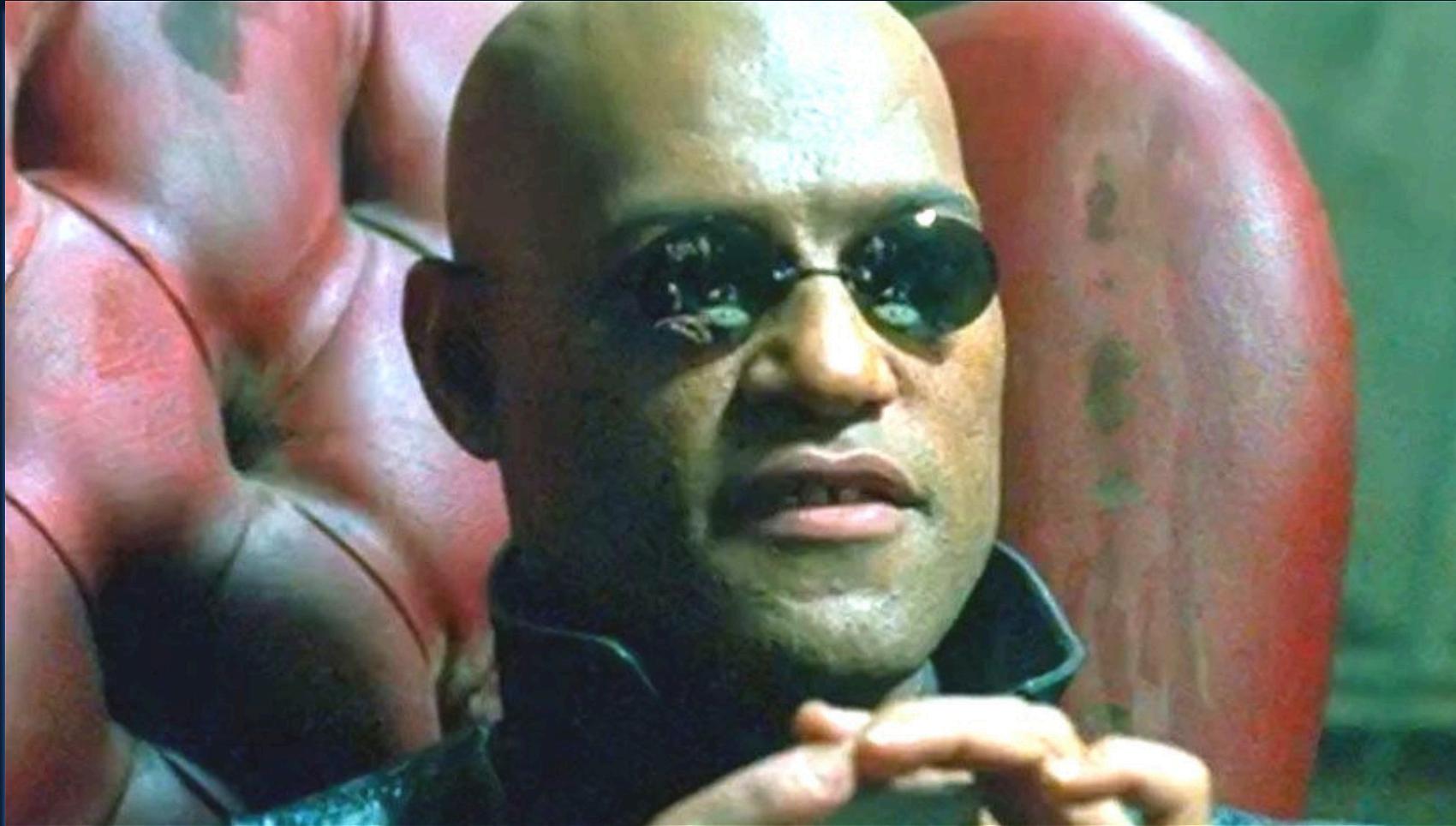
[https://en.wikipedia.org/wiki/Moore%27s\\_law#/](https://en.wikipedia.org/wiki/Moore%27s_law#/)

<https://www.statista.com/statistics/795748/worldwide-seagate-average-hard-disk-drive-capacity/>



# What If I Told You

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





# triage noun

tri·age trē-'äzh 'trē-äzh

- 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*)



SEEK JUSTICE. PROTECT THE INNOCENT.

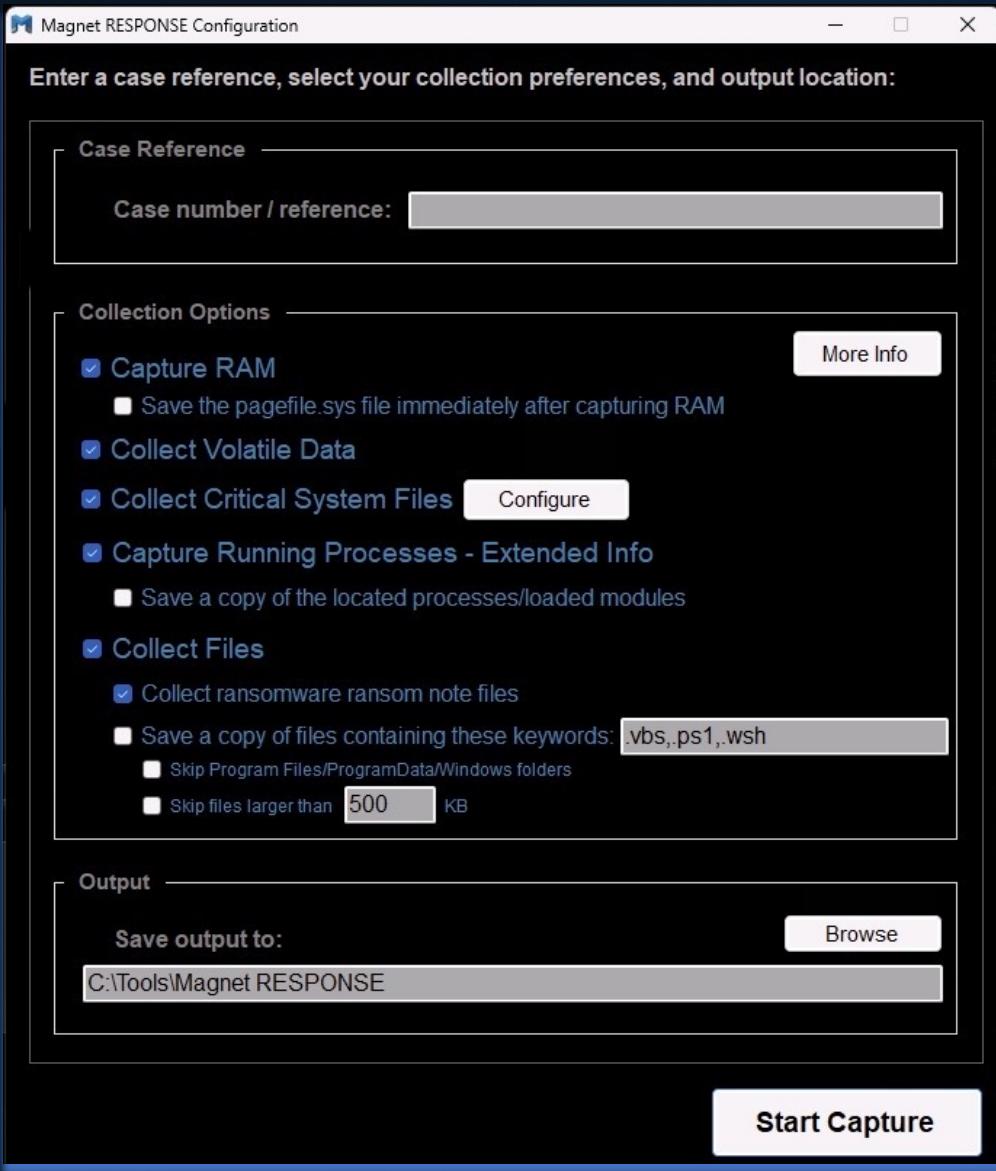
<https://www.magnetforensics.com/free-tools/>

The screenshot shows the Magnet Forensics website's 'Free Tools' page. At the top, there's a navigation bar with links for Training, Support, PRODUCTS, SOLUTIONS, RESOURCES, OUR COMMUNITY, PARTNERS, COMPANY, and a search icon. Below the navigation is a dark banner with a blurred background image of a computer screen displaying code. On the right side of the banner, the text 'Free Tools' is prominently displayed. To the left, there's a paragraph of text: 'We're proud to offer a number of free tools to help give the DFIR community new ways to find evidence in their investigations. Help yourself to what's available and try it in your next examination.' At the bottom of the page, there's another section titled 'Stock Up Your DFIR Toolkit' with a paragraph of text: 'With Magnet Free Tools, we're giving you a chance to supplement your existing solutions with specialized tools that will help you acquire new evidence, obtain fleeting evidence from consenting witnesses, or simulate data from devices.'

[magnetforensics.com](https://magnetforensics.com)



# 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 Dumpl) 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 comprised 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

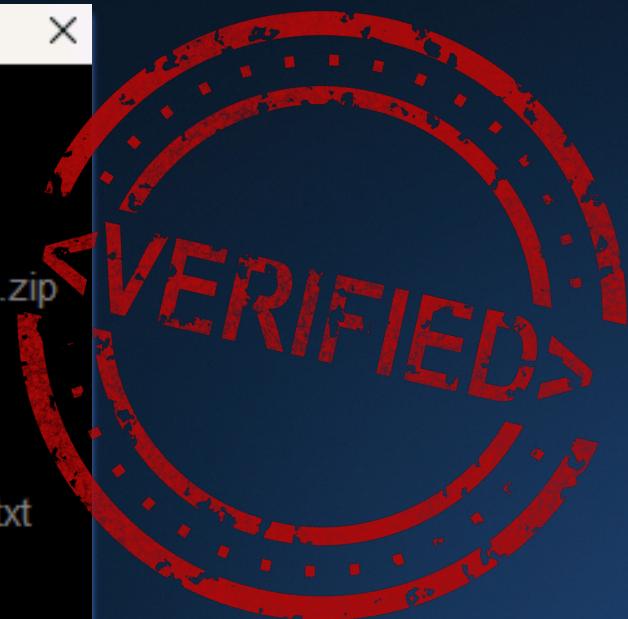
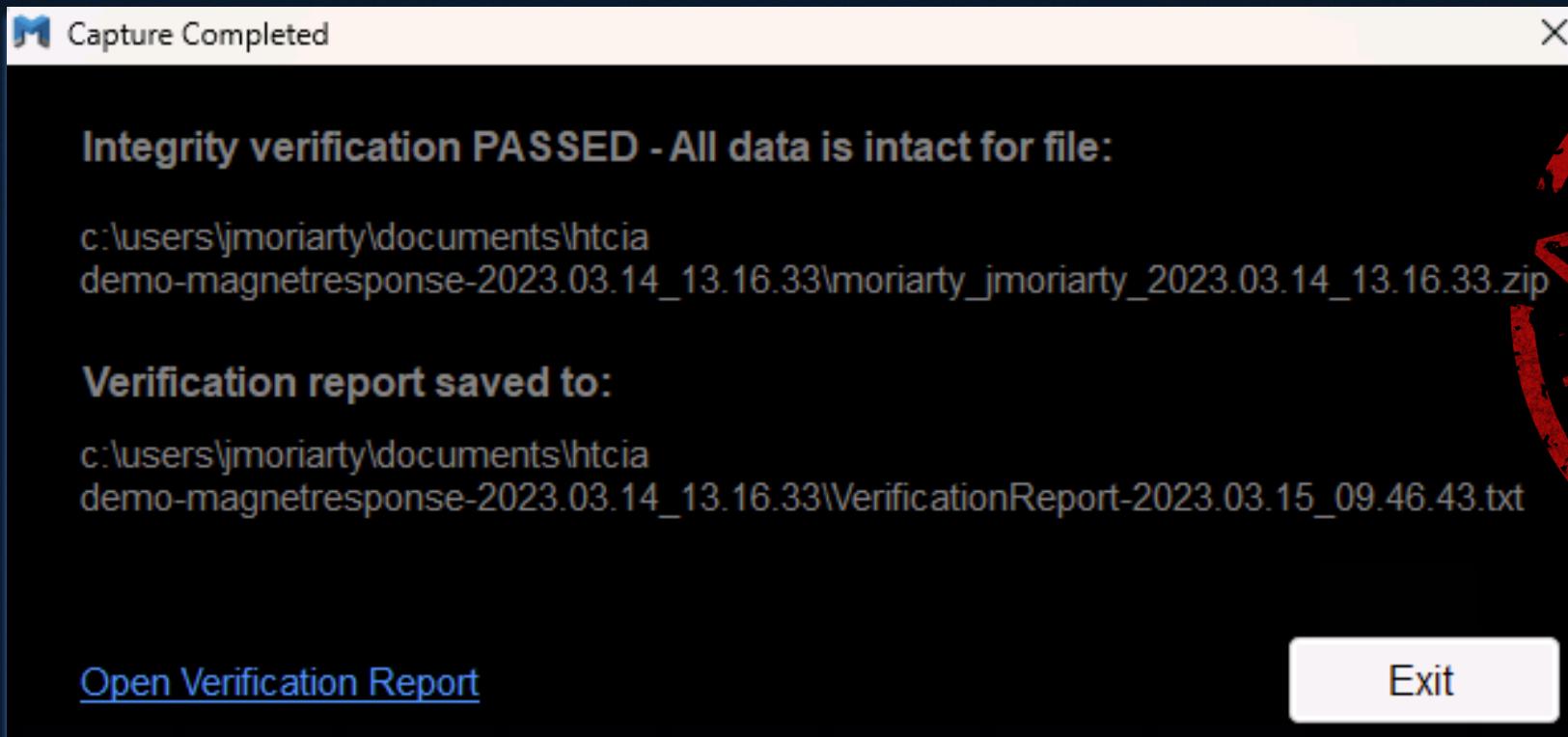




# MAGNET RESPONSE

## 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



HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33			
Name	Date modified	Type	Size
7z MORIARTY_jmoriarty_2023.03.14_13.16.33...	3/14/2023 1:21 PM	ZIP File	909,893 KB
DMP RAMDump-MORIARTY-20230314-131633...	3/14/2023 1:17 PM	DMP File	16,382,988 ...

HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 > extracted >			
Name	Date modified	Type	
Logs	3/14/2023 1:37 PM	File folder	
Processes	3/14/2023 1:37 PM	File folder	
Saved_Files	3/14/2023 1:37 PM	File folder	
Volatile_Data	3/14/2023 1:37 PM	File folder	



# MAGNET RESPONSE: OUTPUT

SEEK JUSTICE. PROTECT THE INNOCENT.

HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 > extracted > Saved_Files				
Name	Date modified	Volatile Data		
Type	Size	Date modified	Type	Size
Amcache	3/14/2023 1:37 PM	Firewall_Info.txt	Text Document	5 KB
Browser_History	3/14/2023 1:37 PM	IP_Info.txt	Text Document	7 KB
Jumplists-AutomaticDestinations	3/14/2023 1:37 PM	Logged_On_Users.txt	Text Document	1 KB
Jumplists-CustomDestinations	3/14/2023 1:37 PM	Network_Connections.txt	Text Document	21 KB
MFT	3/14/2023 1:37 PM	Scheduled_Tasks.txt	Text Document	42 KB
NTUSER.DAT	3/14/2023 1:37 PM	User_Accounts.txt	Text Document	5 KB
PowerShell_History	3/14/2023 1:37 PM	Wifi_Info.txt	Text Document	26 KB
Prefetch_Files	3/14/2023 1:37 PM	Windows_Services.txt	Text Document	53 KB
Recent_Files	3/14/2023 1:37 PM	Windows_Version.txt	Text Document	1 KB
Recycle_Bin	3/14/2023 1:37 PM			
Registry_Hives	3/14/2023 1:37 PM			
Scheduled_Tasks	3/14/2023 1:37 PM			
SRIIM	3/14/2023 1:37 PM			



magnetforensics.com

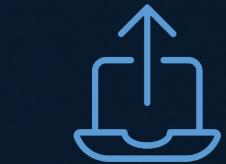
# EVIDENCE PROCESSING TIPS





# MAGNET AXIOM™ CYBER

The screenshot displays the Magnet AXIOM Cyber software interface. On the left, the 'EVIDENCE SOURCES' panel lists various cloud and local storage providers. The 'PROCESSING DETAILS' section shows keyword search, file extraction, and YARA rule identification. The 'ARTIFACT DETAILS' section indicates 195 artifacts found across 195 of 244 cases. The 'ANALYZE EVIDENCE' section is partially visible. The central part of the interface features a 'SELECT EVIDENCE SOURCE' dialog for 'CLOUD'. Below it is a 'SAVED NODES' graph visualization showing connections between various data sources like AWS, Box, Microsoft, and Slack, along with local storage paths and application names. To the right, a 'MATCHING RESULTS' window lists 15 findings, each with a detailed description, file path, and timestamp.



Remote  
Acquisition



Acquire From  
The Cloud



Examine From  
All Sources



Easy  
Reporting



Quick  
Root Cause  
Analysis

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



# MEMORY PROCESSING

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet AXIOM Process 5.2.0.25407

File Tools Help

EVIDENCE SOURCES

CASE DETAILS

EVIDENCE SOURCES

PROCESSING DETAILS

- Search archives and mobile backups On
- Add keywords to search
- Extract text from files (OCR)
- Calculate hash values On
- Categorize chats
- Categorize pictures and videos
- Find more artifacts

ARTIFACT DETAILS 0

- Computer artifacts
- Mobile artifacts
- Cloud artifacts

ANALYZE EVIDENCE

WINDOWS SELECT EVIDENCE SOURCE

DRIVE IMAGE FILES & FOLDERS VOLUME SHADOW COPY MEMORY

Magnet AXIOM Process 7.1.0.35864

File Tools Help

EVIDENCE SOURCES

CASE DETAILS

EVIDENCE SOURCES

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption
- Add keywords to search
- Extract text from files (OCR)
- Calculate hashes and find matches On
- Analyze chats with MagnetAI
- Analyze pictures with MagnetAI
- Add CPS data to search
- Search with YARA rules
- Find more artifacts

ARTIFACT DETAILS 0

- Mobile artifacts
- Cloud artifacts
- Computer artifacts
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

WINDOWS SELECT MEMORY PLUG-IN

Based on the evidence source, you can use the memory plug-ins below. Using different memory plug-ins may return different results. For more information, review the [Selecting memory plug-in with AXIOM Cyber](#) article.

COMAE VOLATILITY

BACK NEXT



# IMAGE PROCESSING

Computer > Windows > Load Evidence > IMAGE

The screenshot displays two windows of the Magnet AXIOM Process 7.1.0.35864 application. The top window shows the 'SELECT EVIDENCE SOURCE' dialog with options for DRIVE, IMAGE, FILES & FOLDERS, VOLUME SHADOW COPY, and MEMORY. The bottom window shows the 'ADD FILES AND FOLDERS' dialog with a list of selected files under 'CLEAR ALL':

- MORIARTY\_jmoriarty\_2023.06.02\_16.05.03.zip
  - Logs
  - Saved\_Files
  - Volatile\_Data

Both windows include sections for CASE DETAILS, PROCESSING DETAILS, ARTIFACT DETAILS, and ANALYZE EVIDENCE.



# YARA

Magnet AXIOM Process 7.1.0.35864

File Tools Help

## SEARCH WITH YARA RULES

**CASE DETAILS**

EVIDENCE SOURCES 2

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption
- Add keywords to search
- Extract text from files (OCR)
- Calculate hashes and find matches On
- Analyze chats with Magnet.AI
- Analyze pictures with Magnet.AI
- Add CPS data to search
- Search with YARA rules** On
- Find more artifacts

ARTIFACT DETAILS 221

- Mobile artifacts
- Cloud artifacts
- Computer artifacts 221 of 271
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

**YARA RULE SETS**

Use YARA rules to identify matching files. You can import YARA rule sets from a folder containing .yar or .yara files, or you can manually add YARA rule sets.

NOTE: Running several YARA rule sets at once might increase scan times.

Reading YARA rule sets from 1 synced folders. [EDIT](#)

X Q

<a href="#">SELECT ALL</a>	<a href="#">ADD NEW RULE SET</a>	<a href="#">REFRESH</a>	Rules selected: 4
Enabled	Rule set name	Source path	Date created
<input checked="" type="checkbox"/>	ADApps.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:26:41 PM
<input checked="" type="checkbox"/>	kiwi_passwords.yar	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:26:54 PM
<input checked="" type="checkbox"/>	remote_access_apps.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:25:24 PM
<input checked="" type="checkbox"/>	SharpHound.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:26:32 PM
<input type="checkbox"/>	Linux.Virus.Vit.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Awfull.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Cmay.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.DeadCode.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Elerad.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Greenp.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Mocket.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Negt.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Trojan.CaddyWiper.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Trojan.Dridex.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM

BACK
GO TO FIND MORE ARTIFACTS



# KEYWORDS

Magnet AXIOM Process 7.1.0.35864

File Tools Help

### ADD KEYWORDS TO SEARCH

CASE DETAILS

EVIDENCE SOURCES 2

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption
- Add keywords to search On
- Extract text from files (OCR)
- Calculate hashes and find matches On
- Analyze chats with Magnet.AI
- Analyze pictures with Magnet.AI
- Add CPS data to search
- Search with YARA rules On
- Find more artifacts

ARTIFACT DETAILS 221

- Mobile artifacts
- Cloud artifacts
- Computer artifacts 221 of 271
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

KEYWORD LISTS

ADD KEYWORD LIST

Keyword lists added: 1

Enabled	File source	Date loaded	Number of records
<input checked="" type="checkbox"/>	F:\RansomCare\keywords.txt	5/26/2023 3:46:50 PM	53

KEYWORDS

ADD KEYWORD

Keywords added: 53

Keyword	Regex / GREP
psexesvc	<input type="checkbox"/>
rar.exe	<input type="checkbox"/>
rclone	<input type="checkbox"/>
recycle	<input type="checkbox"/>
Reflection	<input type="checkbox"/>
Remove-Module	<input type="checkbox"/>
rundll32	<input type="checkbox"/>
scrcons	<input type="checkbox"/>
Set-PSReadLineOption	<input type="checkbox"/>
silver	<input type="checkbox"/>
Start-Process	<input type="checkbox"/>

BACK GO TO EXTRACT TEXT FROM FILES (OCR)



# ARTIFACTS FROM RESPONSE TRIAGE

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet AXIOM Examine v7.1.0.35864 - Magnet RESPONSE Demo

File Tools Process Help

Case dashboard

## CASE OVERVIEW

### CASE OVERVIEW

EVIDENCE SOURCES 3

- RAMDump-MORIARTY-20230602-160503...
- RAMDump-MORIARTY-20230602-160503...
- MORIARTY\_jmoriarty\_2023.06.02\_16.05.03.zip

### INSIGHTS

Potential Cloud Evidence Leads 0

### CASE PROCESSING DETAILS

CASE NUMBER Magnet RESPONSE Demo

SCAN 1

Scanned by Doug Metz  
Scan date/time - local time 6/2/2023 4:31:55 PM  
Scan description

[VIEW SCAN SUMMARY](#)

### PROJECT REVIEW ONLINE

You can integrate Magnet AXIOM with the Project REVIEW Online beta, a SaaS platform that allows users to review and collaborate with important stakeholders. [SHOW MORE](#)

### CASE INFORMATION

The Case Information.txt file contains information about how the case was processed. For example, the file includes the settings that were applied to the search, search type, number of artifacts discovered, and more.

[OPEN CASE INFORMATION FILE](#)

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

[OPEN LOG FILE](#)

## EVIDENCE OVERVIEW

ADD NEW EVIDENCE

RAMDump-MORIARTY-20230602-160503-W... (26,857)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.dmp

Description

Location RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.dmp

Platform Computer

Process method Parsing and carving

No picture added

CHANGE PICTURE

RAMDump-MORIARTY-20230602-160503-W... (141,106)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.json.zip

Description

Location RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.json.zip

Platform Computer

Process method Parsing and carving

No picture added

CHANGE PICTURE

MORIARTY\_jmoriarty\_2023.06.02\_16.05.03... (2,562,195)

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number MORIARTY\_jmoriarty\_2023.06.02\_16.05.03.zip

Description

## PLACES TO START

### ARTIFACT CATEGORIES

VIEW ALL ARTIFACT CATEGORIES

Evidence source All

Number of artifacts 2,730,158

Operating System	Count	Total
Memory	140,821	2,508,197
Web Related	64,513	
Media	9,379	
Refined Results	3,928	
Custom	1,583	
...	...	

### TAGS AND COMMENTS

### IDENTIFIER MATCHES

Magnet AXIOM can compare identifiers found in this case with identifiers from other cases that your organization has uploaded to the Magnet Prague database. These identifiers can include people identifiers, such as email addresses or phone numbers, and device identifiers, such as camera serial numbers or phone IMEs.

For more information and to download a beta copy of the Magnet Prague server software, visit Magnet Idea Lab.

<https://magnetidealab.com/> COPY URL

Once you have installed the Magnet Prague server software, configure product integration settings to connect Magnet AXIOM to Magnet Prague.

[CONFIGURE PRODUCT INTEGRATIONS](#)

### CPS DATA MATCHES

### MAGNET.AI CATEGORIZATION

### KEYWORD MATCHES (2,028,489)

VIEW ALL KEYWORD MATCHES

KEYWORD MATCHES



# POWERSHELL HISTORY

Magnet AXIOM Examine v5.9.0.30292 - CSIRT-USB W11

File Tools Process Help

**FILTERS** Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

Type a search term... GO ADVANCED

**EVIDENCE (2,033)**

**Column view**

	Order	Command List (UTF8)	Command List (Raw)	Artifact type
	1787	\kape.exe --sync	b'\\kape.exe --sync'	PowerShell H
	1788	ls	b'ls'	PowerShell H
	1789	\KAPE-EZToolsAncillaryUpdater.ps1	b'\\KAPE-EZToolsAncillaryUpdater.ps1'	PowerShell H
	1790	ls	b'ls'	PowerShell H
	1791	cd ..	b'cd ..'	PowerShell H
	1792	ls	b'ls'	PowerShell H
	1793	cd .\volatility3\	b'cd .\\volatility3\\'	PowerShell H
	1794	ls	b'ls'	PowerShell H
	1795	\vol.py -h	b'\\vol.py -h'	PowerShell H
	1796	python --version	b'python --version'	PowerShell H
	1797	python .\vol.py -h	b'python .\\vol.py -h'	PowerShell H
	1798	\$LogicalDisk = @()	b'\$LogicalDisk = @()'	PowerShell H
	1799	Get-WmiObject Win32_LogicalDisk -filter "DriveTy..."	b'Get-WmiObject Win32_LogicalDisk -filter "DriveTy..."	PowerShell H
	1800	\$LogicalDisk += @(\$_   Select @{n="Name";e={...}}	b' \$LogicalDisk += @(\$_   Select @{n="Name";e={...}}	PowerShell H
	1801	@{n="Volume Label";e={\$_._VolumeName}}`	b' @{n="Volume Label";e={\$_._VolumeName}},`	PowerShell H
	1802	@{n="Size (Gb)";e=("{0:N2}" -f (\$_.Size/1GB))}`	b' @{n="Size (Gb)";e=("{0:N2}" -f (\$_.Size/1GB))},`	PowerShell H
	1803	@{n="Used (Gb)";e=("{0:N2}" -f ((\$_.Size/1GB) - ...	b' @{n="Used (Gb)";e=("{0:N2}" -f ((\$_.Size/1GB) - ...	PowerShell H
	1804	@{n="Free (Gb)";e=("{0:N2}" -f (\$_.FreeSpace/1G...	b' @{n="Free (Gb)";e=("{0:N2}" -f (\$_.FreeSpace/1...	PowerShell H
	1805	@{n="Free (%)"e=(if(\$_.Size) ("{0:N2}" -f ((\$_.Fre...	b' @{n="Free (%)"e=(if(\$_.Size) ("{0:N2}" -f (\$_.Fre...	PowerShell H
	1806	)`	b' )`	PowerShell H
	1807	\$LogicalDisk   Format-Table -AutoSize   Out-String	b'\$LogicalDisk   Format-Table -AutoSize   Out-String'	PowerShell H
	1808	Invoke-RestMethod -Uri ('https://ipinfo.io/')	b'Invoke-RestMethod -Uri ('https://ipinfo.io/')	PowerShell H
	1809	python .\vol.py -h	b'python .\\vol.py -h'	PowerShell H
	1810	cd /	b'cd /'	PowerShell H
	1811	cd .\Users\dmetz\Downloads\	b'cd .\\Users\\dmetz\\Downloads\\'	PowerShell H

1 **2022-02-15T132640\_DMETZ-W10.vhd**

**DETAILS**

Order 1

Command List (UTF8) python --version

Command List (Raw) b'python --version'

Artifact type PowerShell History

Item ID 586032

**EVIDENCE INFORMATION**

Source 2022-02-15T132640\_DMETZ-W10.vhd  
- Partition 1 (Microsoft NTFS, 11.85 GB)  
KAPE (2022-02-15T13:26:40)\C\Users\dmetz\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost\_history.txt

Recovery method Parsing

Deleted source

Location n/a

Evidence number 2022-02-15T132640\_DMETZ-W10.vhd

TAGS, COMMENTS & PROFILES

Time zone UTC+0:00



# FIREWALL EVENTS

Magnet AXIOM Examine v5.9.0.30292 - CSIRT USB W11

File Tools Process Help

**FILTERS** Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone

Type a search term... GO ADVANCED

**EVIDENCE (1,403)**

Column view

	Event ID	Created Date/Timestamp	Event Type	Event Description Summary	Rule ID
	2004	2/14/2022 8:53:04 PM	307	A rule has been added to the Windows Firewall exception list.	{8B724E29-6C65-4399-B1C8}
	2004	2/14/2022 8:53:04 PM	308	A rule has been added to the Windows Firewall exception list.	{A8E695EF-27BD-4830-B3AF}
	2004	2/14/2022 8:53:04 PM	309	A rule has been added to the Windows Firewall exception list.	{3B65252B-EB81-4B31-B91D}
	2004	2/14/2022 8:53:04 PM	310	A rule has been added to the Windows Firewall exception list.	{E344DFB1-72BC-43AF-B0A1}
	2004	2/14/2022 8:53:04 PM	311	A rule has been added to the Windows Firewall exception list.	{57D99815-6AF3-41B1-8B24}
	2004	2/14/2022 8:53:17 PM	312	A rule has been added to the Windows Firewall exception list.	{80F1EA52-4FED-40F1-98E7}
	2004	2/14/2022 8:53:17 PM	313	A rule has been added to the Windows Firewall exception list.	{FC968866-F413-4D1B-A0C2}
	2006	2/14/2022 8:54:33 PM	314	A rule has been deleted in the Windows Firewall exception list.	{3B65252B-EB81-4B31-B91D}
	2006	2/14/2022 8:54:33 PM	315	A rule has been deleted in the Windows Firewall exception list.	{A8E695EF-27BD-4830-B3AF}
	2004	2/14/2022 8:49:31 PM	10	A rule has been added to the Windows Firewall exception list.	{884168A9-58A1-4719-A111}
	2004	2/14/2022 8:49:31 PM	13	A rule has been added to the Windows Firewall exception list.	{47E0E03C-07D3-417E-933A}
	2004	2/14/2022 8:49:31 PM	12	A rule has been added to the Windows Firewall exception list.	{FC8AEA85-1A02-459A-98F4}
	2006	2/14/2022 8:49:31 PM	14	A rule has been deleted in the Windows Firewall exception list.	{FC8AEA85-1A02-459A-98F4}
	2004	2/14/2022 8:49:31 PM	11	A rule has been added to the Windows Firewall exception list.	{167FD499-2C58-437E-B2FF}
	2006	2/14/2022 8:49:31 PM	15	A rule has been deleted in the Windows Firewall exception list.	{167FD499-2C58-437E-B2FF}
	2006	2/14/2022 8:49:31 PM	16	A rule has been deleted in the Windows Firewall exception list.	{884168A9-58A1-4719-A111}
	2006	2/14/2022 8:49:31 PM	17	A rule has been deleted in the Windows Firewall exception list.	{47E0E03C-07D3-417E-933A}
	2004	2/14/2022 8:49:31 PM	18	A rule has been added to the Windows Firewall exception list.	{2337CE28-2973-4EAS-96EB}
	2004	2/14/2022 8:49:31 PM	19	A rule has been added to the Windows Firewall exception list.	{9864DEDA-F8CA-4990-9BC}
	2004	2/14/2022 8:49:31 PM	20	A rule has been added to the Windows Firewall exception list.	{6E024BF2-B25F-46E7-9203}
	2004	2/14/2022 8:49:31 PM	21	A rule has been added to the Windows Firewall exception list.	{8A6E7D10-A9D4-44AE-B2B}
	2006	2/14/2022 8:51:10 PM	29	A rule has been deleted in the Windows Firewall exception list.	{3daaa47ad-4db9-45b8-8f97-}
	2006	2/14/2022 8:51:10 PM	30	A rule has been deleted in the Windows Firewall exception list.	{88d76b46-70a0-47be-ad62-}
	2004	2/14/2022 8:51:10 PM	31	A rule has been added to the Windows Firewall exception list.	{8044754e-571c-414a-b91b-}
	2004	2/14/2022 8:51:10 PM	32	A rule has been added to the Windows Firewall exception list.	{7f42be00-bd25-41f9-ba12-a}
	2006	2/14/2022 8:51:10 PM	33	A rule has been deleted in the Windows Firewall exception list.	{15090595-6681-4544-96CD}

**2004**

**DMETZ-W10\_20220215\_082500.raw**

**DETAILS**

**ARTIFACT INFORMATION**

Event ID **2004**  
 Created Date/Time **2/14/2022 8:53:17 PM**  
 Event Record ID **313**  
 Event Description Summary **A rule has been added to the Windows Firewall exception list.**  
 Rule ID **{FC968866-F413-4D1B-A0C2-90F00F0EFA02}**  
 Rule Name **OneDrive**  
 Modifying User **S-1-5-80-3088073201-1464728630-1879813800-1107566885-823218052**  
 Modifying Application **C:\WINDOWS\System32\svchost.exe**  
 Direction **Outbound**  
 Event Data **<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="Microsoft-Windows-Firewall With Advanced Security" Guid="d1bc9aff-2abf-4d71-9146-ecb2a986eb85"/><EventID>2004</EventID><Version>0</Version><Level>4</Level><Task>0</Task><Opcode>0</Opcode><Keywords>0x8000020000000000**

Time zone UTC+0:00



# SYSTEM RESOURCE USAGE MONITOR (SRUM)

Magnet AXIOM Examine v5.9.0.30292 - CSIRT USB W11

**FILTERS** Evidence Artifacts Content types Date and time Tags and comments Profiles

**EVIDENCE (69,398)**

Entr...	Application Name
70970	
28271	SMB
71080	SMB
80279	teams.exe
73746	
37402	
73739	teams.exe
60863	SMB
61649	
73557	
55880	SMB
73550	teams.exe
37535	SMB
62551	
55904	SMB
61640	teams.exe
56705	
62543	teams.exe
56695	teams.exe
81459	
87369	
87388	powerpnt.exe
55927	SMB
51669	
70966	onedrive.exe
51666	teams.exe

**INDUSTRY NEWS OCTOBER 5, 2022**

**What is SRUM?**

**Table of Contents**

- [Accessing SRUDB.dat](#)
- [SRUM Artifact Categories](#)
- [SRUM Application Resource Usage](#)
- [SRUM Energy Usage \(and Extended Usage\)](#)
- [SRUM Network Connections](#)
- [SRUM Network Usage](#)
- [SRUM Push Notification Data](#)
- [A Lot to be Learned With SRUM](#)

**SRUM: Forensic Analysis of Windows System Resource Utilization Monitor**

SRUM, or System Resource Utilization Monitor, is a feature of modern Windows systems (Win8+), intended to track the application usage, network utilization and system energy state.

**EVIDENCE INFORMATION**

Source: 2022-02-15T132640 DMETZ-W10.vhdx - Partition 1 (Microsoft NTFS, 11.85 GB)  
KAPE (2022-02-15T13:26:40) \Windows\System32\SRU\SRUDB.dat

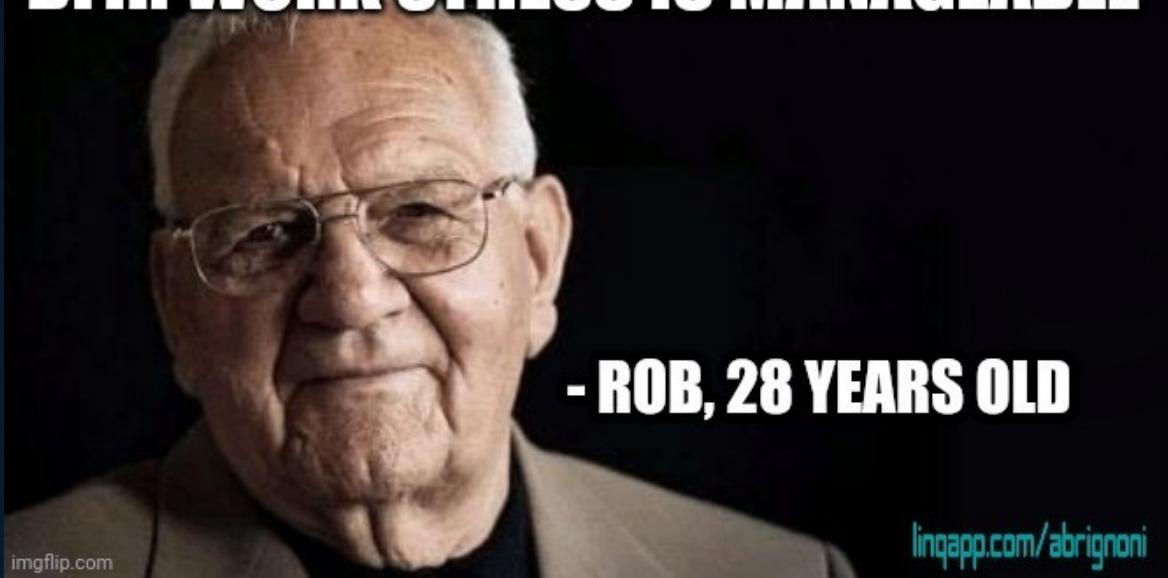
Recovery method: Parsing

Time zone: UTC+0:00



# RESPONDING AT SCALE

**DFIR WORK STRESS IS MANAGEABLE**





# RESPONDING AT SCALE WITH POWERSHELL

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")
#####
```



# 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



# RESPONSE CLI CAPTURE OPTIONS

- |                             |   |
|-----------------------------|---|
| /captoreram                 | - 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<br>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<br>e.g. /maxsize:500                         |
| /captureransomnotes         | - Enables the ransomware ransom note collection   |



# COLLECTION PROFILES

```
##### Extended Process Capture
<#
$profileName = "EXTENDED PROCESS CAPTURE"
$arguments = "/capturevolatile /captureextendedprocessinfo /saveprocfiles"
#>
##### System Files
$profileName = "SYSTEM FILES"
$arguments = "/capturesystemfiles"
#>
##### Just RAM
<#
$profileName = "CAPTURE RAM"
$arguments = "/captureram"
#>
```



# 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





# MAGNET RESPONSE POWERSHELL

A screenshot of an Administrator PowerShell window titled "Administrator: PowerShell". The window displays the following text:

```
Magnet RESPONSE v1.7
©2021-2023 Magnet Forensics Inc

Selected Profile: SYSTEM FILES
Output directory: \\192.168.4.178\Automate\WatchFolders\Magnet_Response

Hostname: MBP-WIN-11
Operating System: Microsoft Windows 11 Home
Architecture: ARM 64-bit Processor

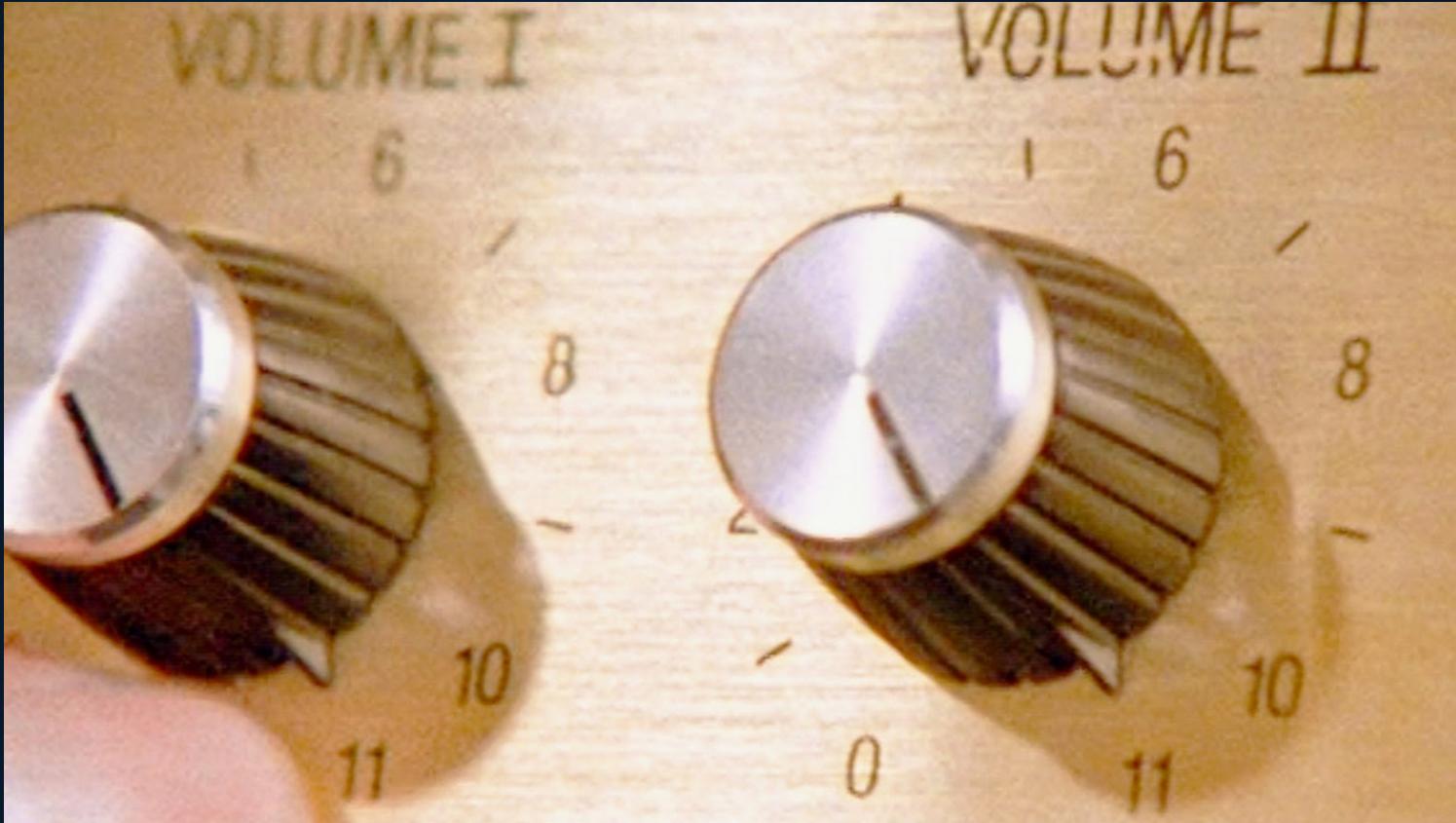
[Collecting Arifacts]
```

The background of the slide features a dark blue abstract wave pattern.

SEEK JUSTICE. PROTECT THE INNOCENT.



# TURN IT UP TO 11



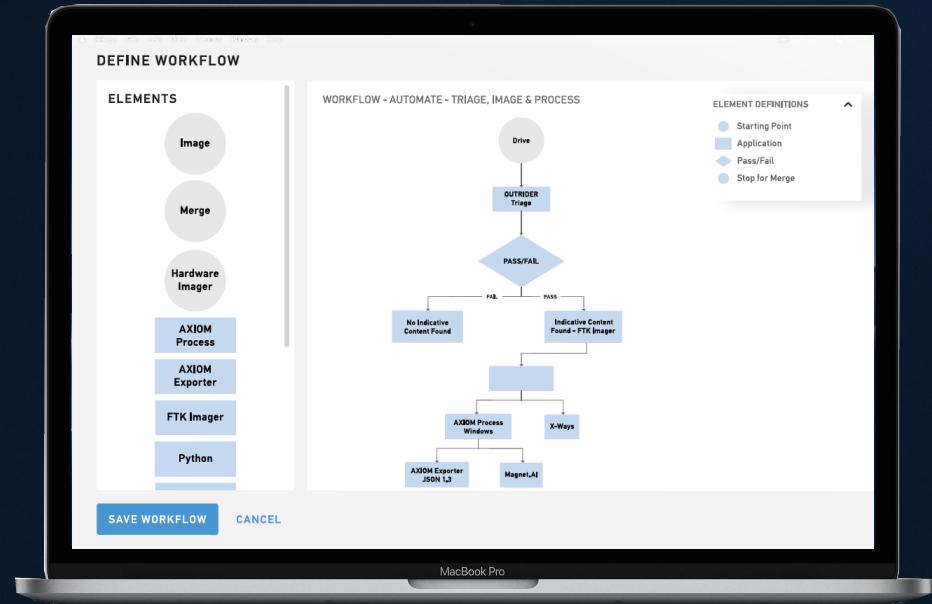
SEEK JUSTICE. PROTECT THE INNOCENT.

[magnetforensics.com](http://magnetforensics.com)



# MAGNET AUTOMATE

SEEK JUSTICE. PROTECT THE INNOCENT.



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

[magnetforensics.com](http://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**

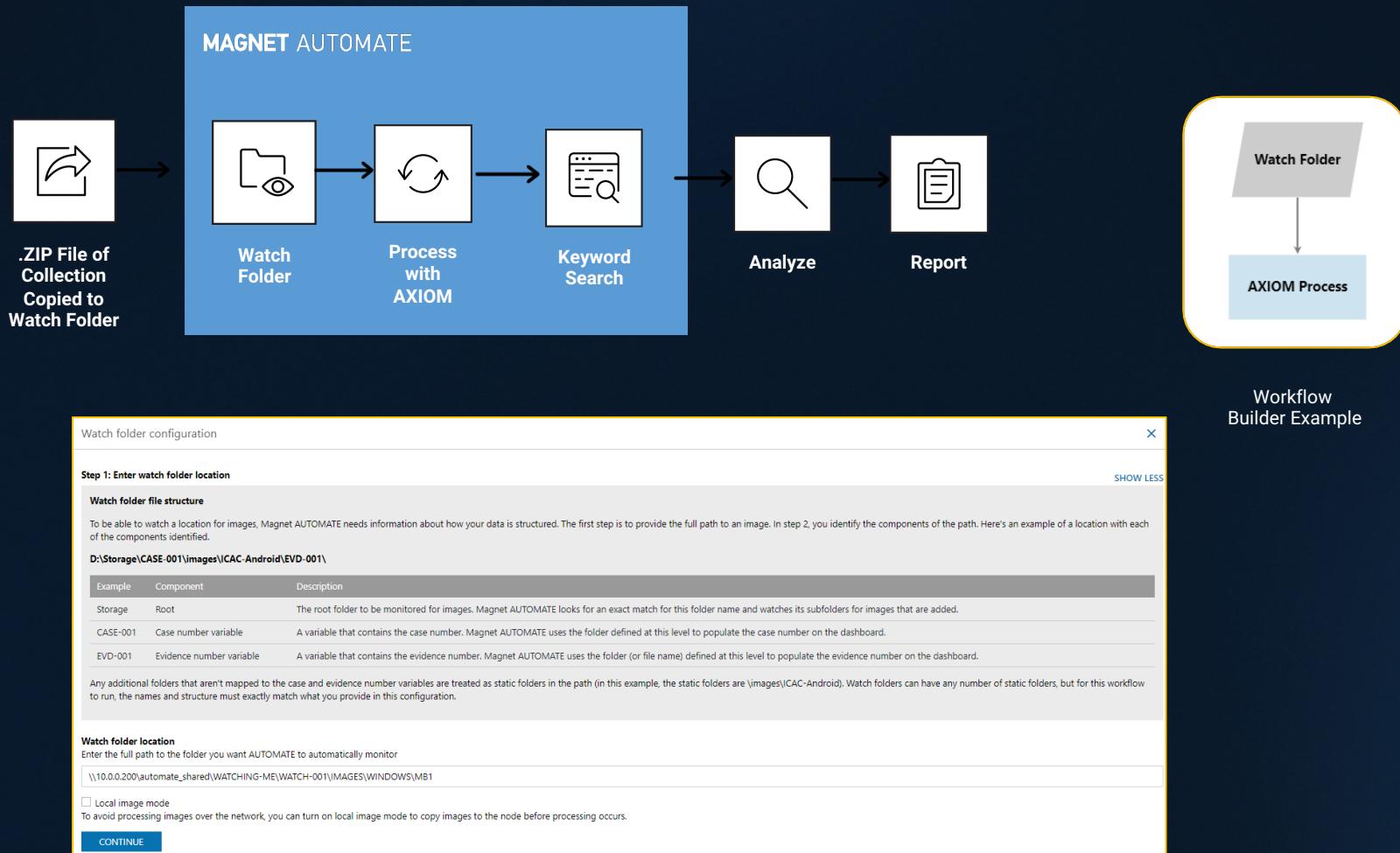
File name of forensic image RESET

**CONTINUE**



# AUTOMATIC FORENSIC PROCESSING

## With a Watch Folder



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 3<sup>rd</sup> party tools that have CLI options.



# TRIAGE AUTOMATION

The collage illustrates the workflow and integration of Magnet Forensics tools:

- Top Left:** A terminal window on a Mac (dmetz@dmetz-mbpro) showing the execution of `sh RESPONSEserver.sh`. It outputs network configuration and a message about serving HTTP on port 80.
- Top Right:** A Windows File Explorer window titled "Magnet\_RESPONSE" showing two folders: "inc-8675309-mbp-win-11" (modified today at 12:04 PM) and "inc-8675309-morarity" (modified today at 11:48 AM).
- Middle Left:** A PowerShell window titled "Administrator: PowerShell" running "MAGNET RESPONSE v1.7". It shows the selected profile is "SYSTEM FILES", the output directory is "\\Automate\WatchFolders\Magnet\_RESPONSE", and the acquisition completed in 1 minute and 44 seconds.
- Middle Right:** A screenshot of the "MAGNET AUTOMATE Enterprise" web interface. The dashboard shows an "Overview" section with three cards: "Node status" (2 nodes, 1 available, 1 processing), "Case status" (2 successful, 1 in progress, 0 needs attention, 0 failed, 0 waiting to merge), and "Cases in progress" (1 case, 50% progress for "inc-8675309-mbp-win-11"). Below the dashboard are sections for "Weekly performance stats" (Data throughput, Evidence sources complete) and "Workflow usage".
- Bottom Center:** A flowchart titled "FORENSIC AUTOMATION" illustrating the process: Collect Endpoint → Process → Analyze → Report.

Triage collection to processed case in <|= 1 click

[magnetforensics.com](https://magnetforensics.com)



# MAGNET AXIOM™ CYBER

## Request Your Free Trial

[magnetforensics.com/magnet-axiom-cyber/](https://magnetforensics.com/magnet-axiom-cyber/)

# THANK YOU

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



<https://github.com/dwmetz>



<https://bakerstreetforensics.com>



[doug.metz@magnetforensics.com](mailto:doug.metz@magnetforensics.com)



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



<https://infosec.exchange/@dwmetz>



@dwmetz

