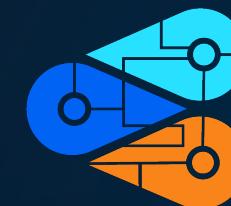




MAGNET RESPONSE for Digital First Responders

Doug Metz

Senior Security Forensics Specialist
MAGNET Forensics

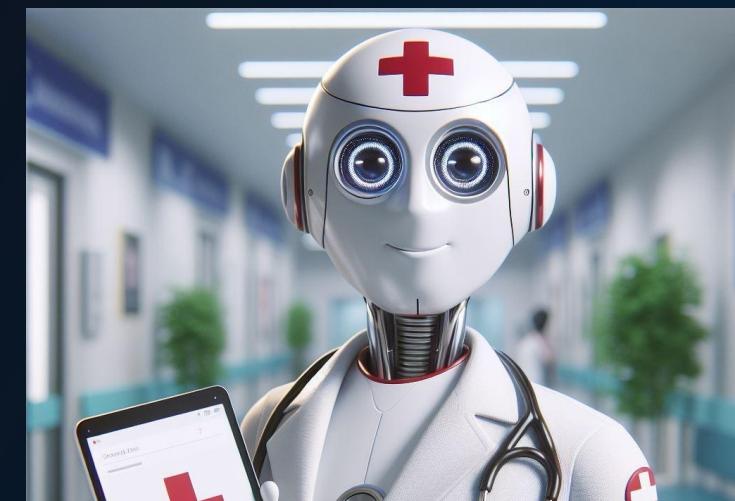


HTCIA

HTCIA New England

27 March 2023

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

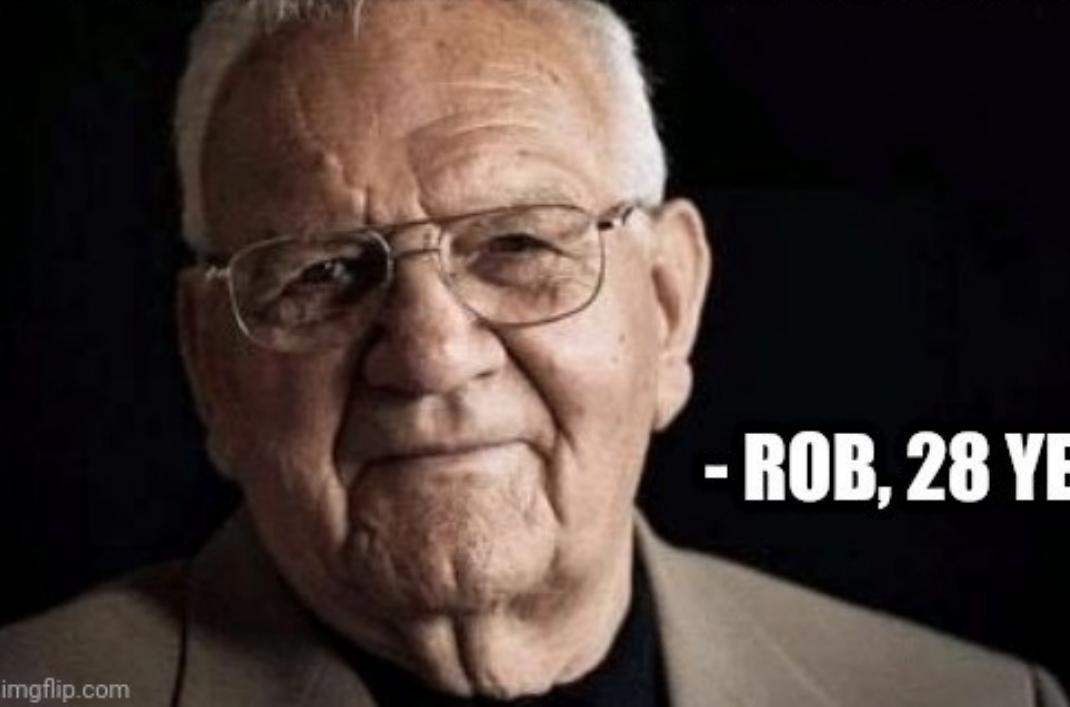


magnetforensics.com



About Me

DFIR WORK STRESS IS MANAGEABLE



imgflip.com

- ROB, 28 YEARS OLD

linqapp.com/abrigoni

About Me



MAGNET
FORENSICS®

The Auxtera Project



BAKER STREET FORENSICS

D . F . I . R .



HTCIA

Delaware Valley - Philadelphia



powered by dot

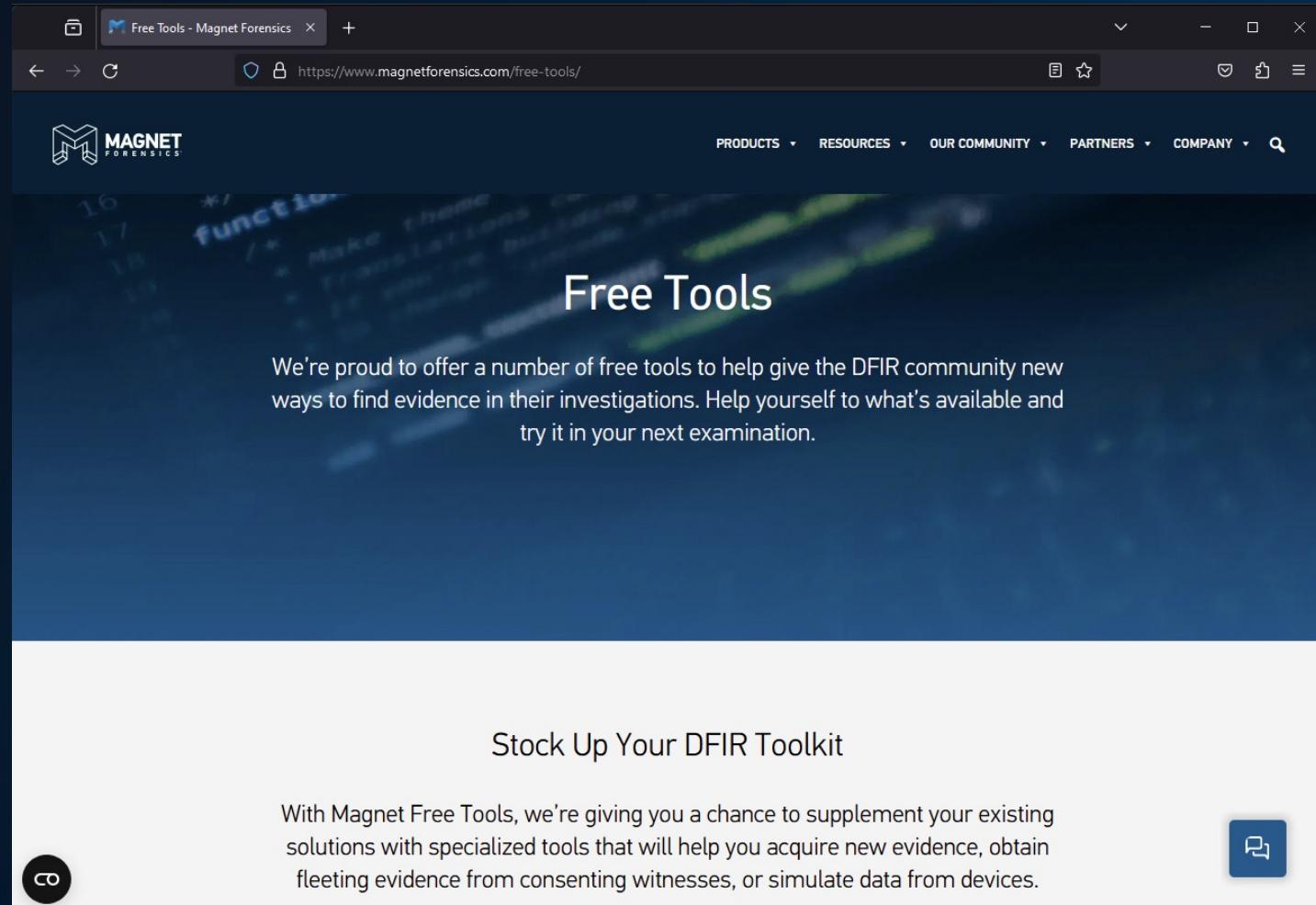
magnetforensics.com



Agenda

- Introduction to MAGNET RESPONSE
- Memory Acquisitions Made Easy
- Local captures with USB
- Triage Collection Verification
- MAGNET Response CLI (Command Line Interface)
- Enterprise Collections with PowerShell
- Processing Triage Collections with MAGNET Axiom
- Taking Triage Collections to the Next Level

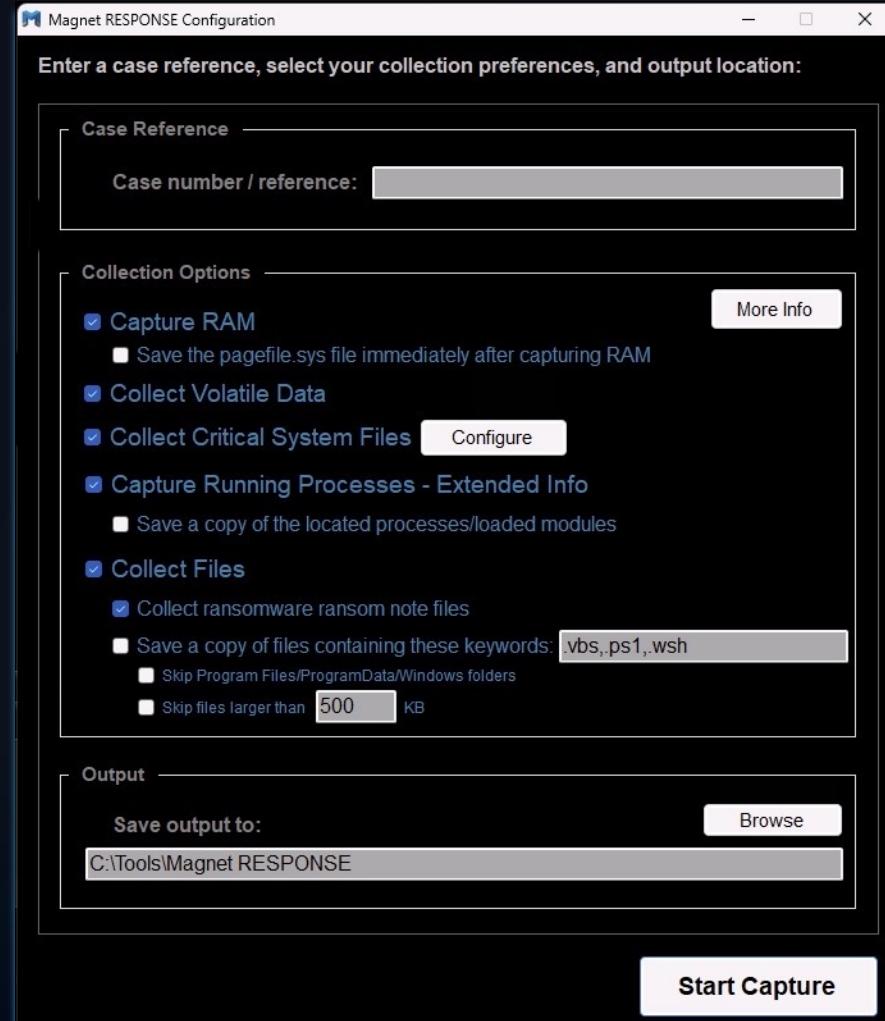
MAGNET RESPONSE



The screenshot shows a web browser window displaying the Magnet Forensics website at <https://www.magnetforensics.com/free-tools/>. The page has a dark blue background with a blurred image of a computer screen showing code. At the top, there's a navigation bar with links for PRODUCTS, RESOURCES, OUR COMMUNITY, PARTNERS, COMPANY, and a search icon. The main heading is "Free Tools" in large white text. Below it, a paragraph reads: "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, there's a section titled "Stock Up Your DFIR Toolkit" with a paragraph about the free tools and a blue "Get Started" button.



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.”

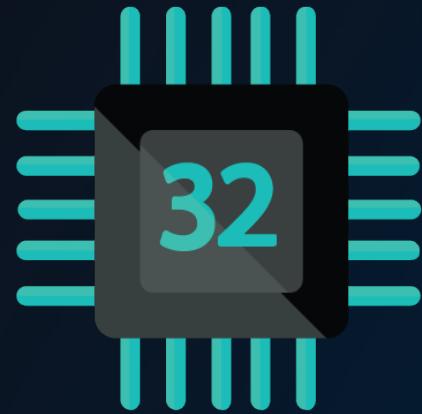
This makes Magnet RESPONSE useful in situations where non-technical users may need to collect and preserve data on behalf of law enforcement investigators as part of a cyber incident investigation.



MAGNET RESPONSE - RAM

Memory collection made easy

UNLOCK THE TRUTH. PROTECT THE INNOCENT.



VS





MAGNET RESPONSE Output



HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33

Name	Date modified	Type	Size
MORIARTY_jmoriarty_2023.03.14_13.16.33...	3/14/2023 1:21 PM	ZIP File	909,893 KB
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

UNLOCK THE TRUTH. 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	5 KB
Browser_History	3/14/2023 1:37 PM		IP_Info.txt	7 KB
Jumplists-AutomaticDestinations	3/14/2023 1:37 PM		Logged_On_Users.txt	1 KB
Jumplists-CustomDestinations	3/14/2023 1:37 PM		Network_Connections.txt	21 KB
MFT	3/14/2023 1:37 PM		Scheduled_Tasks.txt	42 KB
NTUSER.DAT	3/14/2023 1:37 PM		User_Accounts.txt	5 KB
PowerShell_History	3/14/2023 1:37 PM		Wifi_Info.txt	26 KB
Prefetch_Files	3/14/2023 1:37 PM		Windows_Services.txt	53 KB
Recent_Files	3/14/2023 1:37 PM		Windows_Version.txt	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			



USB Capture

High capacity/speed USB drive

SSD or NVME

* Tested on:

Samsung T5 1TB SSD

Samsung T7 1TB SSD

500GB NVME M.2 in enclosure

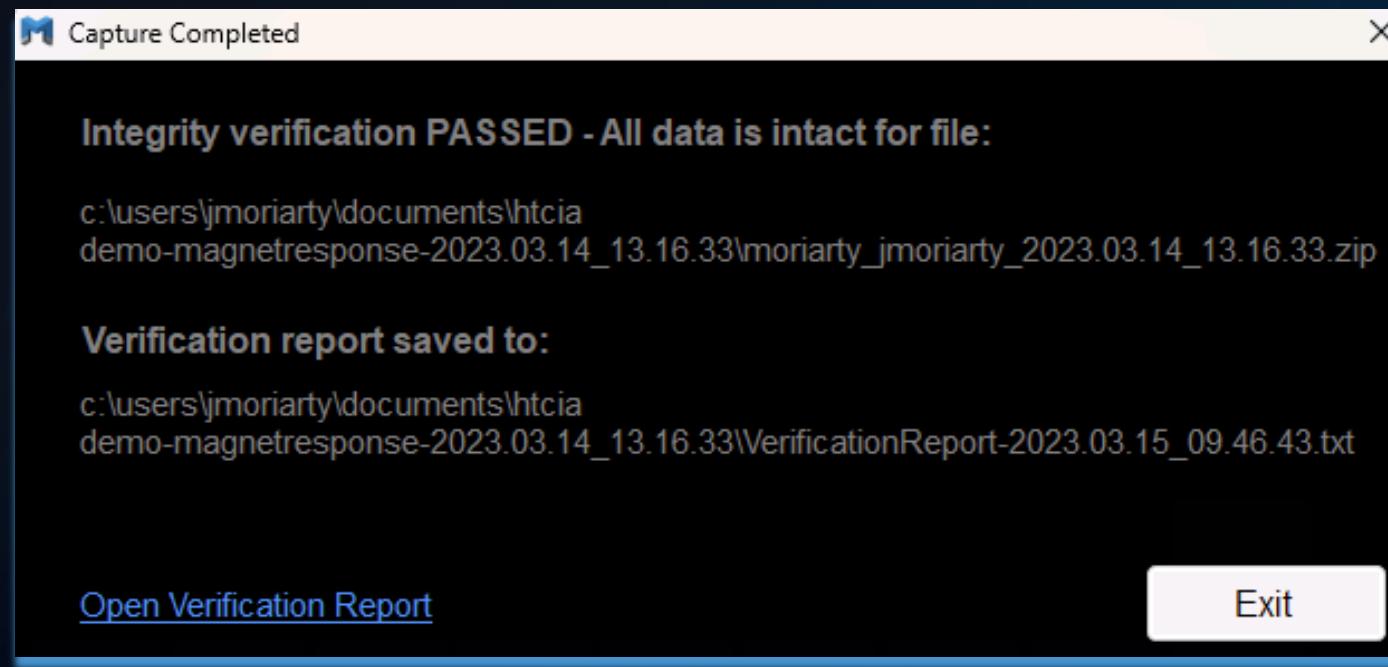




MAGNET RESPONSE Verification

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.





MAGNET RESPONSE CLI (Command Line Interface)



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
 - e.g. /capturefiles:secret,badfile,.vbs,confidential
 - 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
- /silent
 - No GUI output to screen



MAGNET RESPONSE

PowerShell



RESPONSE POWERSHELL OPERATIONS FLOW



Triggering Event



Script Executed on Endpoint



Endpoint retrieves MAGNETResponse.zip from Web server



Collection runs on endpoint per script parameters



Collection saved to Network share



MAGNET RESPONSE PowerShell

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

```
<#  
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.  
}  
### 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



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 with Microsoft Defender for Endpoint



DEFENDER RESPONSE OPERATIONS FLOW



Triggering Event



Analyst opens remote console session with
Defender for Endpoint



PowerShell script invoked via console



Collection runs on endpoint per script parameters



Collection saved to Network share or Local*



Local Collection downloaded to Examiner workstation



```
<#
.NOTES
Defender_RESPONSE.ps1
doug.metz@magnetforensics.com
v1.1

.SYNOPSIS
This script can be used to leverage Magnet RESPONSE and the Microsoft Defender for Endpoint Live Response console to capture triage collections on remote endpoints.

Prerequisites:
- Defender Live Response Console - upload MagnetRESPONSE.exe to the Library
- Defender Live Response Console - upload Defender_RESPONSE.ps1 to the Library

Operation:
1. 'connect' to endpoint in Live Response // establish connection with the endpoint
2. 'put MagnetRESPONSE.exe' // copies the exe to the target system
3. 'run Defender_RESPONSE.ps1' // where the magic happens

Retrieving the Data:

Once the script has finished running, the zipped output will be saved at the location "C:\Temp\RESPONSE" on the remote machine.

* Navigate to output folder using command - cd c:\Temp\RESPONSE
* List files using "dir" command
* Copy the zip filename <filename.zip>
* After the output filename is copied, collect the output by downloading it from the remote machine to your local system using the "Download" command. Download <filename.zip>

#>
Write-Host ""
Write-Host "Magnet RESPONSE v1.7
$([char]0x00A9)2021-2023 Magnet Forensics, LLC
"
$OS = $(((gcim Win32_OperatingSystem -ComputerName $server.Name).Name).split('|')[0])
$Arch = (get-wmiobject win32_operatingsystem).osarchitecture
$name = (get-wmiobject win32_operatingsystem).csname
$stopwatch = [System.Diagnostics.Stopwatch]::StartNew()
Write-Host "
Hostname: $name
Operating System: $OS
Architecture: $Arch
"
./MagnetRESPONSE.exe /accepteula /unattended /output:C:\temp\RESPONSE /caseref:DefenderRESPONSE /captureram
Write-Host "[Collecting Arifacts]"
Wait-Process -name "MagnetRESPONSE"
$null = $stopwatch.Elapsed
$Minutes = $StopWatch.Elapsed.Minutes
$Seconds = $StopWatch.Elapsed.Seconds
Write-Host "** Acquisition Completed in $Minutes minutes and $Seconds seconds.**"
```



C:\> library

File name

	Description	Parameters	Uploaded by
--	-------------	------------	-------------

Defender_RESPONSE.ps1		
-0500 (Eastern Standard Time)		
MagnetRESPONSE.exe		
-0500 (Eastern Standard Time)		

	Parameters description	Uploaded on
--	------------------------	-------------

No		Thu Nov 16 2023 10:59:23 GMT
----	--	------------------------------

GMT

Endpoints

General

[Advanced features](#)[Licenses](#)[Email notifications](#)[Auto remediation](#)

Permissions

[Roles](#)[Device groups](#)

APIs

[SIEM](#)

Rules

[Alert suppression](#)[EDR Exclusions](#)[Indicators](#)[Process Memory Indicators](#)[Web content filtering](#) On

Download quarantined files

Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine.

 On

Live Response

Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.

 Off

Live Response for Servers

Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.

 On

Live Response unsigned script execution

Enables using unsigned PowerShell scripts in Live Response.

 Off

Share endpoint alerts with Microsoft Compliance Center

Fowards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing you to enhance [insider risk management](#) policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.

 On

Microsoft Intune connection

Connects to [Microsoft Intune](#) to enable sharing of device information and enhanced policy enforcement.

Intune provides additional information about managed devices for secure score. It can use risk information to enforce [conditional access](#) and other security policies.

 On

Authenticated telemetry



```
C:\> run Defender_RESPONSE.ps1
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp\PSScriptOutputs\PSScript_Transcript_{94264446-9ED8-497F-AFE7-45A1DD98777A}.txt

Magnet RESPONSE v1.7
©2021-2023 Magnet Forensics, LLC

Hostname: OFFICE-2701139
Operating System: Microsoft Windows 10 Enterprise
Architecture: 64-bit

[Collecting Arifacts]
** Acquisition Completed in 0 minutes and 11 seconds.**

C:\> █
```

Retrieving the Data

Once the script finishes, the zipped output will be saved to “C:\Temp\RESPONSE” on the remote machine.

- Navigate to the output folder using the command — cd c:\Temp\RESPONSE
- List files using the “dir” command
- *Copy the zip filename*
- Download <filename.zip>



CYBERPIPE

V5.0 MAGNET Response

V4.01 KAPE

Administrator: PowerShell

```
.'';::cccccc:;..          ...'.....'.
.;ccc l l l o o o d x c .      .';cloo d d o o l c c :;:;.
.;ccc l l l o o o d x o .     ,.coxxxxx d l :,'..
'cccc c l l o o o d d d '     .,,,'lxkxxxo:'.
'cccc c l l o o o d d d '     .,:lxOkl,:oxo,.
';ccc c l l o o o d d d o .   .:dk00000k d ;''.
.;ccc c l l o o o d d d o .   .:lk00000lk d ;
.;ccc c l l o o o d d d c :co x k k k k 0 0 0 0 0 x :.
'cccc c l l o o o d d d x x x k k k k 0 0 0 0 x :.
,ccc c l l o o o d d d x x x k k k k x l c ,.
':l l l l o o o d d d x x x o c ;.
.'';:cloo d d d o l c :;:.
.....
```

CyberPipe IR Collection Script v5.0
<https://github.com/dwmetz/CyberPipe>
@dwmetz | ©2024 bakerstreetforensics.com

Mapping network drive...
Drive is mapped.
Collections directory exists.
Host directory created.

Running MAGNET Response...

Magnet RESPONSE v1.7
©2021-2024 Magnet Forensics Inc

Hostname: MORIARTY
Operating System: Microsoft Windows 11 Pro
Architecture: 64-bit
Selected Profile: Volatile (testing)
Output Directory: \Collections\MORIARTY-202402131644

HONEY, YOU SHOULD SEE ME IN A CROWN.

UNLOCK THE TRUTH. PROTECT THE INNOCENT.



CYBERPIPE OPERATIONS FLOW



Triggering Event



Script Executed on Endpoint



Triage Collection+ saved to USB or



Triage Collection+ Saved to Network share



CYBERPIPE

Functions:

- Capture a memory image with MAGNET DumplIt for Windows, (x32, x64, ARM64), or MAGNET RAM Capture on legacy systems;
- Create a Triage collection* with MAGNET Response;
- Check for encrypted disks with Encrypted Disk Detector;
- Recover the active BitLocker Recovery key;
- Save all artifacts, output, and audit logs to USB or source network drive.

There are collection profiles available for:

- Volatile Artifacts
- Triage Collection (Volatile, RAM, Pagefile, Triage artifacts)
- Just RAM
- RAM & Pagefile
- or build your own using the RESPONSE CLI options

Prerequisites:

- [MAGNET Response](#)
- [MAGNET Encrypted Disk Detector](#)



Processing

MAGNET RESPONSE

Collections with

MAGNET AXIOM™ CYBER



MAGNET AXIOM™ CYBER

Simplify your remote forensic investigations by focusing on the evidence that matters.

AXIOM Cyber is a digital forensics solution that allows organizations to perform remote acquisitions while collecting and analyzing evidence from cloud services, computers, and mobile devices.



Remote
Acquisition



Acquire From
The Cloud



Examine From
All Sources



Easy
Reporting



Quick
Root Cause
Analysis

Request a free trial <http://magnetforensics.com/magnet-axiom-cyber/>



Triage Processing

Computer > Windows > Load Evidence > IMAGE

The screenshot displays two windows from the Magnet AXIOM software interface.

Top Window: SELECT EVIDENCE SOURCE

- CASE DETAILS:** EVIDENCE SOURCES (1)
- PROCESSING DETAILS:** Options like "Search archives and mobile backups" (On), "Decode file-based encryption", "Add keywords to search", etc.
- ARTIFACT DETAILS:** 221 artifacts found, including Computer artifacts (221 of 271).
- ANALYZE EVIDENCE:**

Bottom Window: ADD FILES AND FOLDERS

- CASE DETAILS:** EVIDENCE SOURCES (1)
- PROCESSING DETAILS:** Options like "Search archives and mobile backups" (On), "Decode file-based encryption", etc.
- ARTIFACT DETAILS:** 221 artifacts found, including Computer artifacts (221 of 271).
- EVIDENCE SOURCES:** A list of selected files and folders:
 - MORIARTY_jmoriarty_2023.06.02_16.05.03.zip
 - Logs
 - Saved_Files
 - Volatile_Data
- Buttons:** BACK, NEXT



Comae Memory Processing

Computer > Windows > Load Evidence
> MEMORY

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



Artifacts from RESPONSE RAM & Triage

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

Magnet AXIOM Examine v7.1.0.35864 - Magnet RESPONSE Demo

File Tools Process Help

Case dashboard

CASE OVERVIEW

EVIDENCE SOURCES 3

- RAMDump-MORIARTY-20230602-160503...
- RAMDump-MORIARTY-20230602-160503...
- MORIARTY_jmoriarty_2023.06.02_16.05.03.zip

INSIGHTS 0

Potential Cloud Evidence Leads

CASE SUMMARY NOTES

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name Doug Metz

Case summary

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	2,508,197
Memory	140,821
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

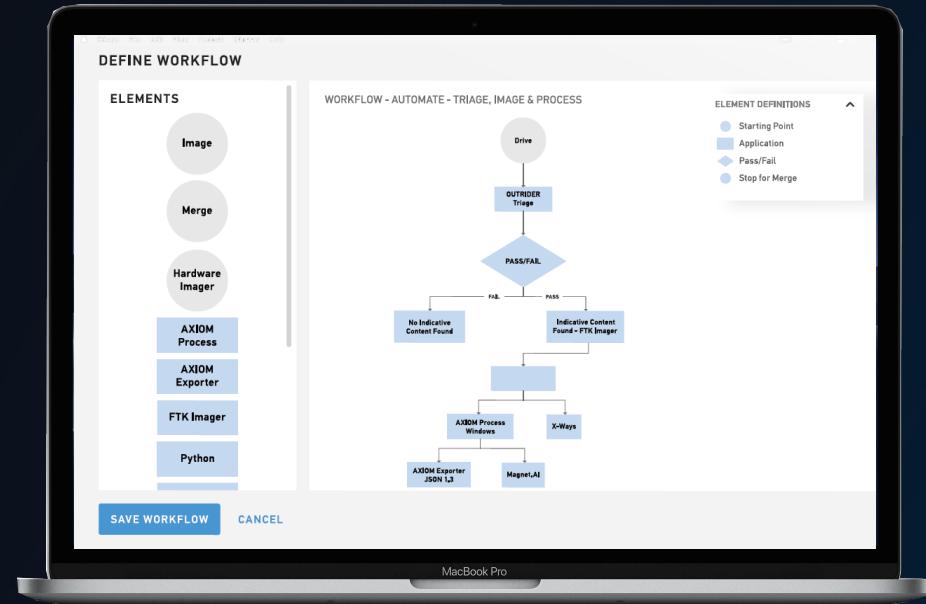


Turn It Up To 11





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



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

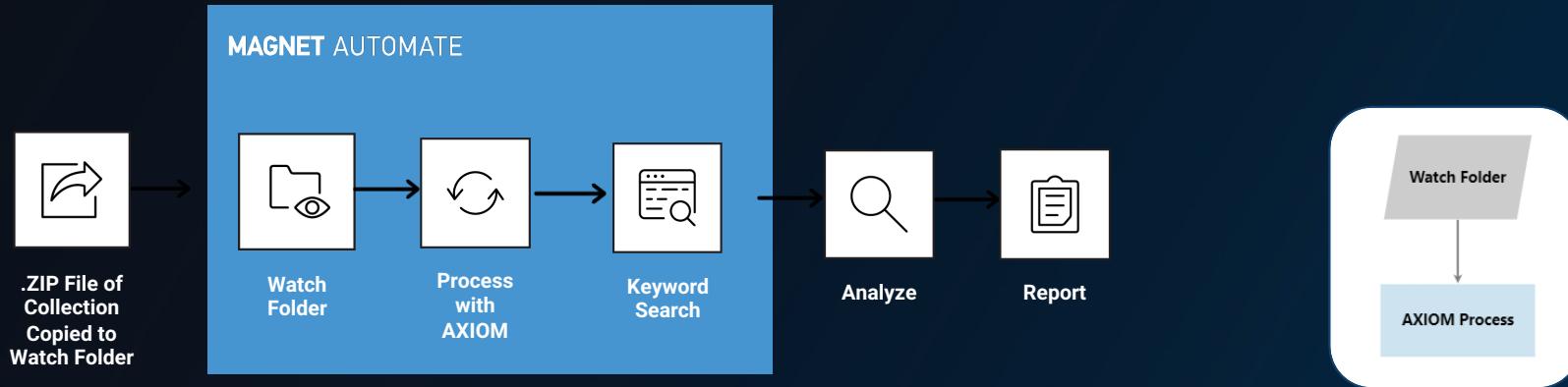
RESET

CONTINUE



Automatic Forensic Processing

With a Watch Folder



Watch folder configuration

Step 1: Enter watch folder location

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\{CAC-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\{CAC-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

\\\10.0.0.200\automate_shared\WATCHING-ME\WATCH-001\IMAGES\WINDOWS\MB1

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.

CONTINUE

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.

Triage Automation

The screenshot displays several windows illustrating the forensic automation process:

- Top Left:** A terminal window titled "Windows 11" showing the command "sh RESPONSEserver.sh" being run, indicating a live response or collection setup.
- Top Right:** A file explorer window titled "Magnet_RESPONSE" showing two folders: "inc-8675309-mbp-win-11" and "inc-8675309-moriarty".
- Middle Left:** A PowerShell window titled "Administrator: PowerShell" showing the output of the "Magnet RESPONSE v1.7" tool. It details the acquisition of "SYSTEM FILES" from "MBP-WIN-11" on "Microsoft Windows 11 Home" with an "ARM 64-bit Processor". The process took 1 minute and 44 seconds. The output directory is "\\Automate\WatchFolders\Magnet_RESPONSE".
- Middle Right:** A web browser window titled "MAGNET AUTOMATE Enterprise" showing the "OVERVIEW" dashboard. It includes sections for "Node status", "Case status", and "Cases in progress". The "Node status" section shows 2 nodes: BSL-AUTO-01 (7.3 GB free space) and BSL-AUTO-02 (30.8 GB free space). The "Case status" section shows 2 successful cases (66.67%), 1 in progress (33.33%), and 0 needs attention. The "Cases in progress" section shows 1 case for "inc-8675309-mbp-win-11" at 50% completion.
- Bottom Center:** A diagram titled "FORENSIC AUTOMATION" showing a linear process: Collect Endpoint → Process → Analyze → Report.

Triage collection to processed case in < | = 1 click

magnetforensics.com



Resources

Free Tools:

- MAGNET Response <https://magnetforensics.com/free-tools>
- MAGNET Encrypted Disk Detector <https://magnetforensics.com/free-tools>
- Magnet RESPONSE PowerShell <https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell>
- Defender Response PowerShell <https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell>
- CyberPipe <https://github.com/dwmetz/CyberPipe>

Blogs:

- Baker Street Forensics <https://bakerstreetforensics.com>
- Getting Started with MAGNET Response <https://www.magnetforensics.com/blog/getting-started-with-magnet-response>
- Responding at Scale with MAGNET Response <https://www.magnetforensics.com/blog/responding-at-scale-with-magnet-response>
- How To Run Remote Triage Collections on Quarantined Endpoints <https://www.magnetforensics.com/blog/how-to-run-remote-triage-collections-on-quarantined-endpoints/>



Thank You



<https://github.com/dwmetz>



<https://bakerstreetforensics.com>



doug.metz@magnetforensics.com



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



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



@dwmetz

