MAGNET RESPONSE for Digital First Responders

Doug Metz
Senior Security Forensics Specialist
MAGNET Forensics

HTCIA New England
27 March 2023

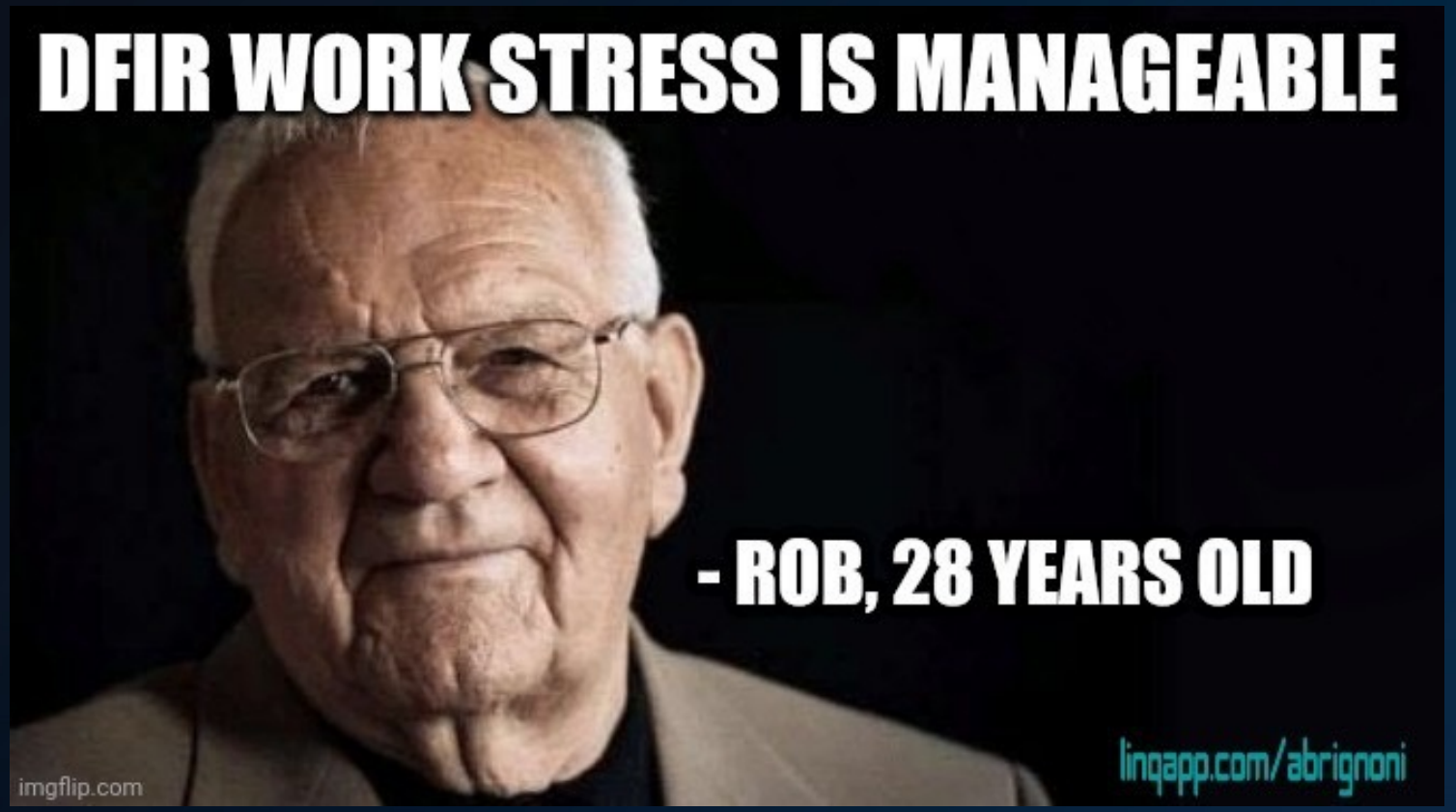
UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

About Me


DFIR WORK STRESS IS MANAGEABLE
- ROB, 28 YEARS OLD
linqapp.com/abrignoni
imgflip.com

About Me

MAGNET FORENSICS

The **Aux**tera Project

BAKER STREET FORENSICS

D . F . I . R .

HTCIA

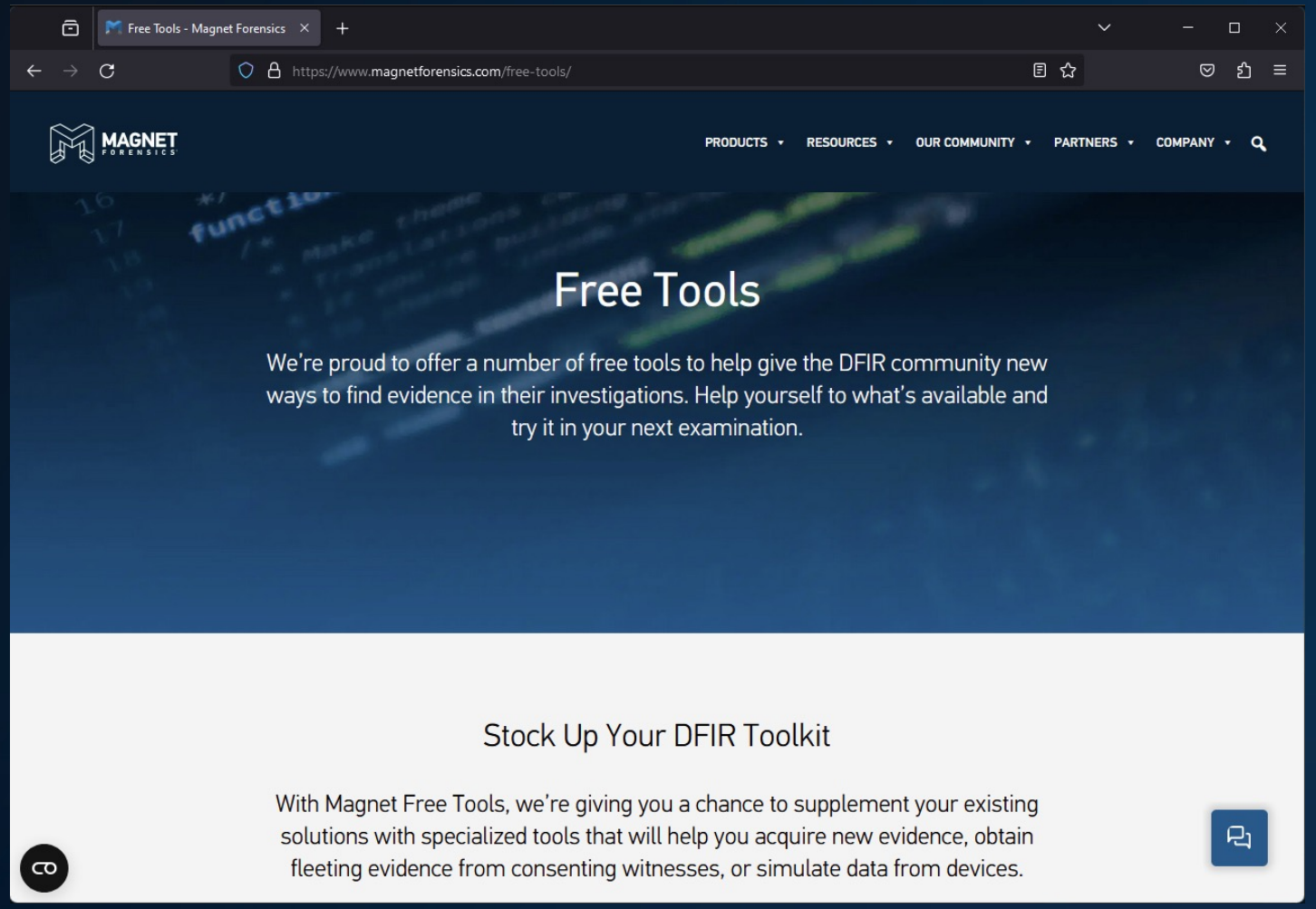
Delaware Valley - Philadelphia

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

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

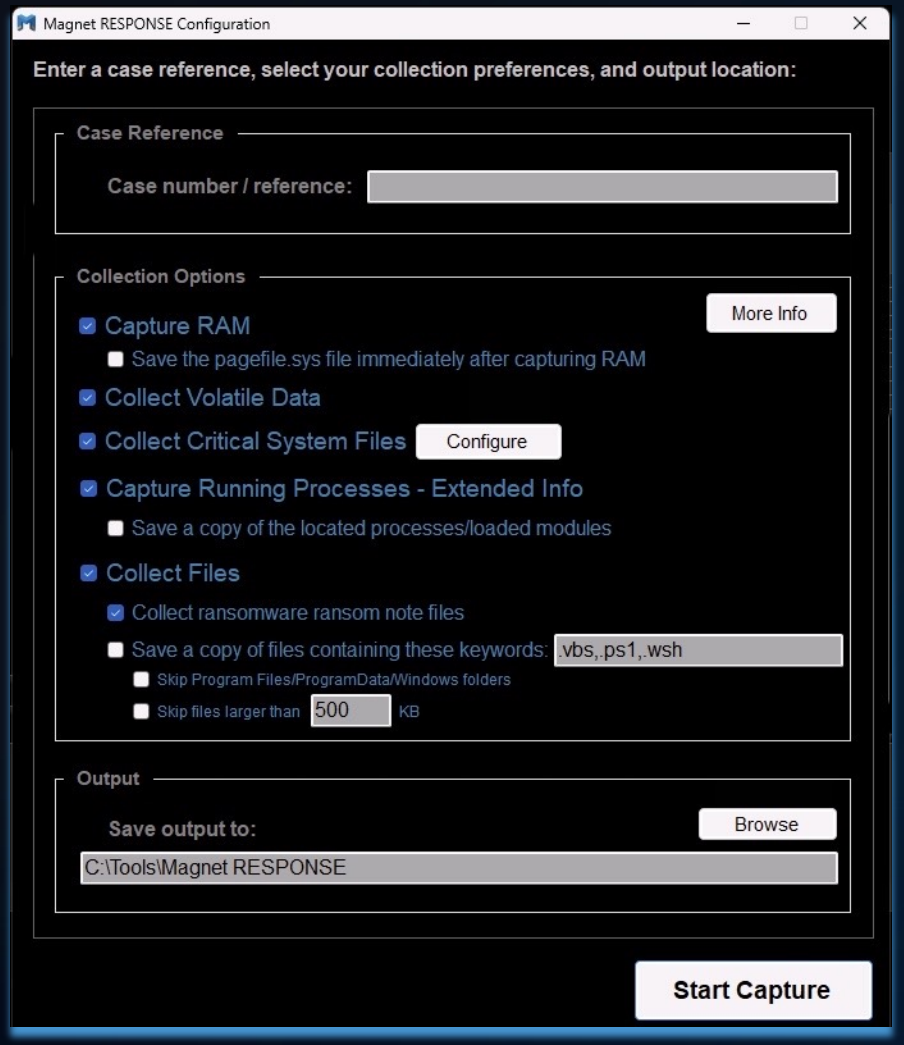
MAGNET RESPONSE



UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

MAGNET RESPONSE



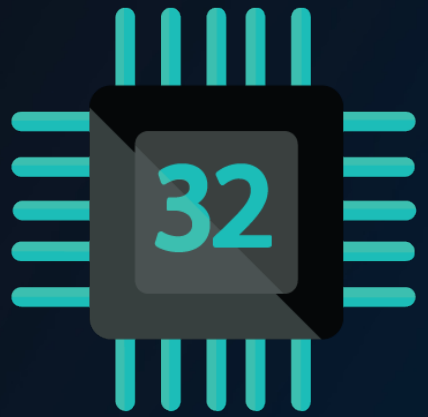
Magnet RESPONSE lets investigators and non-technical users easily collect and preserve critical data relevant to incident response investigations from local endpoints.

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

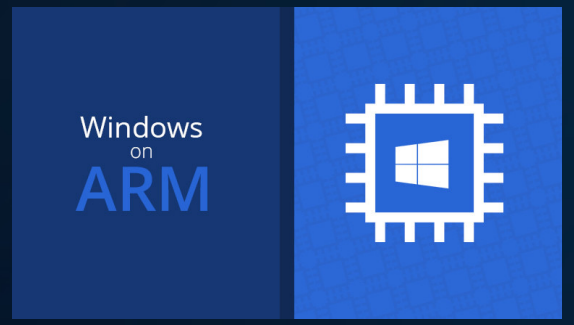
This makes Magnet RESPONSE useful in situations where non-technical users may need to collect and preserve data on behalf of law enforcement investigators as part of a cyber incident investigation.

MAGNET RESPONSE - RAM

Memory collection made easy

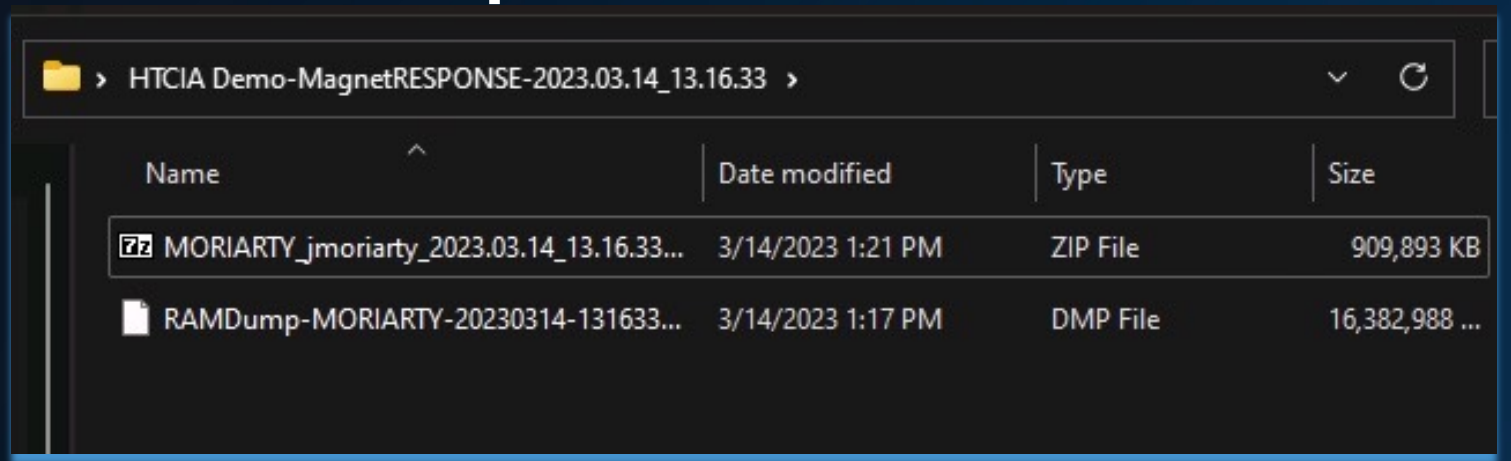


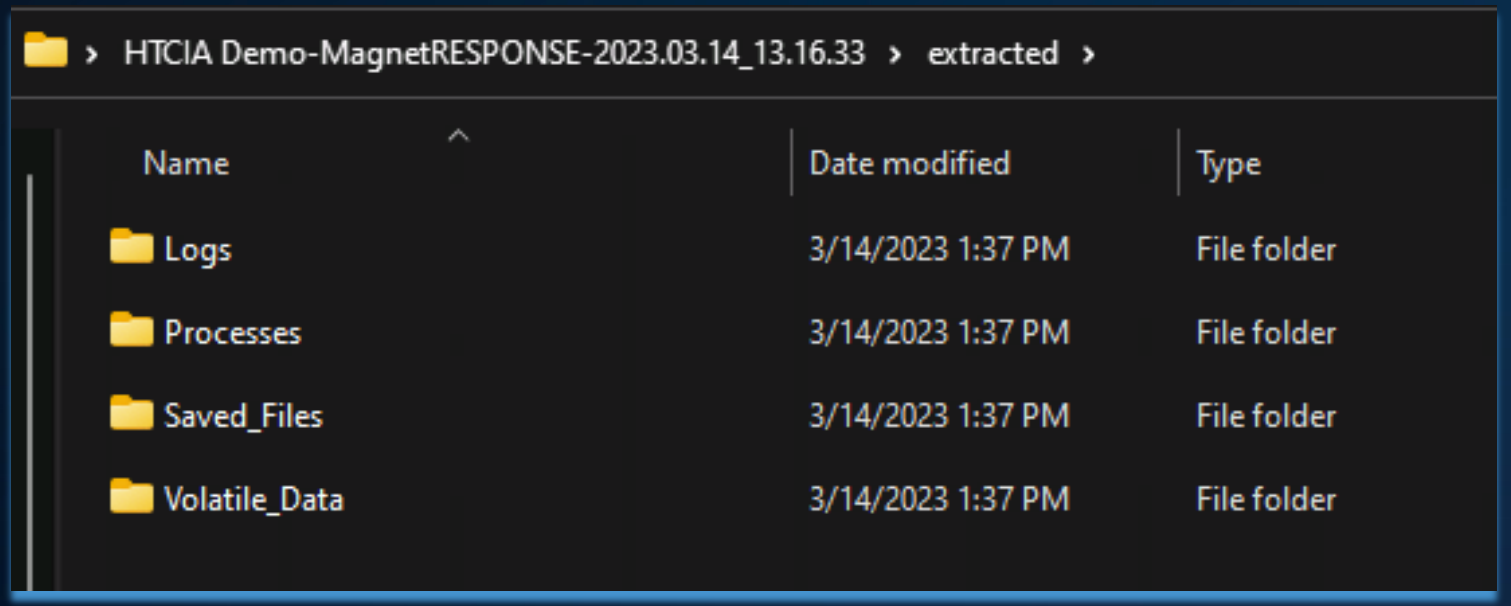
VS



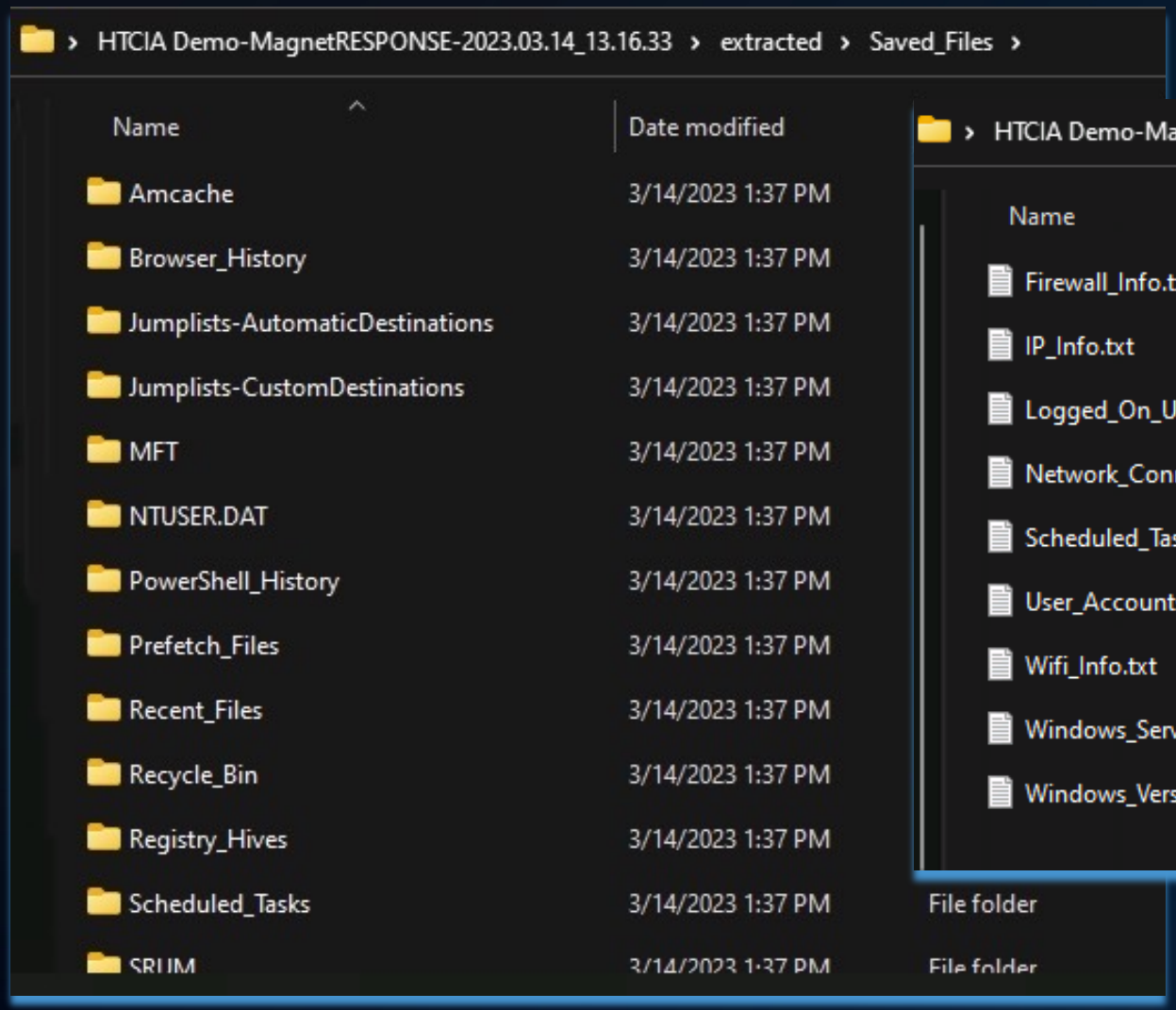
UNLOCK THE TRUTH. PROTECT THE INNOCENT.

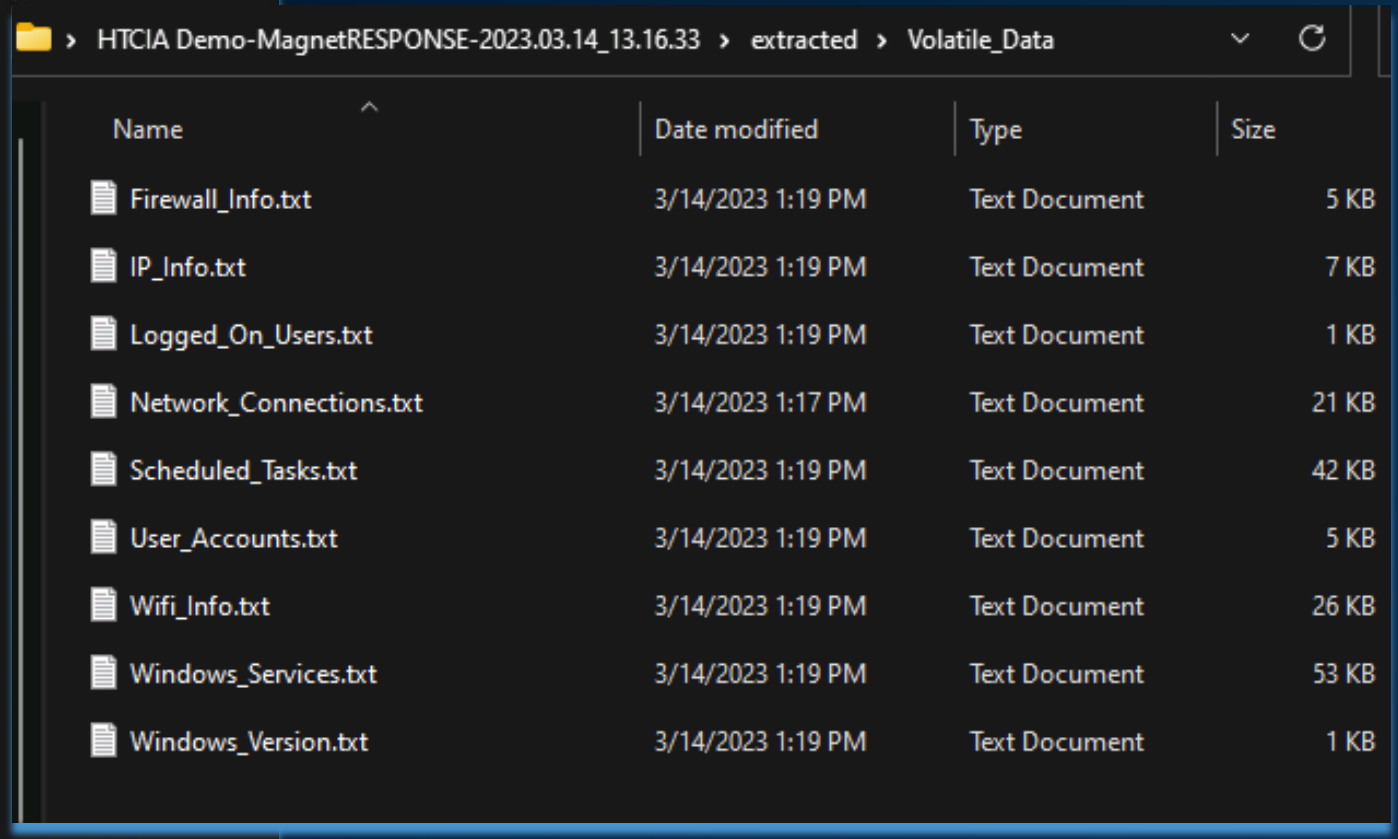
MAGNET RESPONSE Output





MAGNET RESPONSE Output





USB Capture

High capacity/speed USB drive

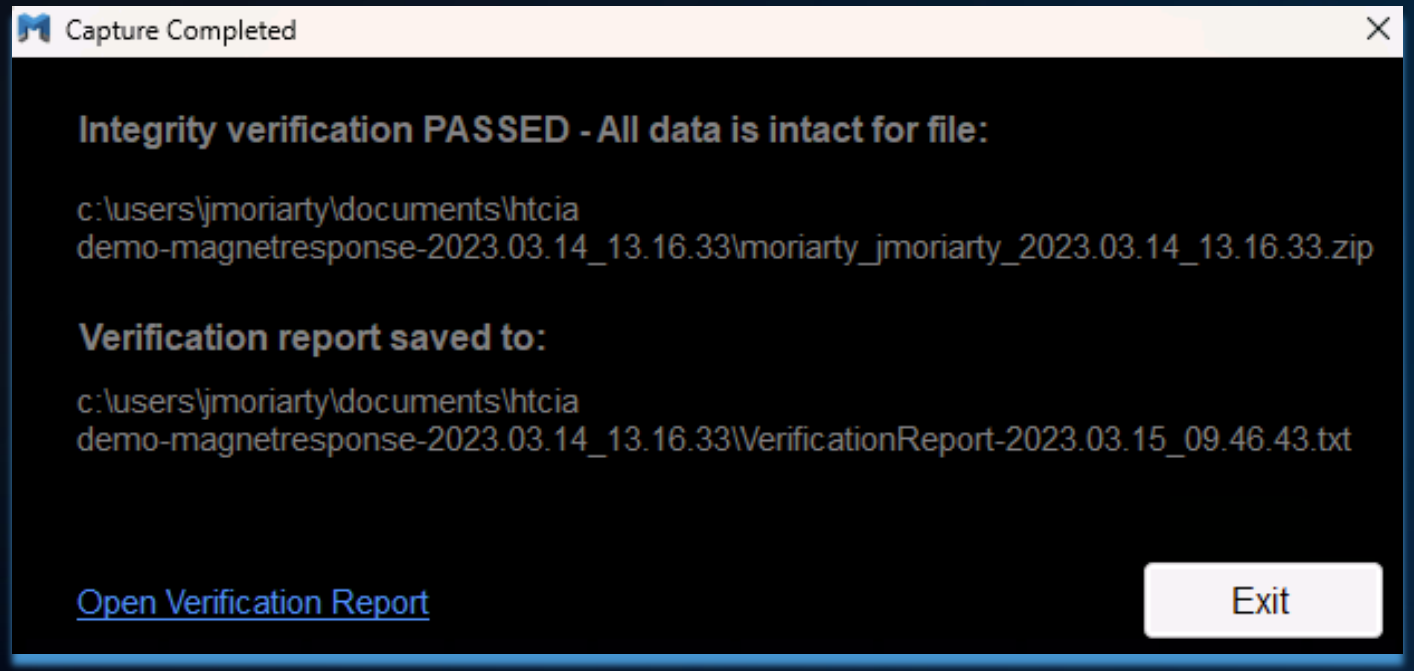
SSD or NVME

* 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)

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

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
/silent	- No GUI output to screen

MAGNET RESPONSE PowerShell

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

RESPONSE POWERSHELL OPERATIONS FLOW

Triggering Event

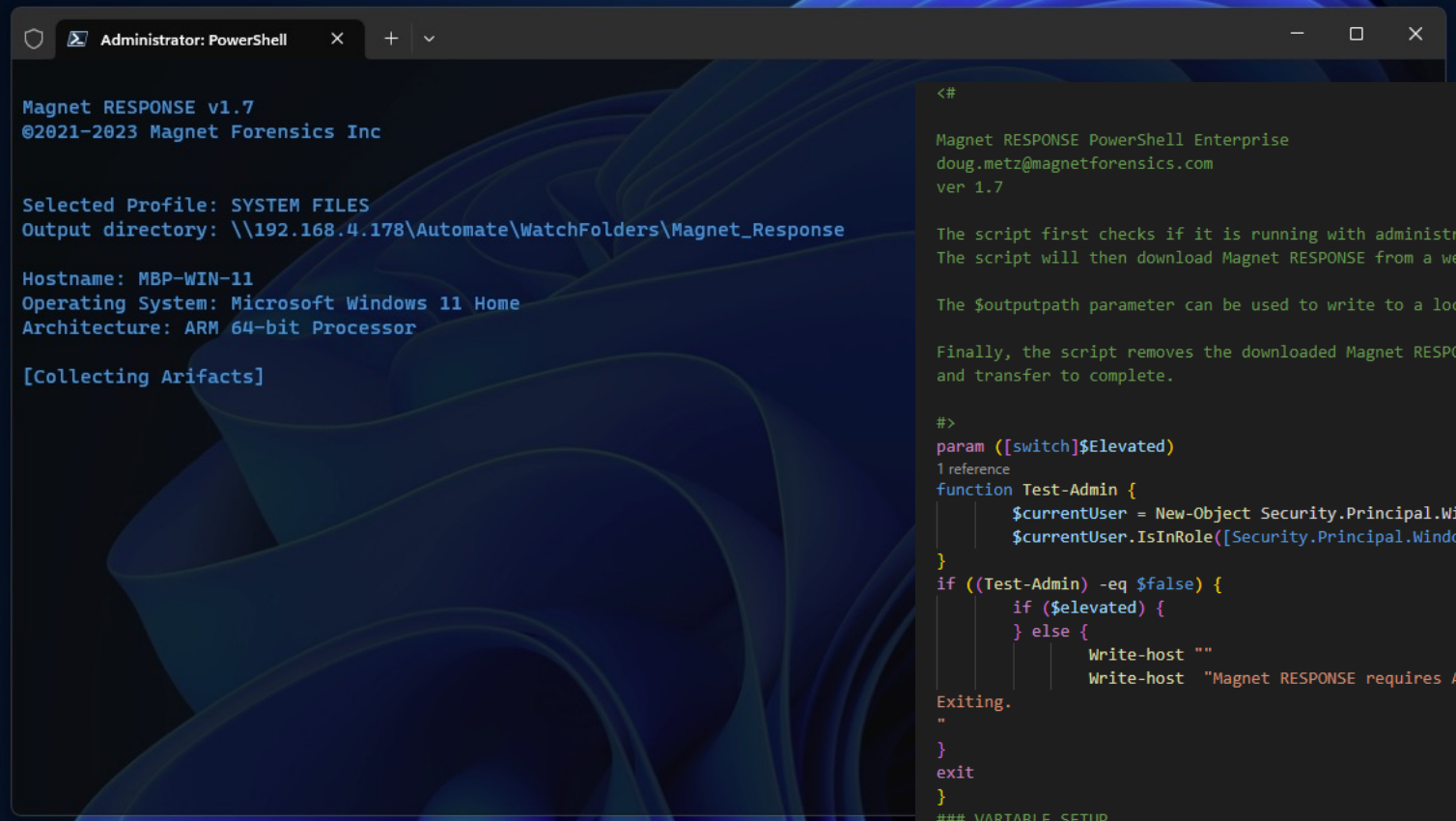
Script Executed on Endpoint

Endpoint retrieves MAGNETResponse.zip from Web server

Collection runs on endpoint per script parameters

Collection saved to Network share

MAGNET RESPONSE PowerShell




```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")
#######
```

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

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"
#>
#### Systen 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

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

MAGNET RESPONSE with Microsoft Defender for Endpoint

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

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*

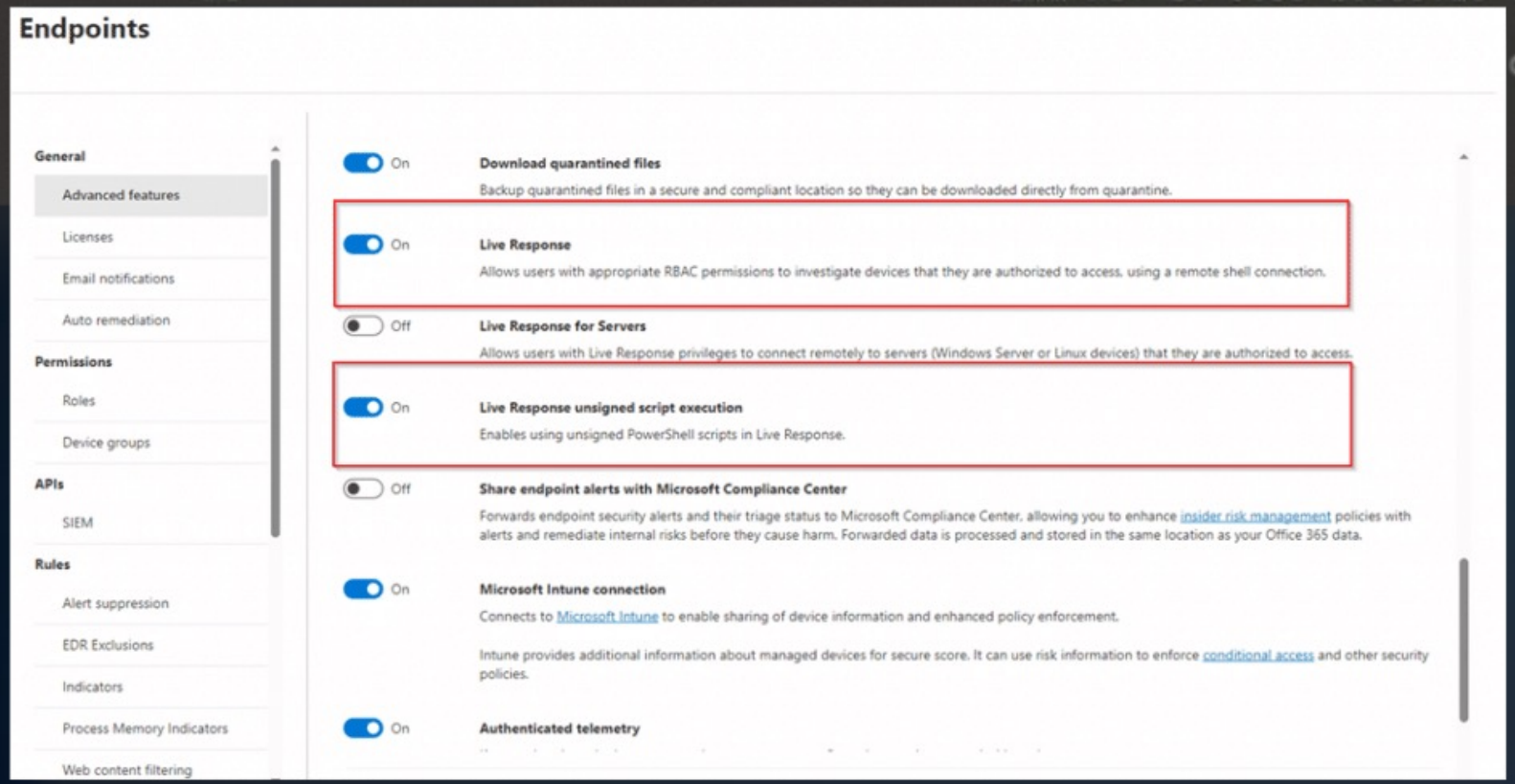
Local Collection downloaded to Examiner workstation

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

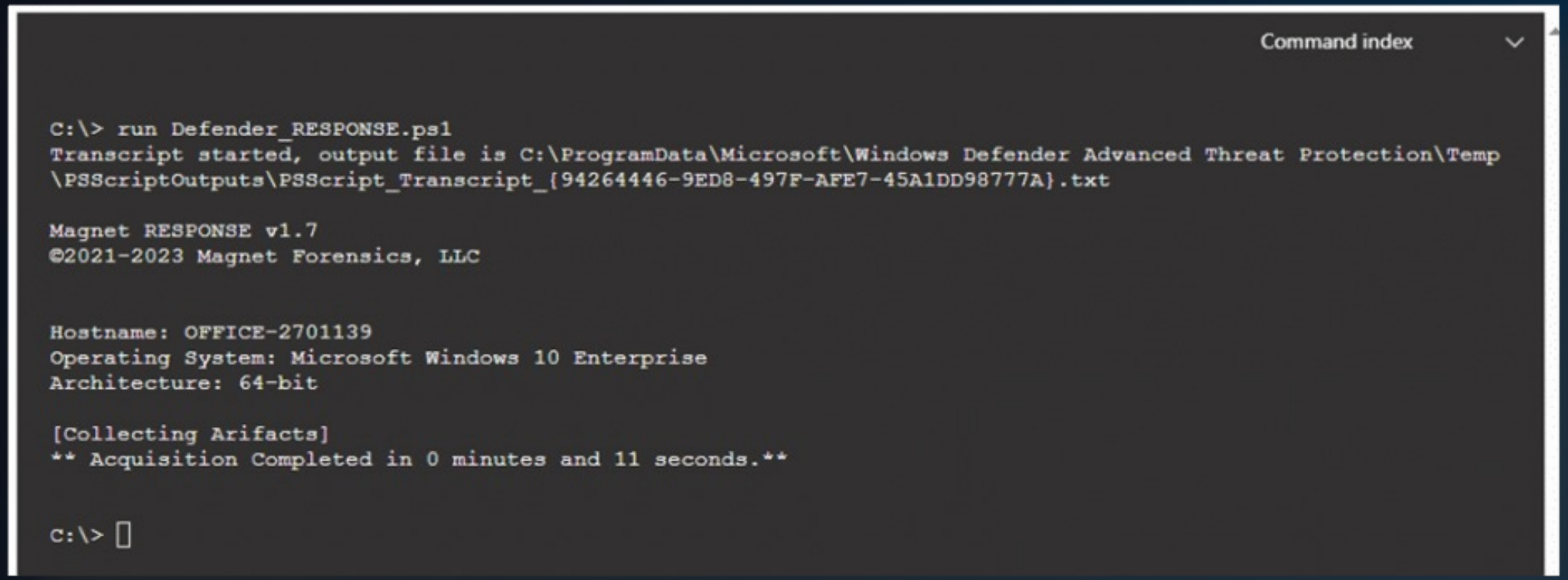
```
<#
.NOTES
Defender_RESPONSE.ps1
doug.metz@magnetforensics.com
v1.1

.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      Parameters description  Uploaded on
                                  Uploaded by
=======================  ==========  ==========  ============================  ================================
=================================  ==============================

Defender_RESPONSE.ps1                        No                                  Thu Nov 16 2023 10:59:23 GMT
-0500 (Eastern Standard Time)
MagnetRESPONSE.exe                                                                                           GMT
-0500 (Eastern Standard Time)
```



UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com



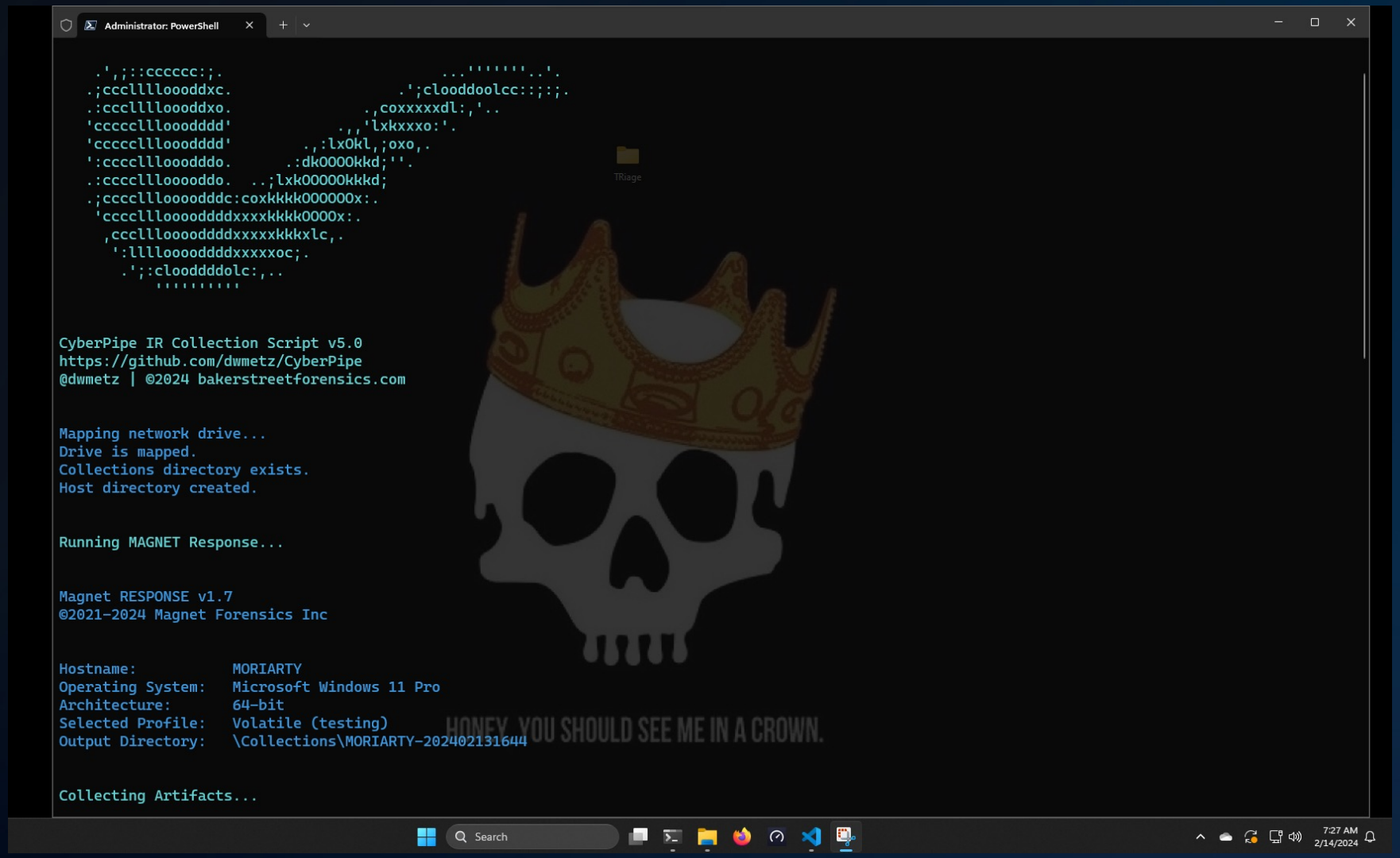
Retrieving the Data

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



UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

CYBERPIPE OPERATIONS FLOW

Triggering Event

Script Executed on Endpoint

Triage Collection+ saved to USB or

Triage Collection+ Saved to Network share

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

CYBERPIPE

Functions:

- 🐏 Capture a memory image with MAGNET DumpIt 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

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

Processing

MAGNET RESPONSE

Collections with

MAGNET AXIOM™ CYBER

magnetforensics.com

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

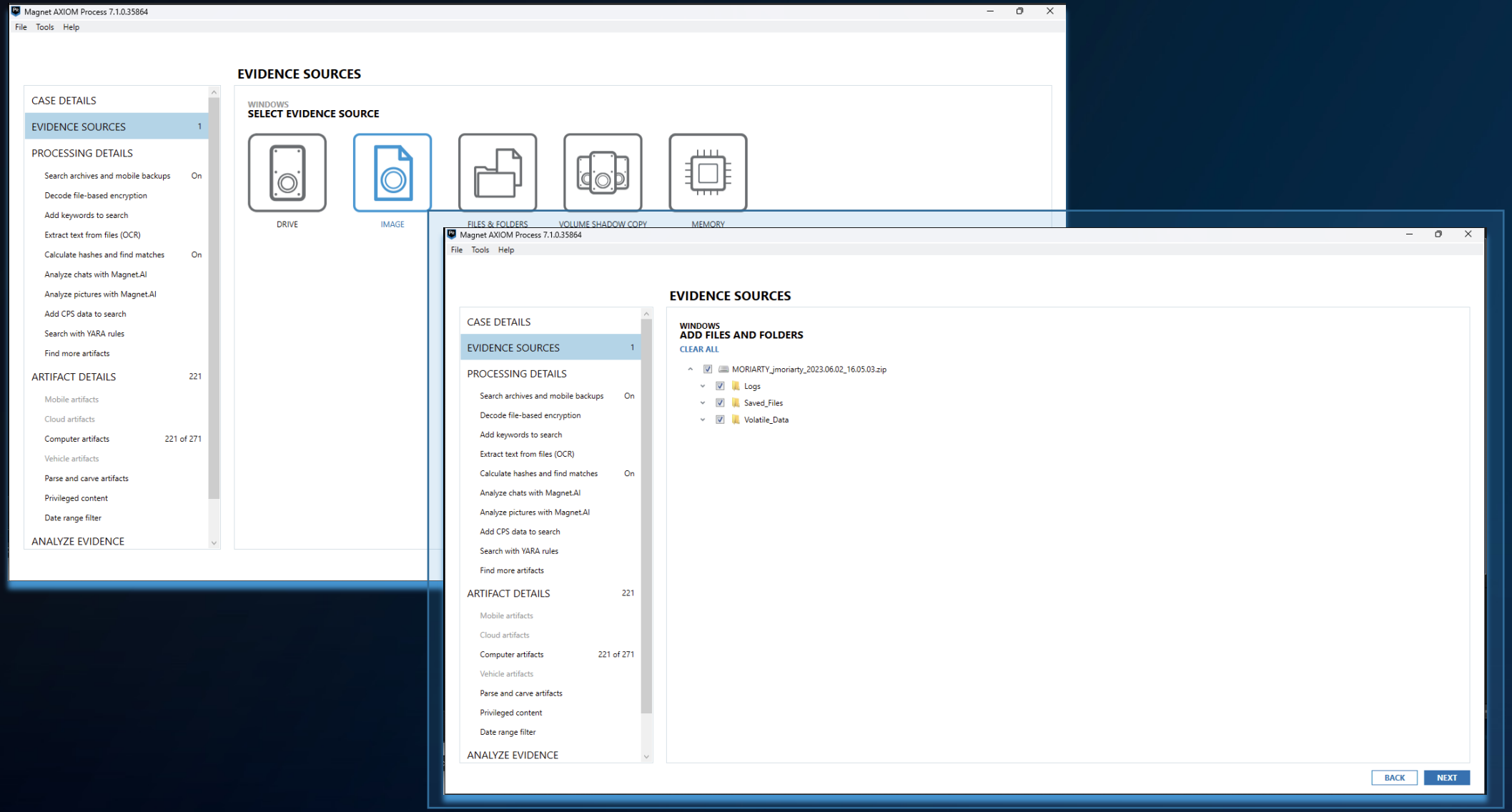
Request a free trial http://magnetforensics.com/magnet-axiom-cyber/

magnetforensics.com

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

Triage Processing

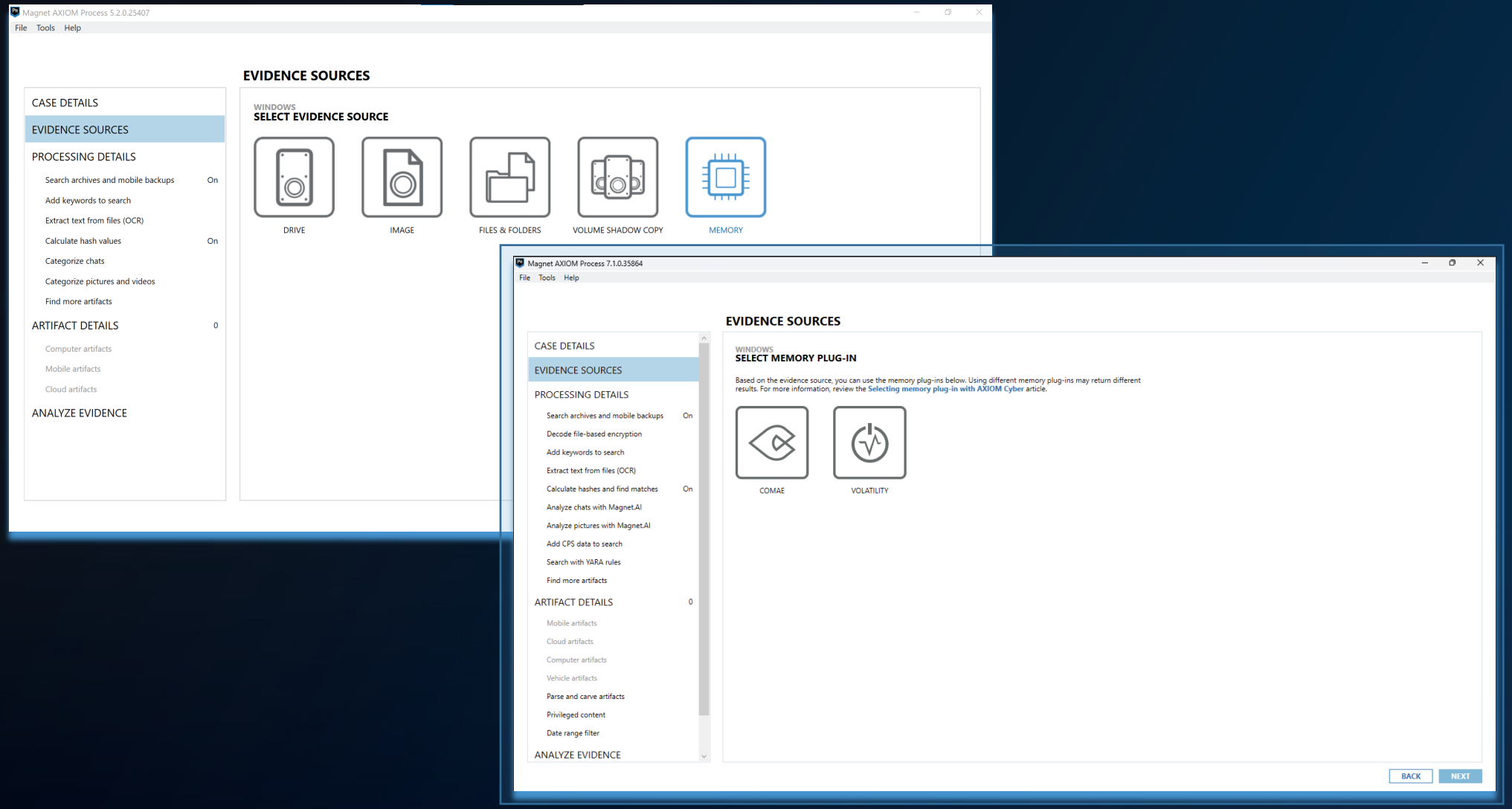
Computer > Windows > Load Evidence > IMAGE



UNLOCK THE TRUTH. PROTECT THE INNOCENT.

Comae Memory Processing

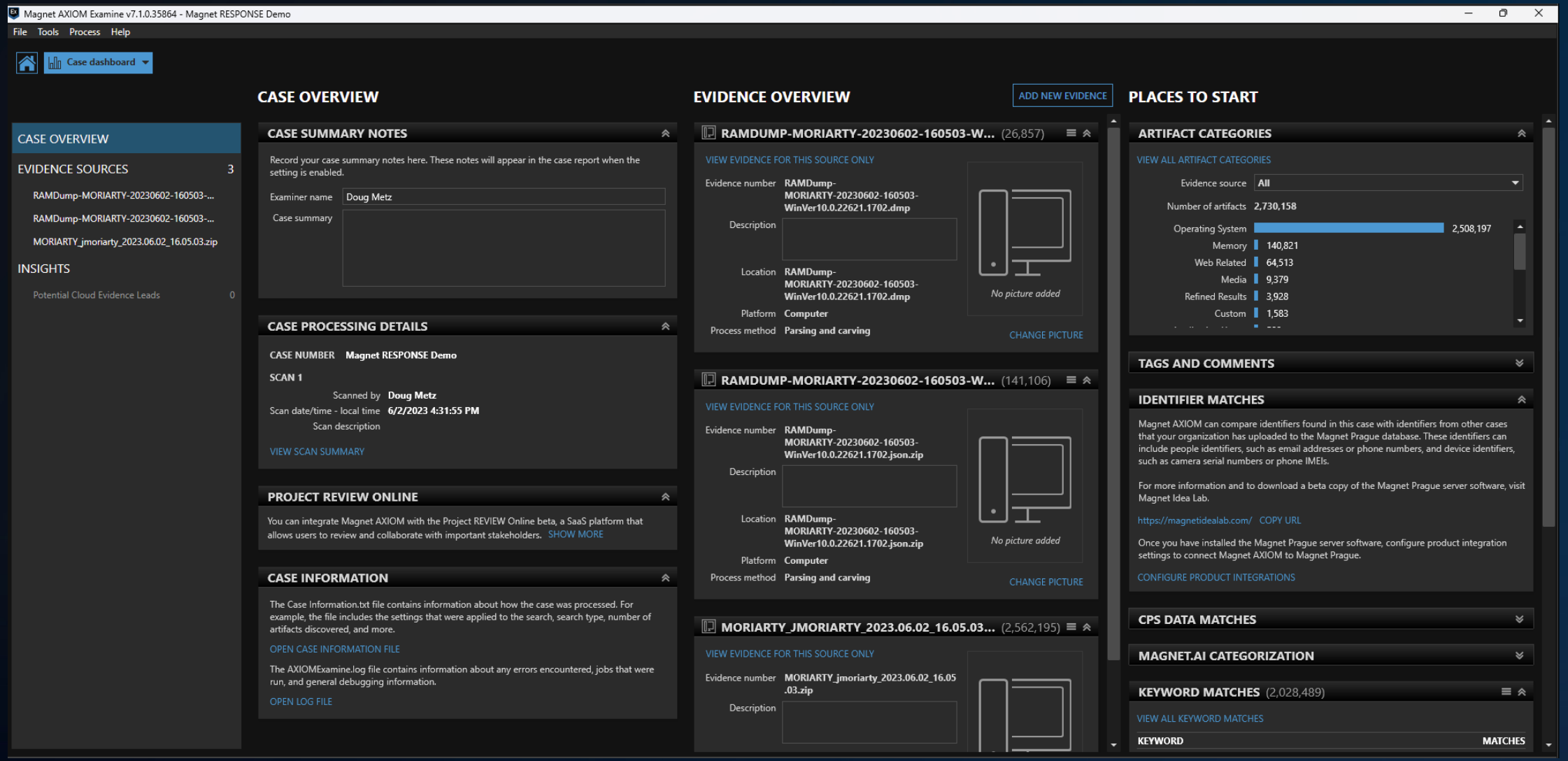
Computer > Windows > Load Evidence > MEMORY



UNLOCK THE TRUTH. PROTECT THE INNOCENT.

magnetforensics.com

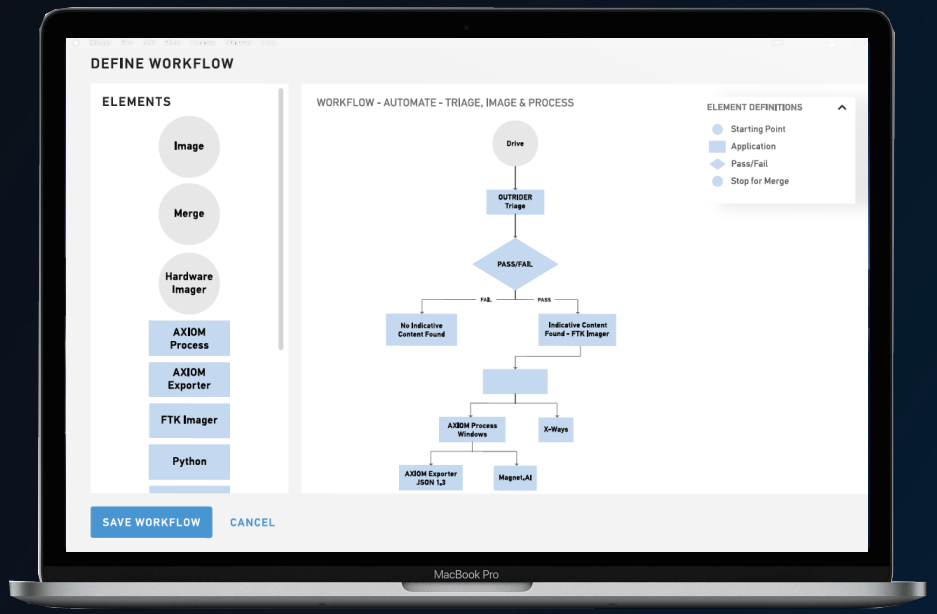
Artifacts from RESPONSE RAM & Triage



UNLOCK THE TRUTH. PROTECT THE INNOCENT.

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

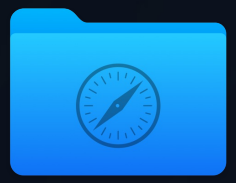
Faster Processing

Remote Collections

UNLOCK THE TRUTH. 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

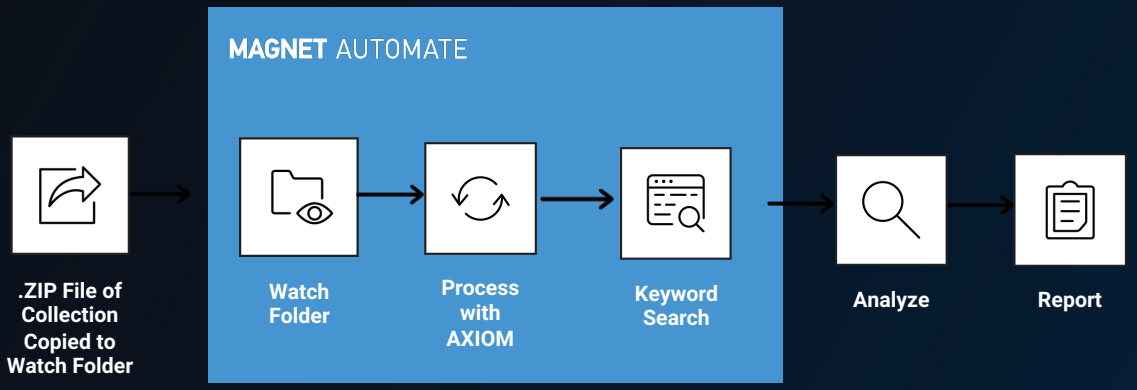
Evidence number variable

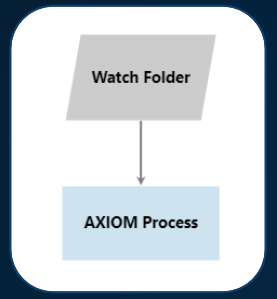
File name of forensic image RESET

CONTINUE

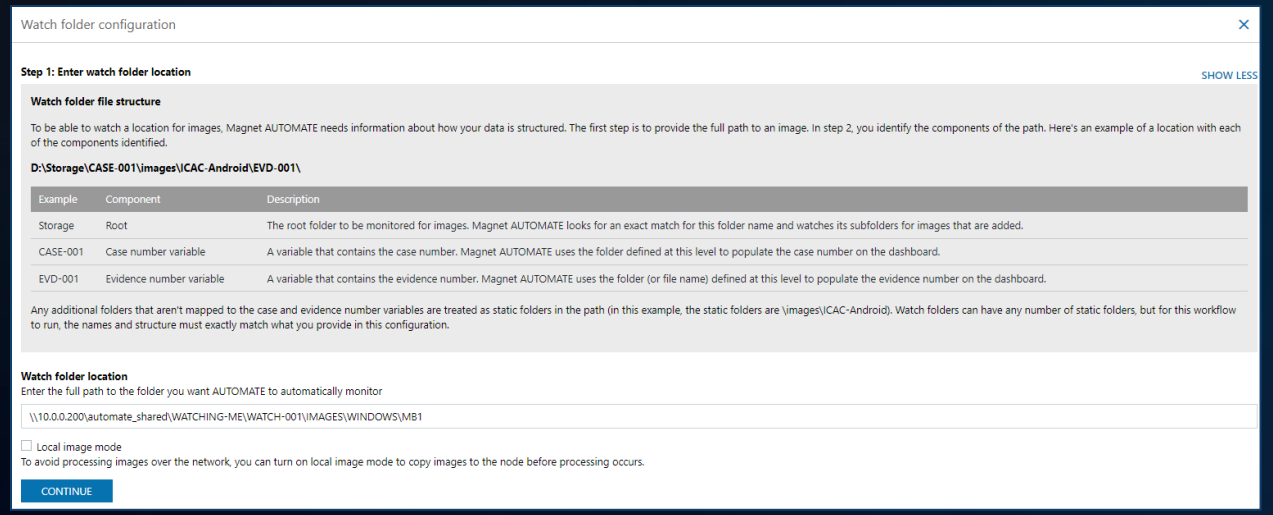
Automatic Forensic Processing

With a Watch Folder





Workflow Builder Example

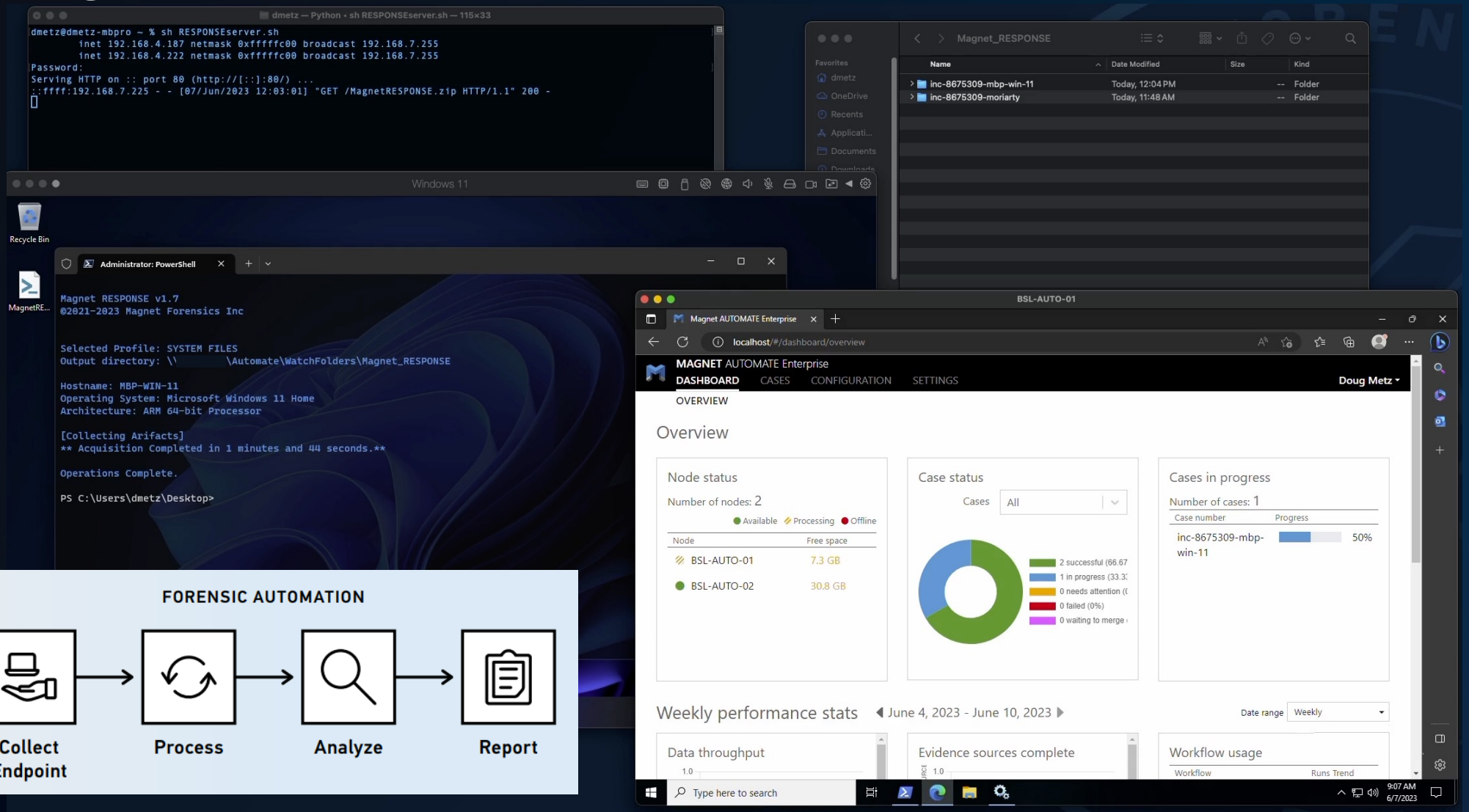


DFIR teams using AUTOMATE save time by reducing manual touchpoints and integrating their tech stack into automated workflows.

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

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

Triage Automation



Triage collection to processed case in < | = 1 click

magnetforensics.com

UNLOCK THE TRUTH. PROTECT THE INNOCENT.

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

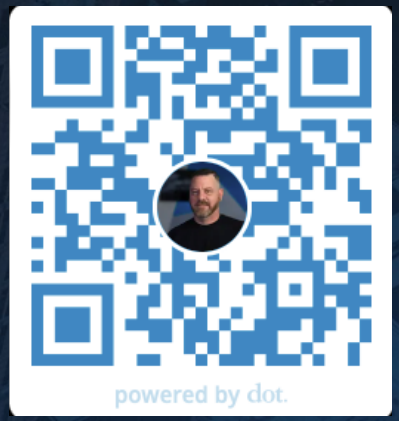
https://bakerstreetforensics.com

doug.metz@magnetforensics.com

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

https://infosec.exchange/@dwmetz

~~@dwmetz~~



UNLOCK THE TRUTH. PROTECT THE INNOCENT.