Time Is Not On Our Side:

Triage Collections in Incident Response Investigations

Doug Metz, Professional Services Consultant
Magnet Forensics

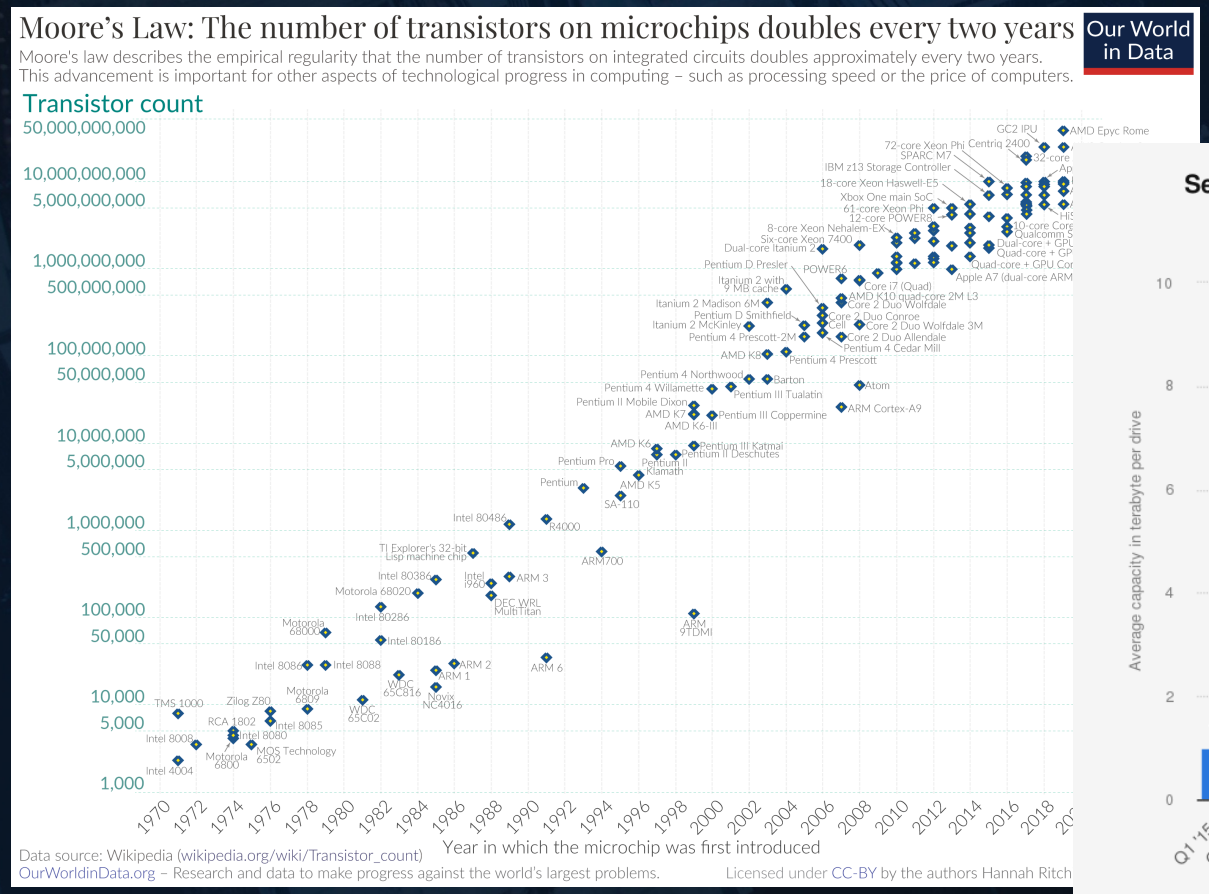
HTCIA Delaware Valley Chapter
1st Quarter Meeting
March 31, 2023

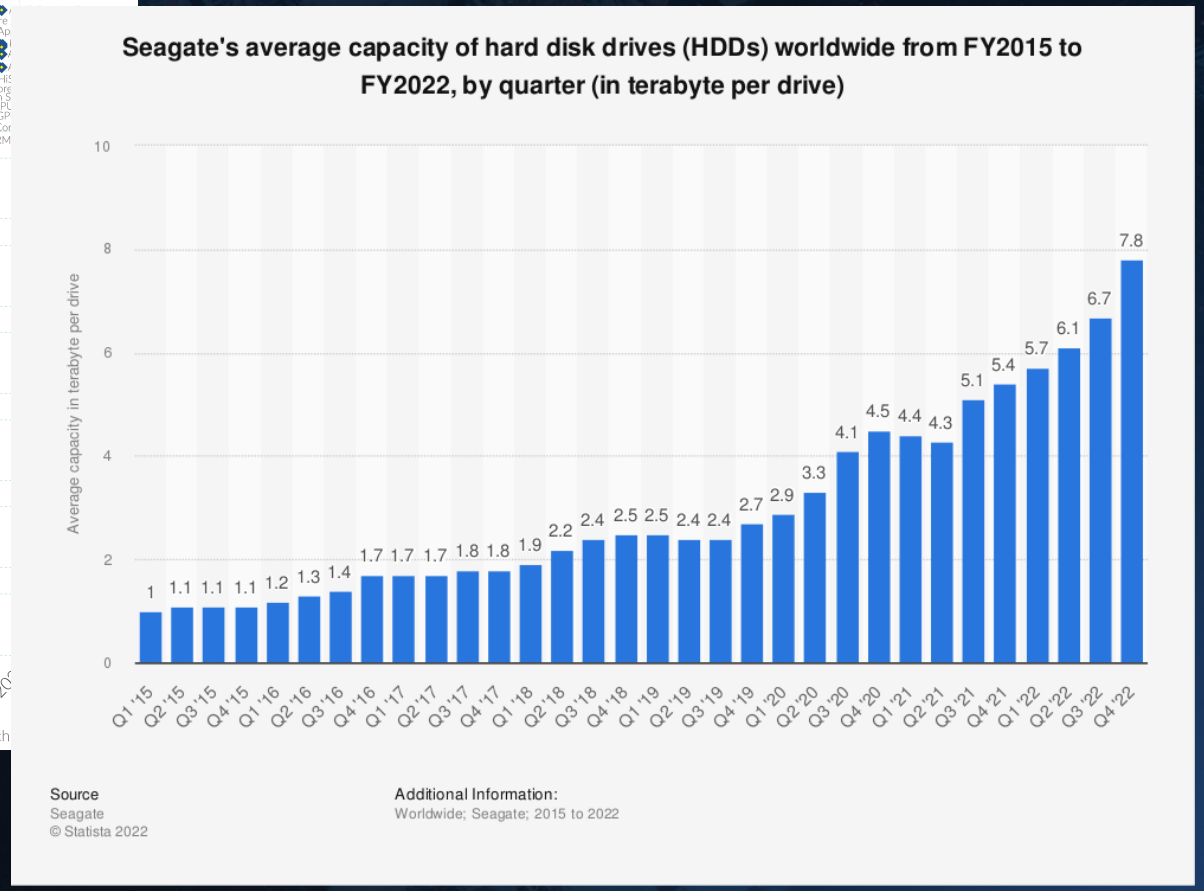
WHO AM I

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


Professional Services 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

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

SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNITUDES OF DATA





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

SEEK JUSTICE. PROTECT THE INNOCENT.

What If I told You

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

triage noun

tri·age trē-ˈäzh ˈtrē-ˌäzh

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

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

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

triage transitive verb

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

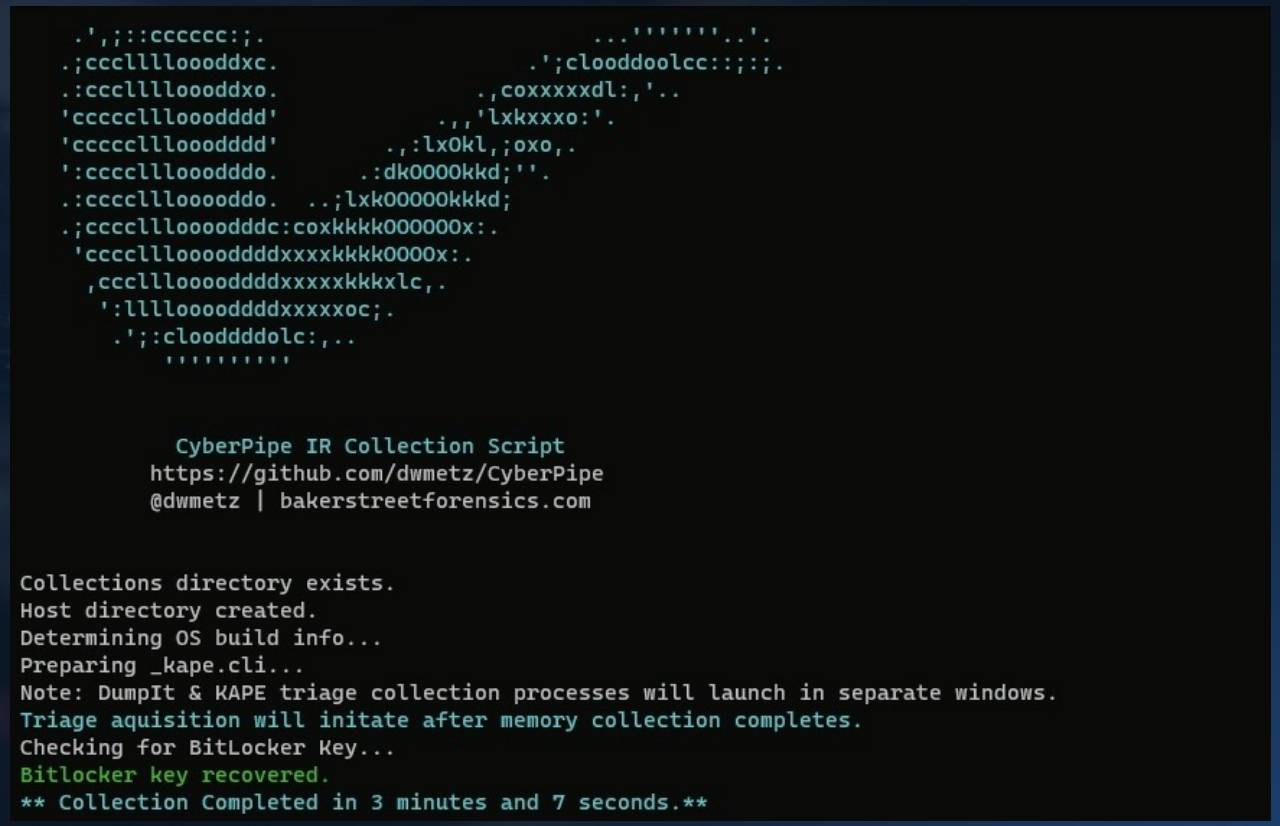
CyberPipe

An easy-to-use PowerShell script to collect memory and disk forensics for DFIR investigations.

Supports Windows: X64, x86, ARM

Functions:

- Capture a memory image with DumpIt for Windows,
- Capture a triage image with KAPE,
- Check for encrypted disks,
- Recover the active BitLocker Recovery key,
- Save all artifacts, output, and audit logs to USB or source network drive.



SEEK JUSTICE. PROTECT THE INNOCENT.

CyberPipe

v4.0 Features: “One Script to Rule them All”

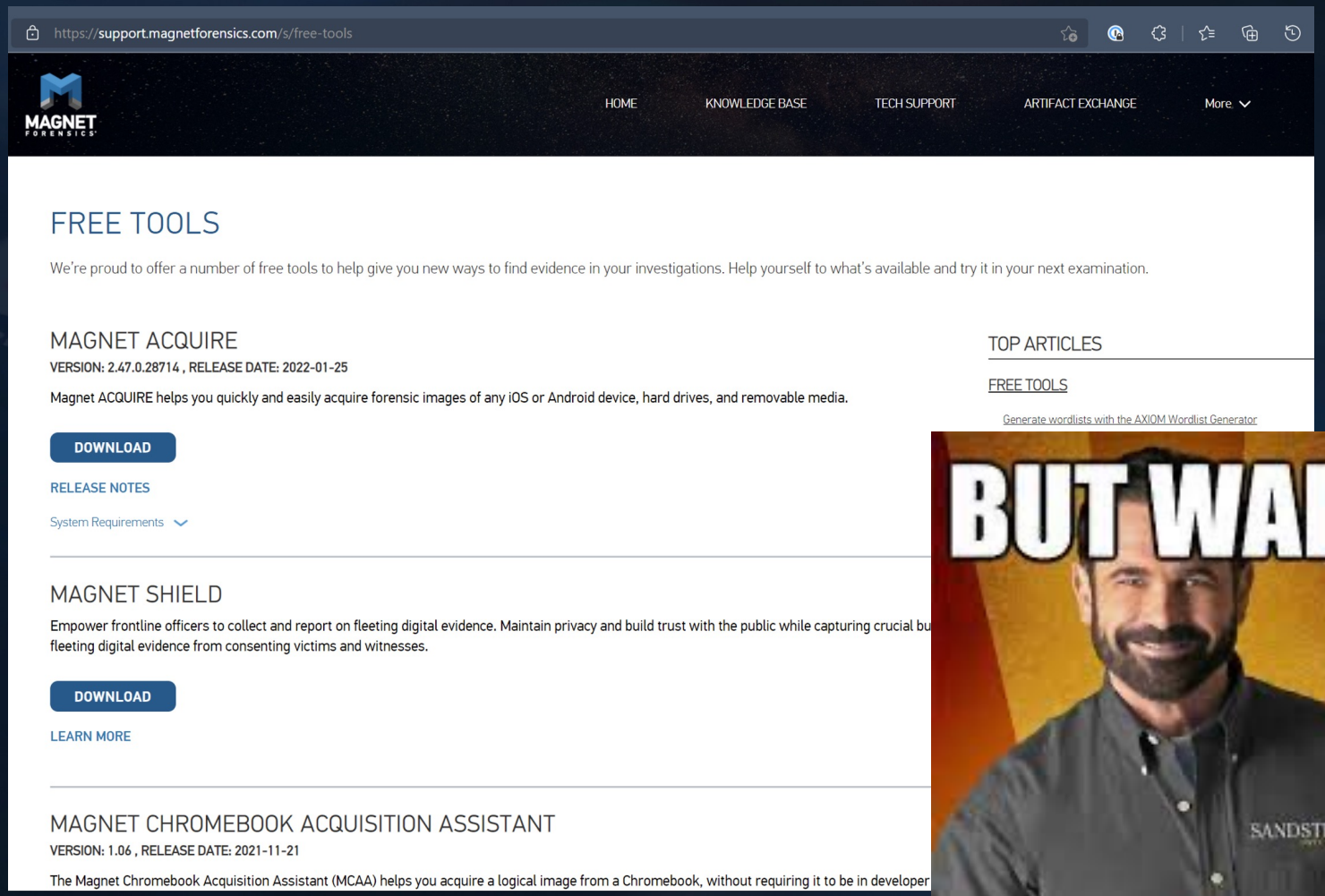
- Admin permissions check before execution.
- Memory acquisition will use Magnet DumpIt for Windows (previously used Magnet RAM Capture).
- Support for x64, ARM64 and x86 architectures.
- Both memory acquisition and triage collection now facilitated via KAPE batch mode with _kape.cli dynamically built during execution.
- Capture directories now named to $hostname-$timestamp to support multiple collections from the same asset without overwriting.
- Alert if Bitlocker key not detected. Both display and (empty) text file updated if encryption key not detected.
- If key is detected it is written to the output file.
- More efficient use of variables for output files rather than relying on renaming functions during operations.
- Now just one script for Network or USB usage. Uncomment the “Network Collection” section for network use.
- Stopwatch function will calculate the total runtime of the collection.
- ASCII art “Ceci n’est pas une pipe.”

```
      ':lllloooodddxxxxxoc;.
       .';:cloodddolc:,..
          ''''''''''
"
Write-Host -Fore Cyan "            CyberPipe IR Collection Script"
Write-Host -Fore Gray "          https://github.com/dwmetz/CyberPipe"
Write-Host -Fore Gray "          @dwmetz | bakerstreetforensics.com"
Write-Host ""
Write-Host ""
$stopwatch = [System.Diagnostics.Stopwatch]::StartNew()
## Network Collection - uncomment the section below for Network use
<#
Write-Host -Fore Gray "Mapping network drive..."
$Networkpath = "X:\"
If (Test-Path -Path $Networkpath) {
    Write-Host -Fore Gray "Drive Exists already."
}
Else {
    # map network drive
    (New-Object -ComObject WScript.Network).MapNetworkDrive("X:","\\Server\Triage")
    # check mapping again
    If (Test-Path -Path $Networkpath) {
        Write-Host -Fore Gray "Drive has been mapped."
    }
    Else {
        Write-Host -Fore Red "Error mapping drive."
    }
}
Set-Location X:
#>
## Below is for USB and Network:
$tstamp = (Get-Date -Format "_yyyyMMddHHmm")
$collection = $env:COMPUTERNAME+$tstamp
$wd = Get-Location
If (Test-Path -Path Collections) {
    Write-Host -Fore Gray "Collections directory exists."
}
Else {
```

SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNET FREE TOOLS

- Magnet DumpIt for Windows
- Encrypted Disk Detector (EDD)



MAGNET FORENSICS®

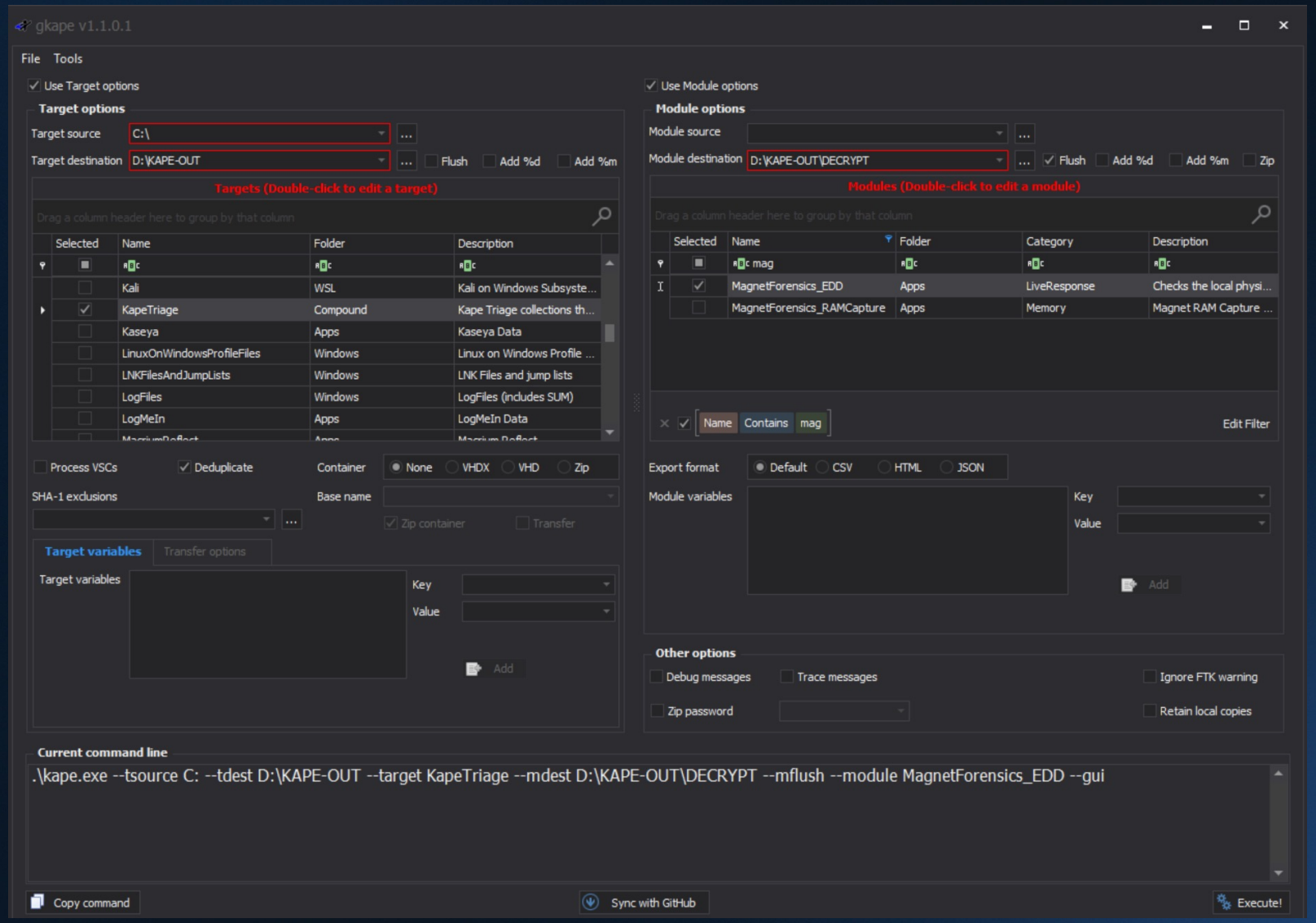
SEEK JUSTICE. PROTECT THE INNOCENT.

KAPE

Targets: categories of artifacts that can be collected (registry, event logs, browser activity…)

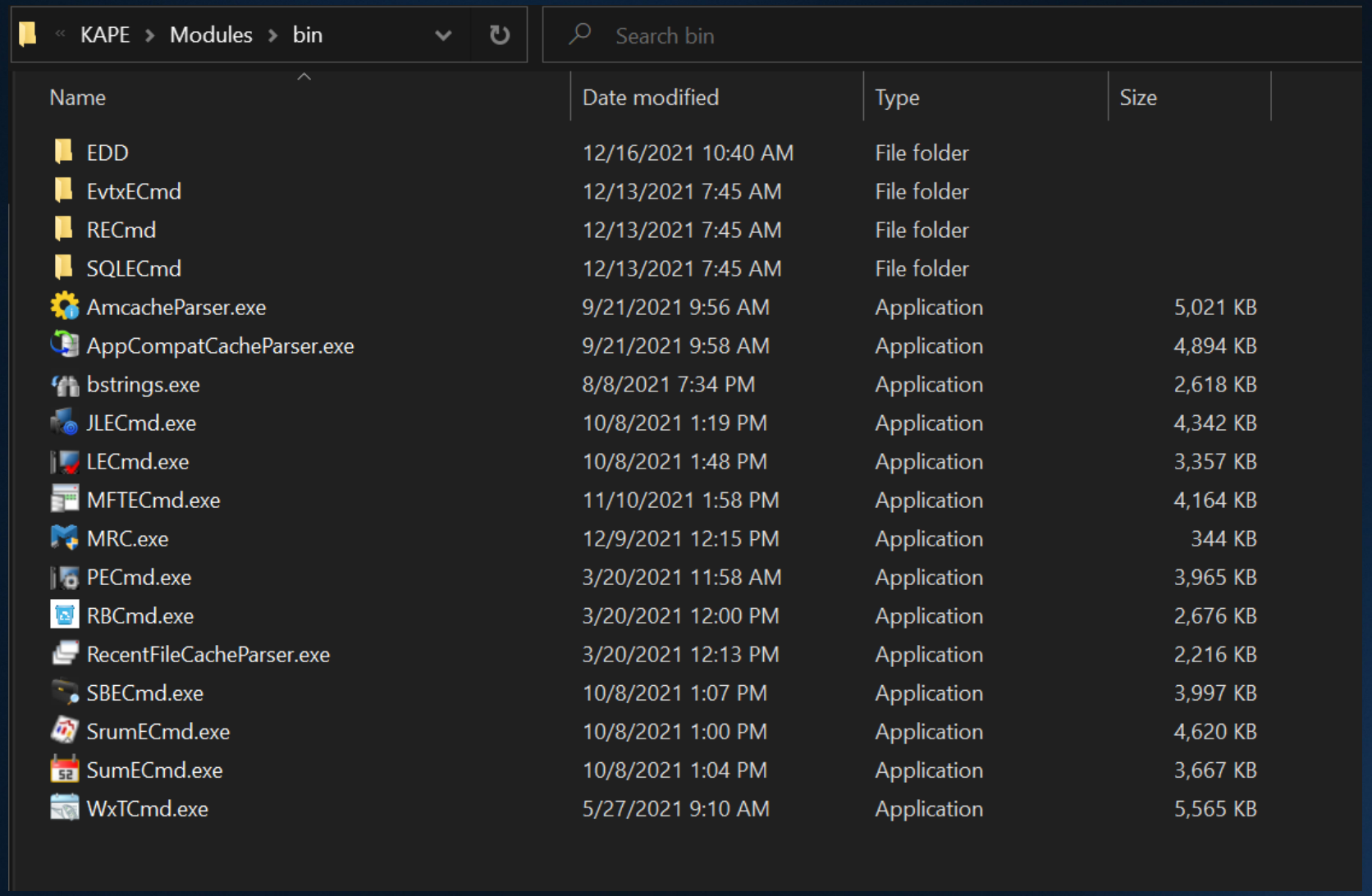
Modules: processing routines that can be run on what is collected (parse, convert to CSV, more) and run exe's.

GUI and Command Line



SEEK JUSTICE. PROTECT THE INNOCENT.

TOOLS IN THE /bin - BYOE



CHECK YOUR BINARIES

Editor: MagnetForensics_EDD

```
Description: Checks the local physical drives on a system for TrueCrypt, PGP, VeraCrypt, SafeBoot, or Bitlocker encrypted
volumes
Category: LiveResponse
Author: Mohamed El-Hadidi
Version: 1.1
Id: c7212da1-ed41-4560-95f7-1a2d99acc1f8
BinaryUrl: https://www.magnetforensics.com/resources/encrypted-disk-detector/
ExportFormat: txt
Processors:
    -
      Executable: EDD\EDDv310.exe
      CommandLine: /batch >> %destinationDirectory%
      ExportFormat: txt
      ExportFile: EDD.txt

# Documentation
# https://www.magnetforensics.com/resources/encrypted-disk-detector/
# Create a folder "EDD" within the "Modules\bin" KAPE folder
# Place "EDDv310.exe", "EDDv310.exe.config" files into "Modules\bin\EDD"
```

Reload | Generate GUID

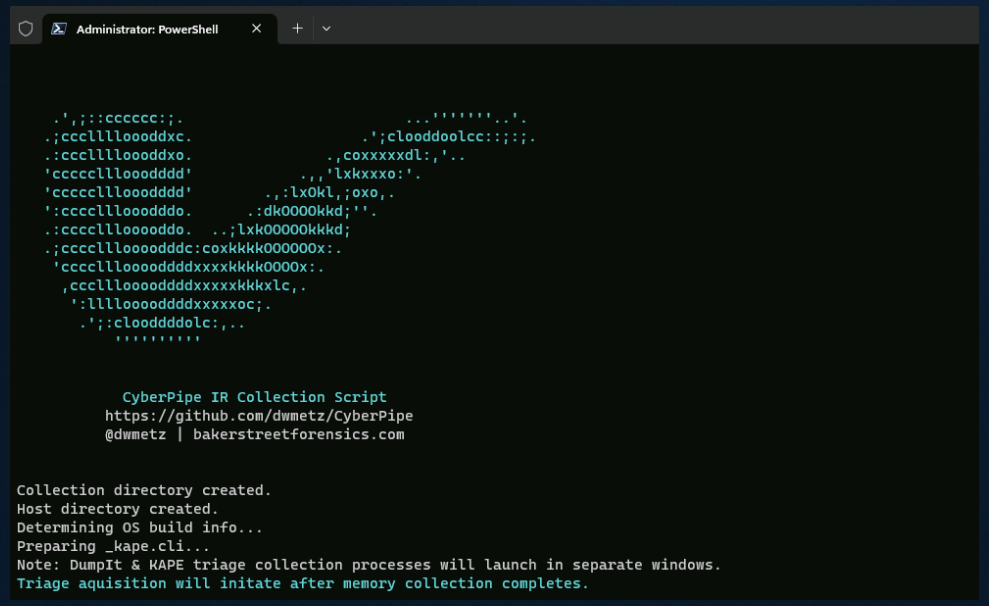
KAPE › Modules › Apps

Search Apps

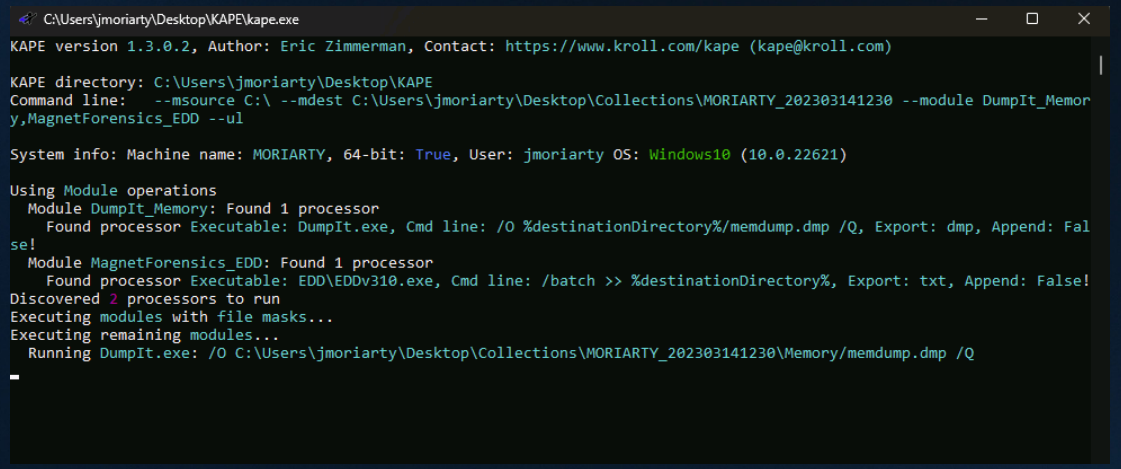
Name	Date modified	Type	Size
GitHub	12/13/2021 7:45 AM	File folder	
LogParser	12/13/2021 7:45 AM	File folder	
NirSoft	12/13/2021 7:45 AM	File folder	
SOFELK	12/13/2021 7:45 AM	File folder	
SysInternals	12/13/2021 7:45 AM	File folder	
TZWorks	12/13/2021 7:45 AM	File folder	
CrowdStrike_CrowdResponse.mkape	12/17/2021 9:41 AM	MKAPE File	2 KB
DensityScout.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
DumpIt_Memory.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
Everything_ParseEFU.mkape	12/17/2021 9:41 AM	MKAPE File	2 KB
ExifTool.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
KAPE_Automation.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
Kaspersky_TDSSKiller.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
MagnetForensics_EDD.mkape	2/8/2022 2:46 PM	MKAPE File	1 KB
NTFSLogTracker_$J.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
NTFSLogTracker_$LogFile.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
PowerShell_5SecondPause.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
Snap2HTML.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
SQLite3_TeraCopy_History.mkape	12/17/2021 9:41 AM	MKAPE File	2 KB
SQLite3_TeraCopy_Main.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
Thor-Lite_IOCScanner.mkape	12/17/2021 9:41 AM	MKAPE File	2 KB

SEEK JUSTICE. PROTECT THE INNOCENT.

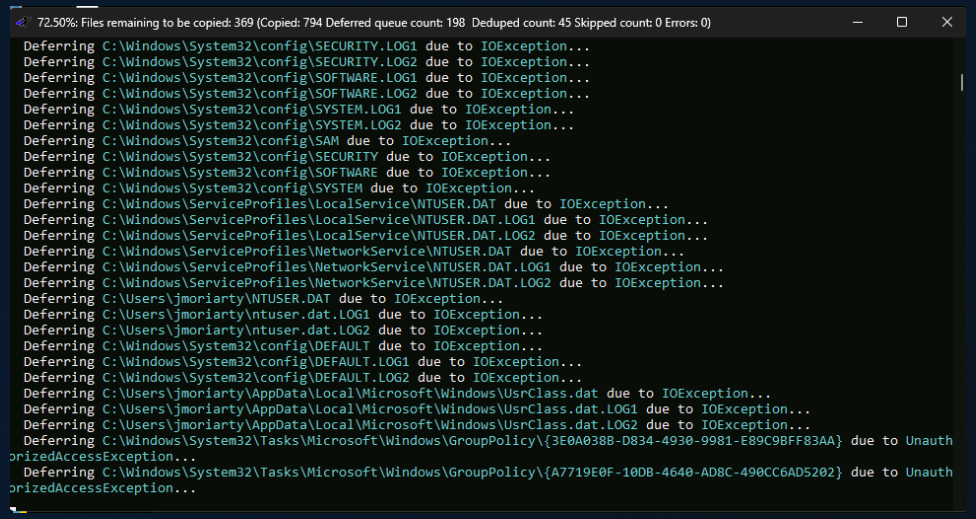
CyberPipe Operations



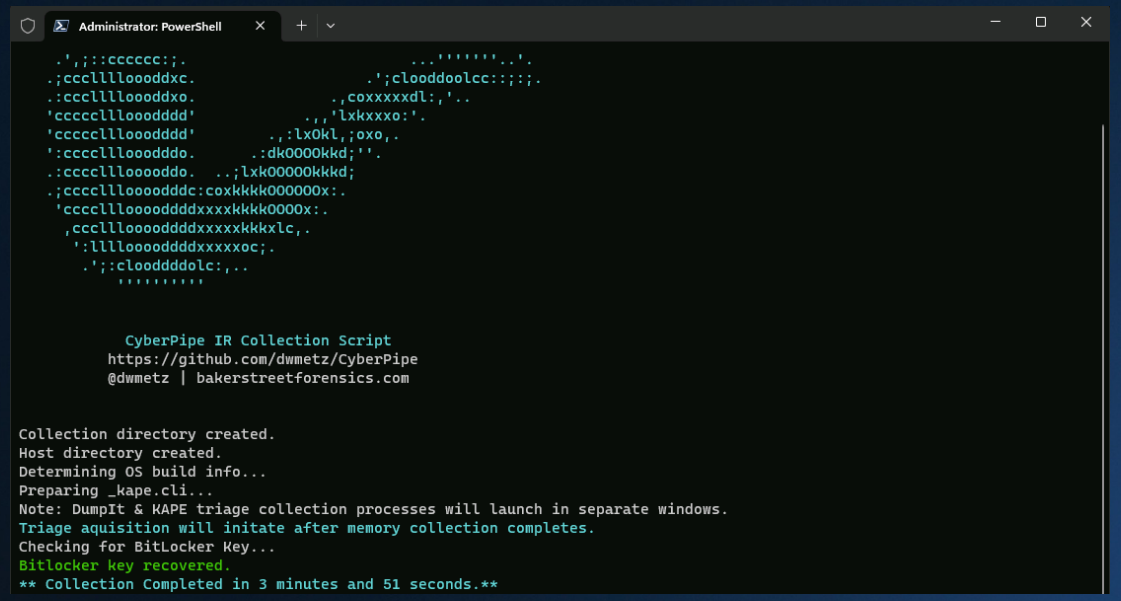
1. Script launch



2. (new window) Memory Collection



3. (2nd new window) Triage Collection



4. Clean-up and Complete

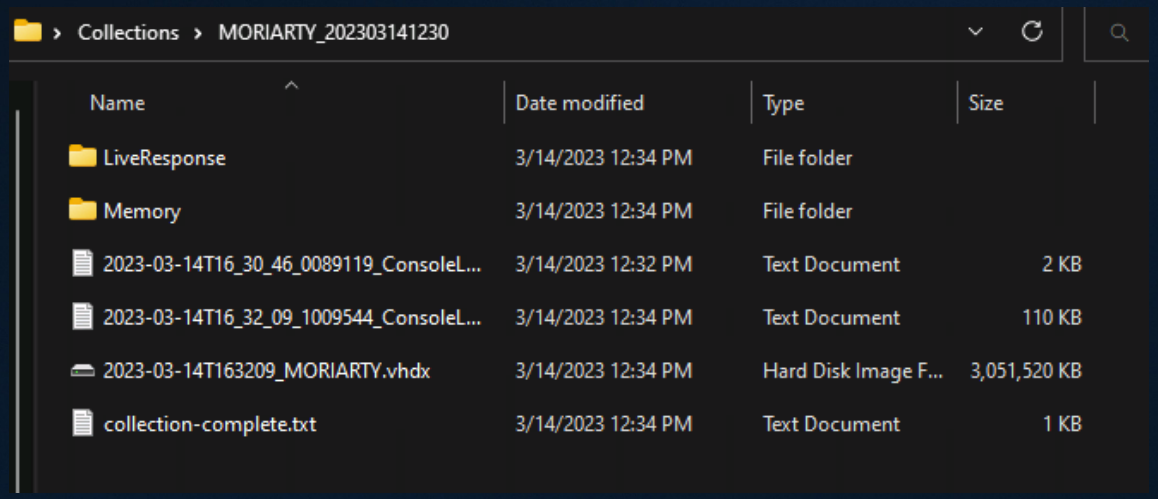
SEEK JUSTICE. PROTECT THE INNOCENT.

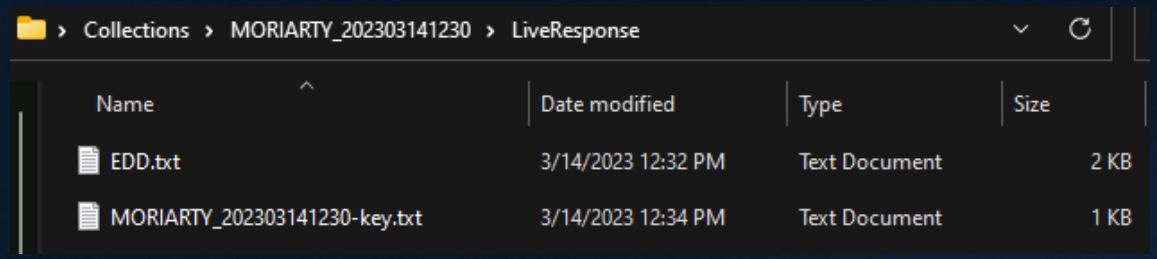
magnetforensics.com

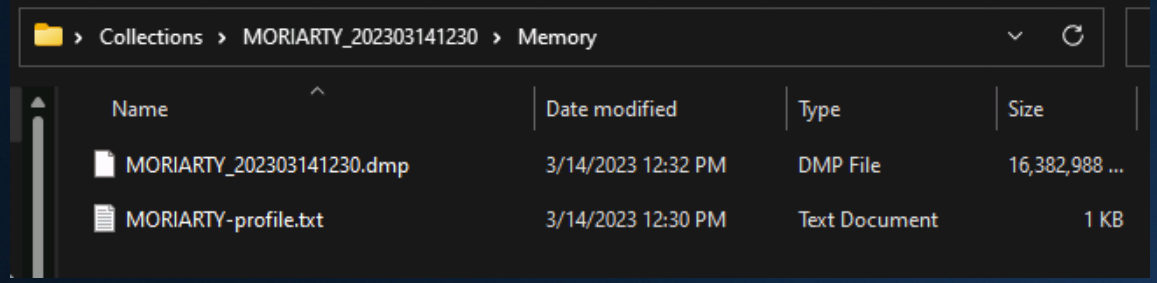
CyberPipe Demo

SEEK JUSTICE. PROTECT THE INNOCENT.

CyberPipe Output

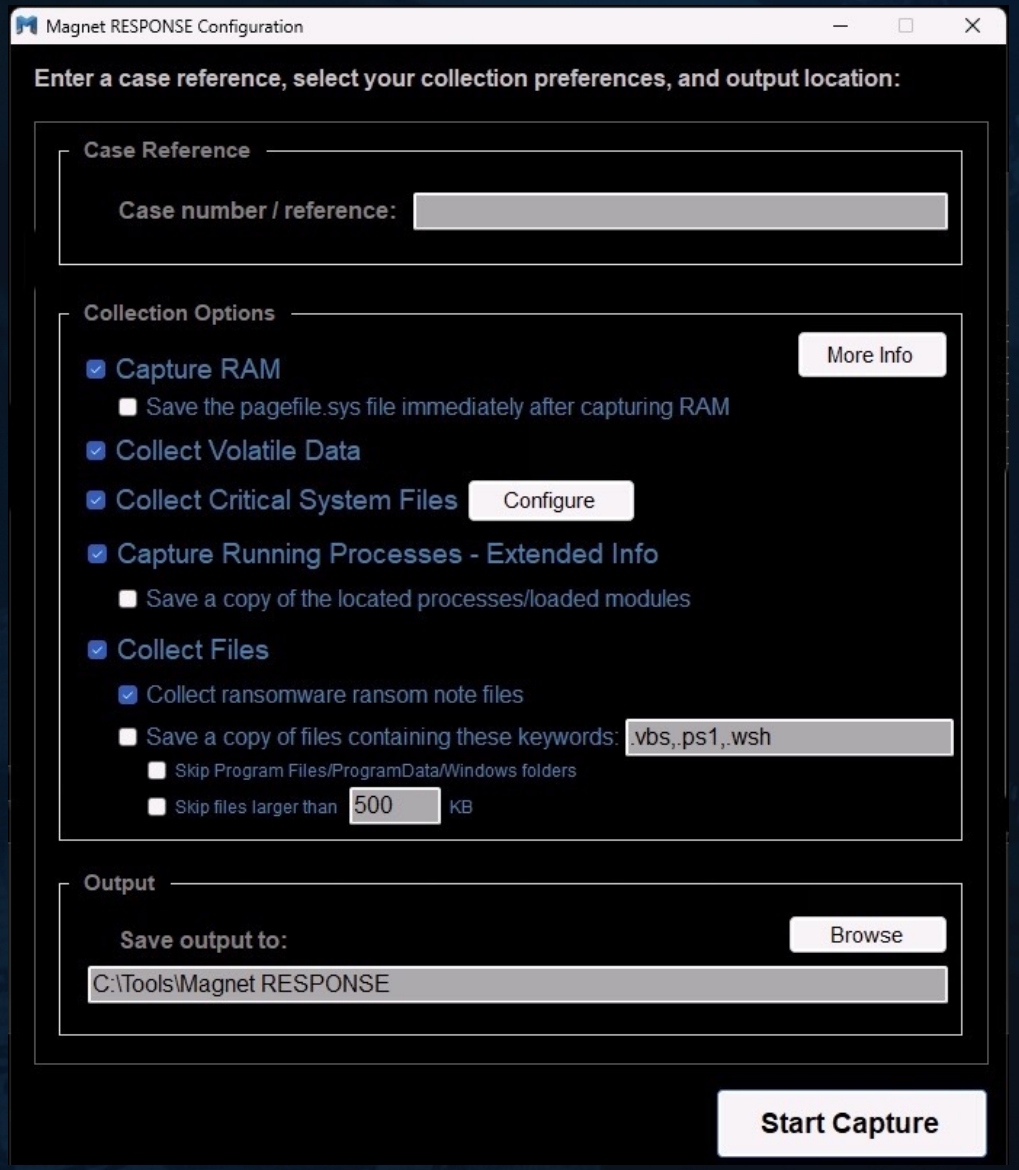






SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet RESPONSE



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

Magnet RESPONSE is a free and easy-to-use solution to quickly collect and preserve data from local endpoints before it is potentially modified or lost. A pre-set collection profile lets you target a comprehensive set of files and data relevant to incident response investigations, including RAM.

Minimal to no training is required—it's as simple as running it on the endpoint, configuring the collection and clicking "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

Key Benefits & Features:

•Easy-To-Use: A guided two-step process and progress bar is straightforward for even non-technical users to use

•Fast & Comprehensive: Collect and preserve data starting with the most volatile using the built-in Comae RAM capture (MAGNET DumpIt) functionality, and volatile data and files commonly associated to cybercrime, such as Windows Event Logs, Registry Hives, Jumplist files, and many other log files in minutes – no need for multiple tools to get the IR data you need

•Portable: It is compromised of a single executable file (less than 1MB), is easily downloaded, and can be stored and run from a USB key

•Collect by Keyword & Skip Large Files: configure free-form collections using your own set of keywords (or the defaults provided), with the option to limit the size of files collected to maintain speed

•Consolidated Output: Output is consolidated and saved as a .zip file for easy delivery or processing and analysis in Magnet AXIOM & Magnet AXIOM Cyber

•Data Integrity: An embedded hash value is provided to verify the integrity of the data

Magnet RESPONSE

Auto-collect Options

These options can be useful if you are providing the tool to a non-technical operator to simply capture the data and bring it back to you for processing/analysis.

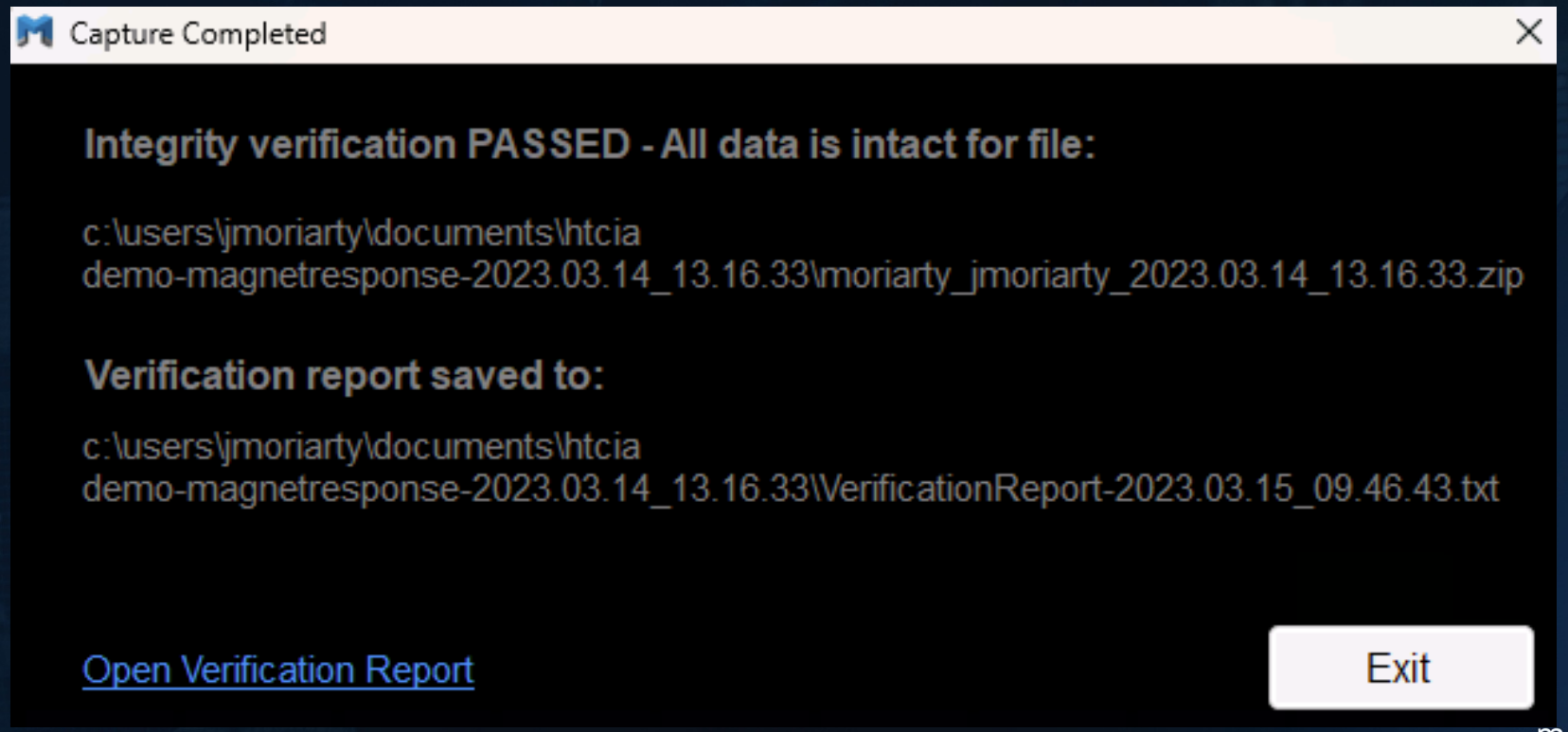
•Option 1 - Capture Everything Rename the executable to have the text "AutoCapture" (no quotes) anywhere in the filename. All options will be enabled, and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs from.

•Option 2 - Minimal Capture Rename the executable to have the text "AutoCaptureMinimal" (no quotes) anywhere in the filename. Only the "Volatile Data" and "Critical System Files" options will be enabled (no extended info saved for running processes), and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs from.

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.

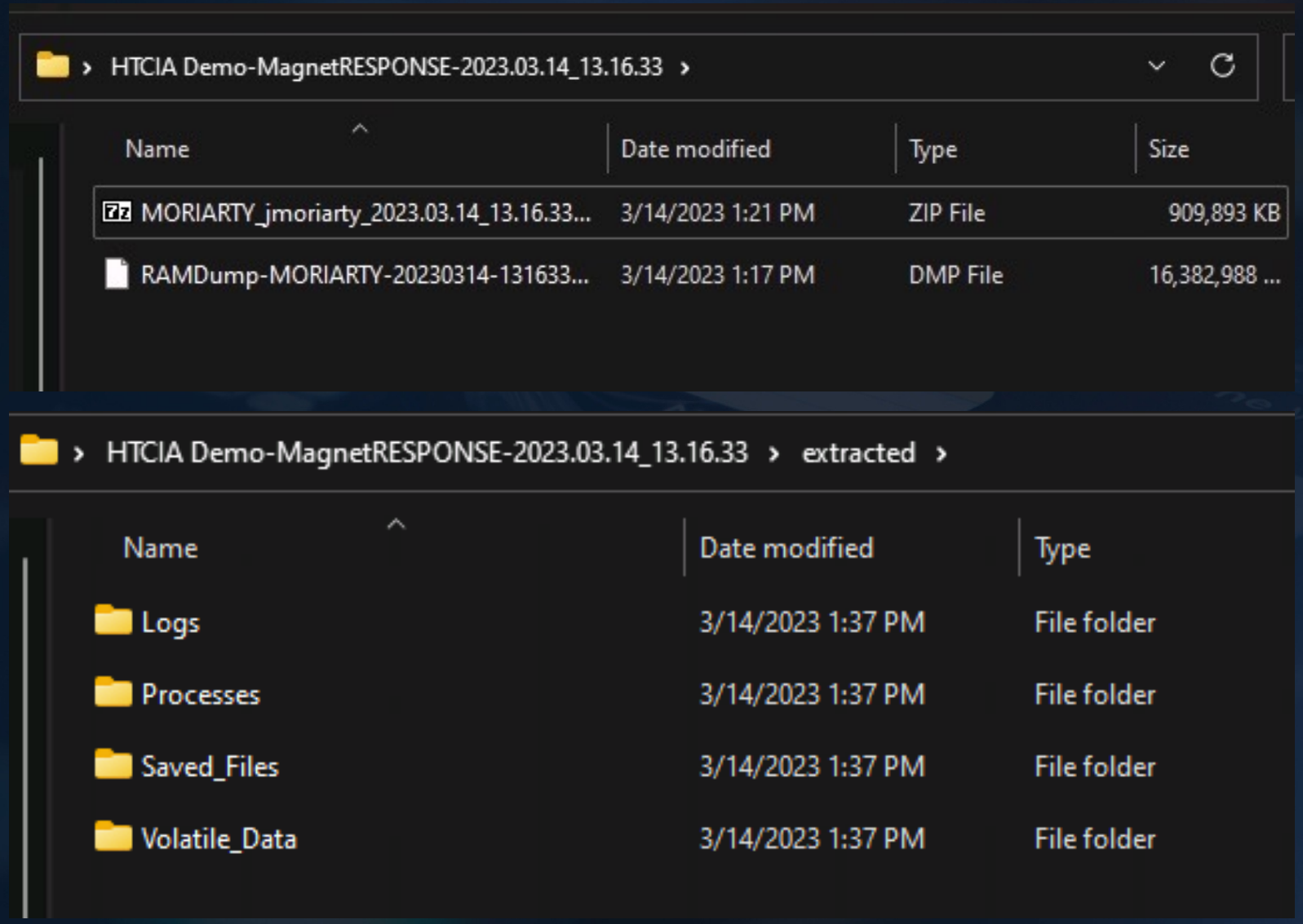


Magnet RESPONSE Demo

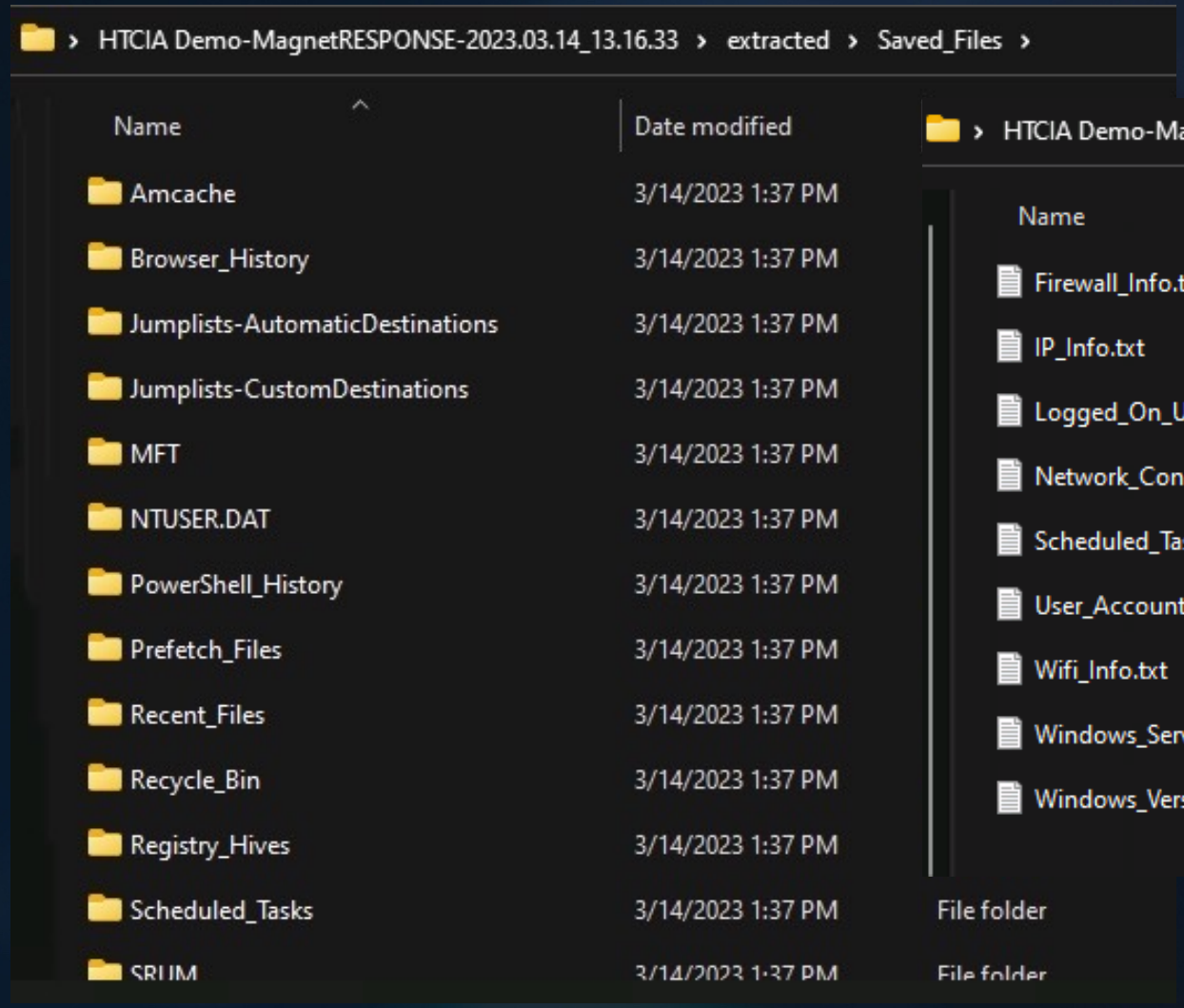
SEEK JUSTICE. PROTECT THE INNOCENT.

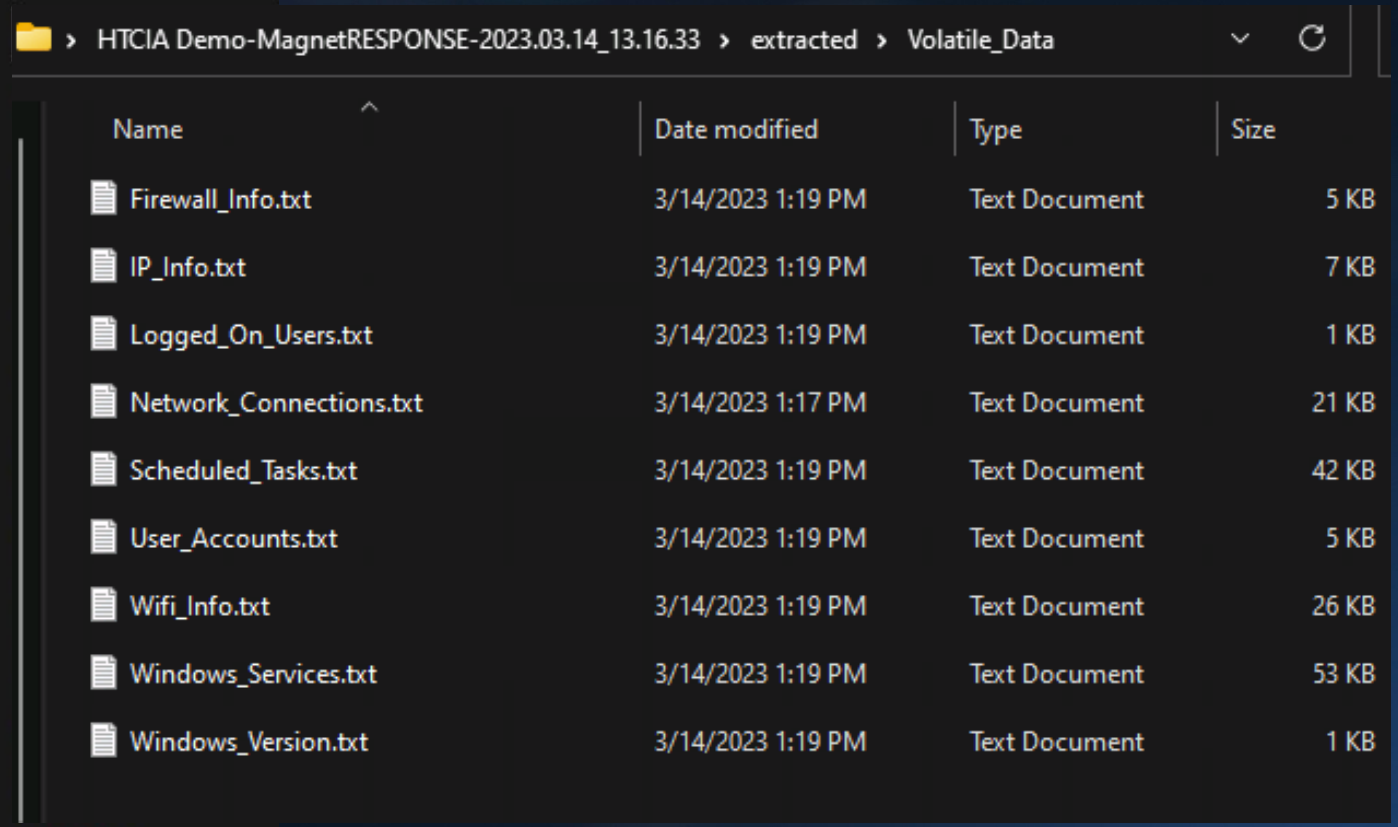
magnetforensics.com

Magnet RESPONSE Output



Magnet RESPONSE Output





SEEK JUSTICE. PROTECT THE INNOCENT.

HARDWARE CHOICES

15:30 Memory Acquisition

20:00 VHDX Created

25:48 Complete

1:45 Memory Acquisition

3:15 VHDX Created

3:55 Complete

SEEK JUSTICE. PROTECT THE INNOCENT.

ADDITIONAL POWERSHELL RESOURCES

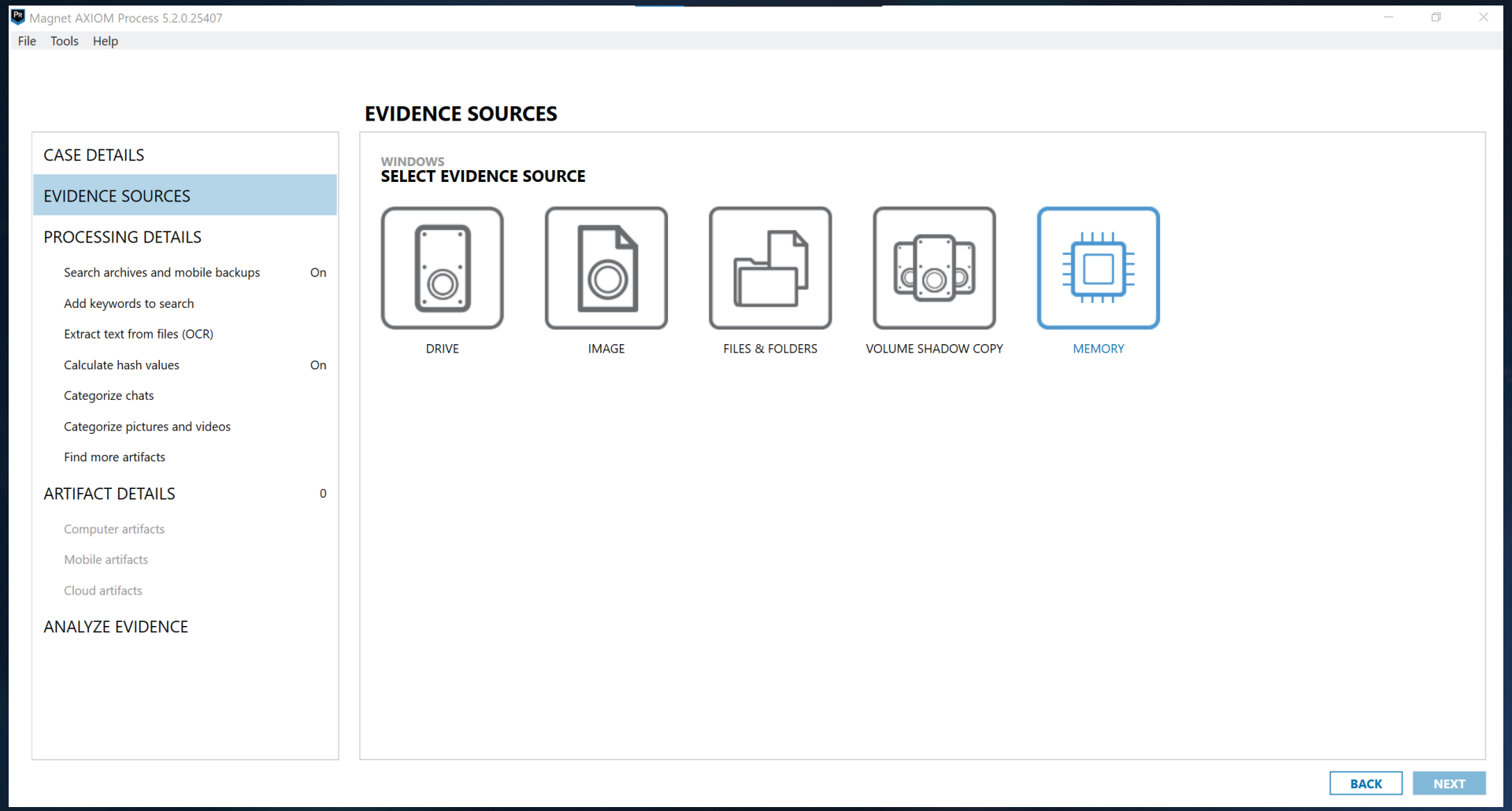
QuickPcap.ps1	A quick and easy PowerShell script to collect a packet trace on a Windows host without installing additional tools; with an option to convert .etl to .pcap.
MalHash.ps1	A PowerShell script that utilizes the Virus Total API to interact with VT from the command-line. The script uses PowerShell to get the MD5, SHA1 and SHA256 hash of the file. The script then (referencing your API key for the lookup), submits the MD5 (by default) hash to Virus Total. The results of the query are displayed back to the PowerShell instance and are also recorded to a text file.
Axiom-PowerShell	Set of PowerShell scripts to aid investigators when utilizing O365 and Magnet Axiom.

EVIDENCE PROCESSING TIPS

MAGNET FORENSICS®

SEEK JUSTICE. PROTECT THE INNOCENT.

MEMORY PROCESSING

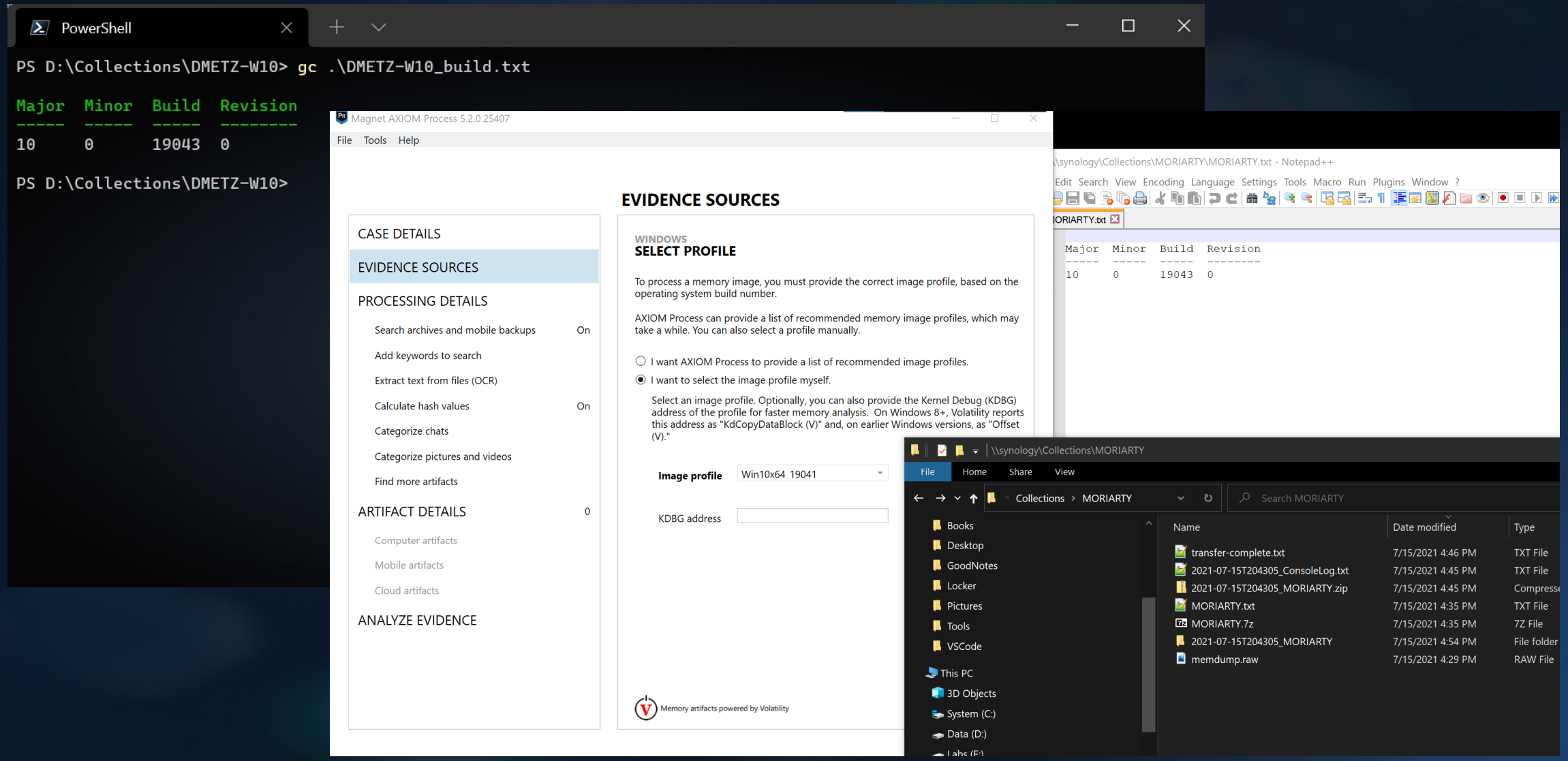


SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

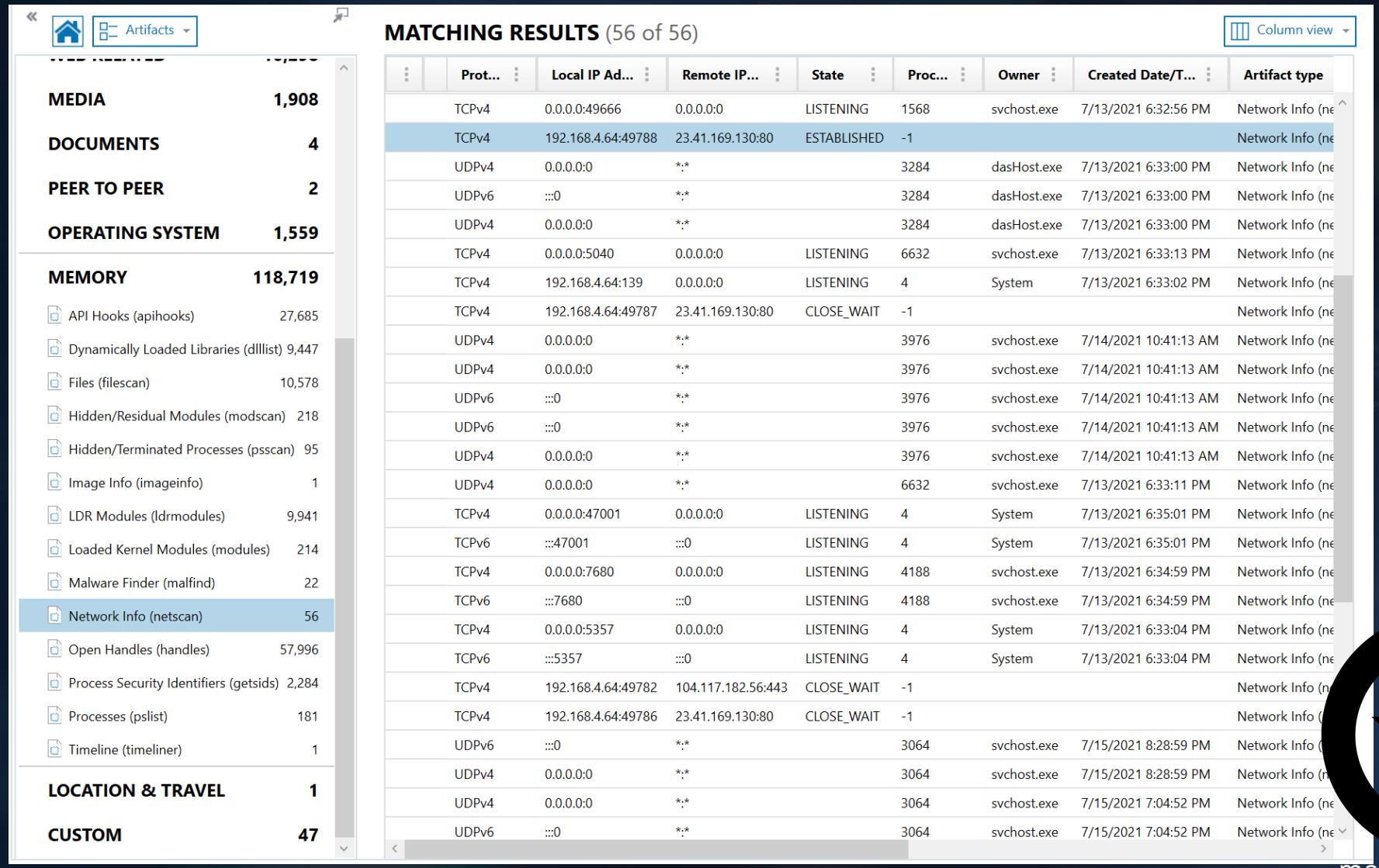
MEMORY PROCESSING

Use the Build Info ($hostname.txt) to specify memory profile



SEEK JUSTICE. PROTECT THE INNOCENT.

MEMORY ARTIFACTS FROM VOLATILITY

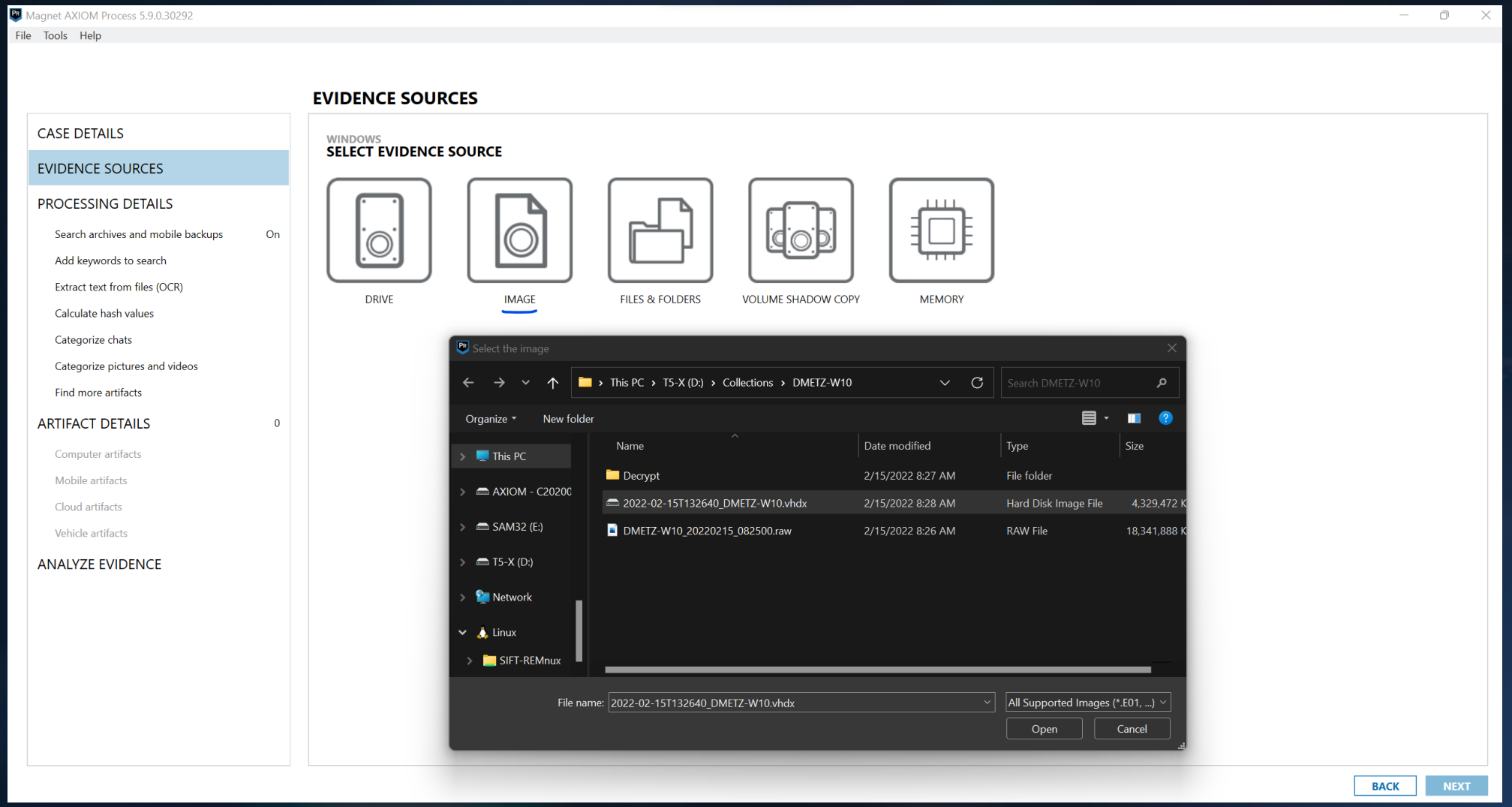


Prot...	Local IP Ad...	Remote IP...	State	Proc...	Owner	Created Date/T...	Artifact type
TCPv4	0.0.0.0:49666	0.0.0.0:0	LISTENING	1568	svchost.exe	7/13/2021 6:32:56 PM	Network Info (ne
TCPv4	192.168.4.64:49788	23.41.169.130:80	ESTABLISHED	-1			Network Info (ne
UDPv4	0.0.0.0:0	*:*		3284	dasHost.exe	7/13/2021 6:33:00 PM	Network Info (ne
UDPv6	:::0	*:*		3284	dasHost.exe	7/13/2021 6:33:00 PM	Network Info (ne
UDPv4	0.0.0.0:0	*:*		3284	dasHost.exe	7/13/2021 6:33:00 PM	Network Info (ne
TCPv4	0.0.0.0:5040	0.0.0.0:0	LISTENING	6632	svchost.exe	7/13/2021 6:33:13 PM	Network Info (ne
TCPv4	192.168.4.64:139	0.0.0.0:0	LISTENING	4	System	7/13/2021 6:33:02 PM	Network Info (ne
TCPv4	192.168.4.64:49787	23.41.169.130:80	CLOSE_WAIT	-1			Network Info (ne
UDPv4	0.0.0.0:0	*:*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
UDPv4	0.0.0.0:0	*:*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
UDPv6	:::0	*:*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
UDPv6	:::0	*:*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
UDPv4	0.0.0.0:0	*:*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
UDPv4	0.0.0.0:0	*:*		6632	svchost.exe	7/13/2021 6:33:11 PM	Network Info (ne
TCPv4	0.0.0.0:47001	0.0.0.0:0	LISTENING	4	System	7/13/2021 6:35:01 PM	Network Info (ne
TCPv6	:::47001	:::0	LISTENING	4	System	7/13/2021 6:35:01 PM	Network Info (ne
TCPv4	0.0.0.0:7680	0.0.0.0:0	LISTENING	4188	svchost.exe	7/13/2021 6:34:59 PM	Network Info (ne
TCPv6	:::7680	:::0	LISTENING	4188	svchost.exe	7/13/2021 6:34:59 PM	Network Info (ne
TCPv4	0.0.0.0:5357	0.0.0.0:0	LISTENING	4	System	7/13/2021 6:33:04 PM	Network Info (ne
TCPv6	:::5357	:::0	LISTENING	4	System	7/13/2021 6:33:04 PM	Network Info (ne
TCPv4	192.168.4.64:49782	104.117.182.56:443	CLOSE_WAIT	-1			Network Info (n
TCPv4	192.168.4.64:49786	23.41.169.130:80	CLOSE_WAIT	-1			Network Info (
UDPv6	:::0	*:*		3064	svchost.exe	7/15/2021 8:28:59 PM	Network Info (
UDPv4	0.0.0.0:0	*:*		3064	svchost.exe	7/15/2021 8:28:59 PM	Network Info (n
UDPv4	0.0.0.0:0	*:*		3064	svchost.exe	7/15/2021 7:04:52 PM	Network Info (ne
UDPv6	:::0	*:*		3064	svchost.exe	7/15/2021 7:04:52 PM	Network Info (ne

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

VMDK IMAGE PROCESSING

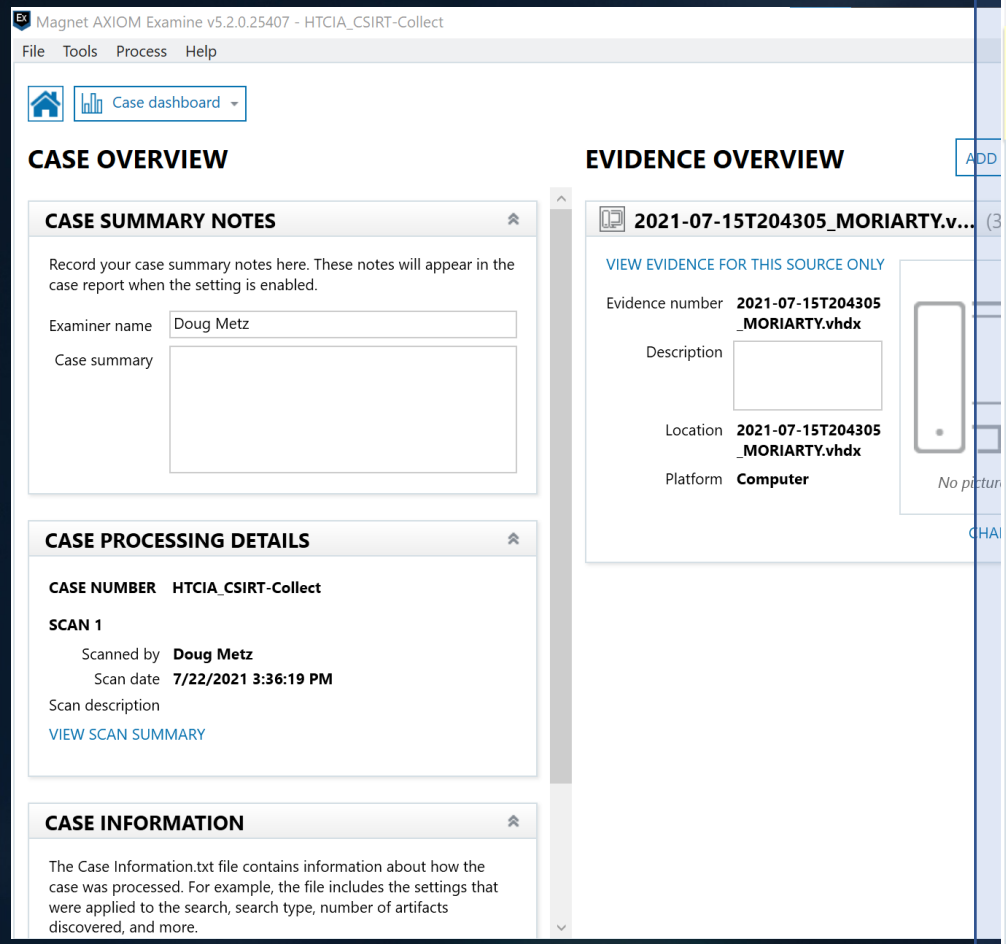


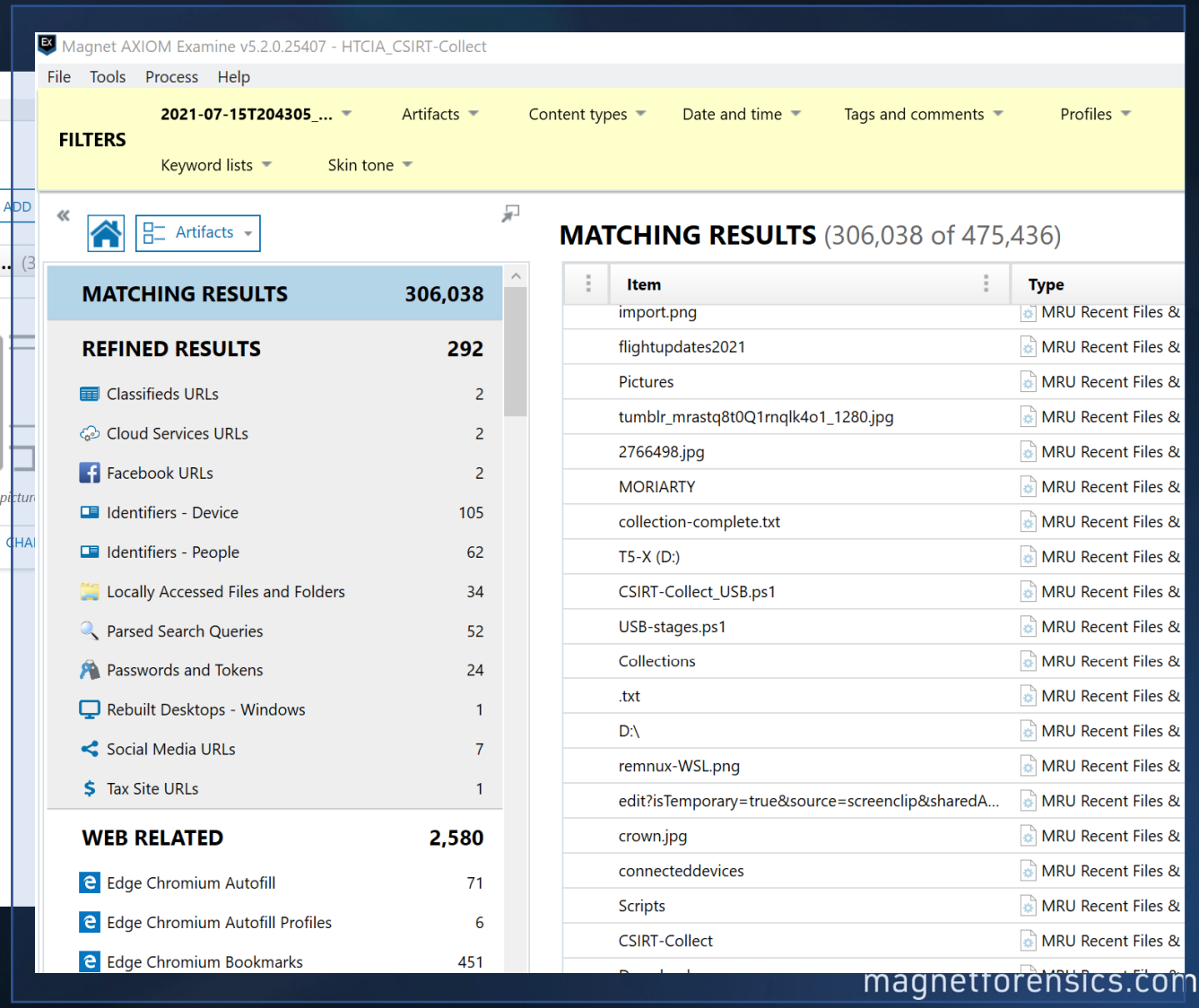
Computer > Windows > Load Evidence > IMAGE

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

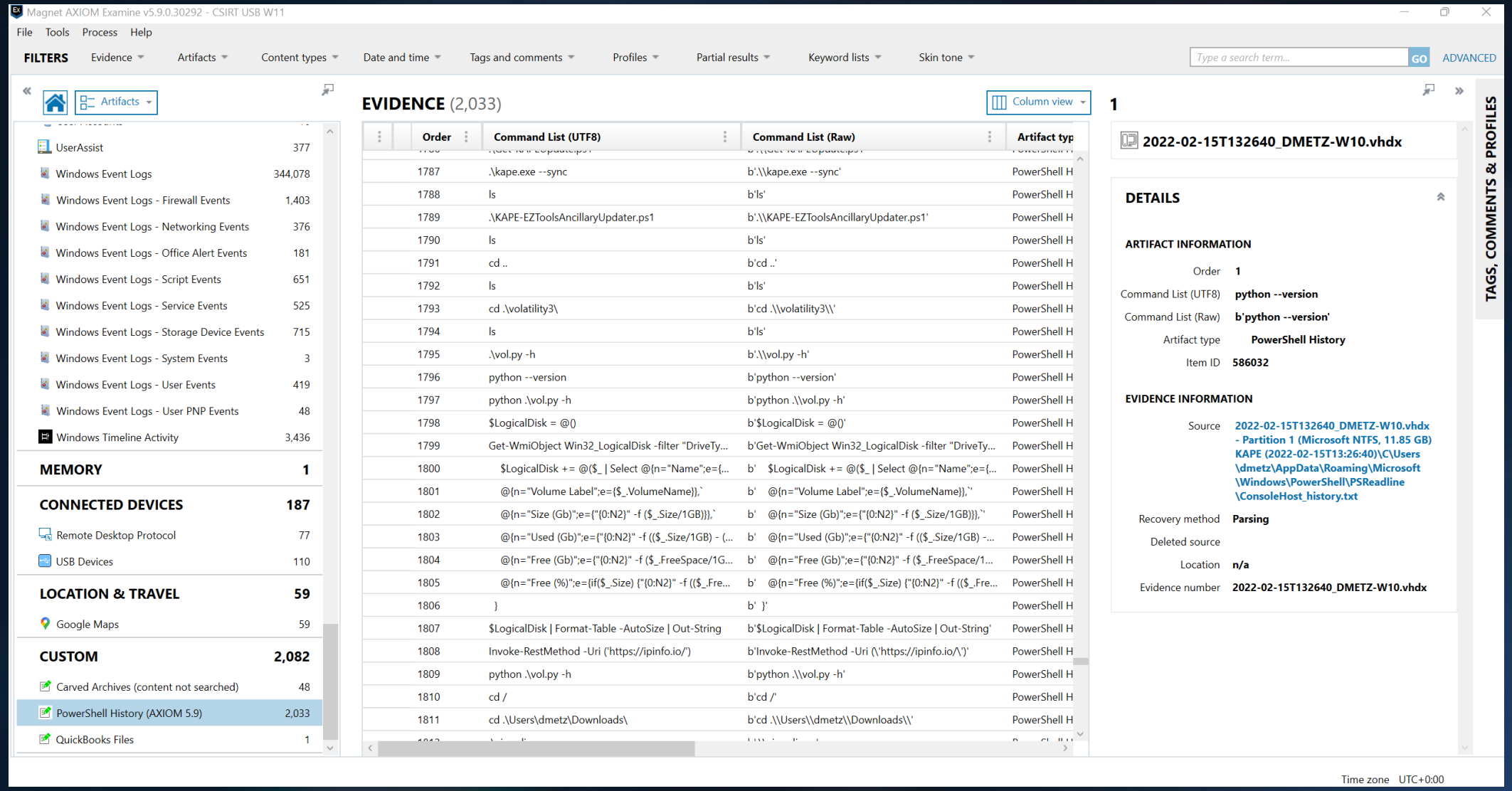
ARTIFACTS FROM TRIAGE IMAGE (VMDK)





SEEK JUSTICE. PROTECT THE INNOCENT.

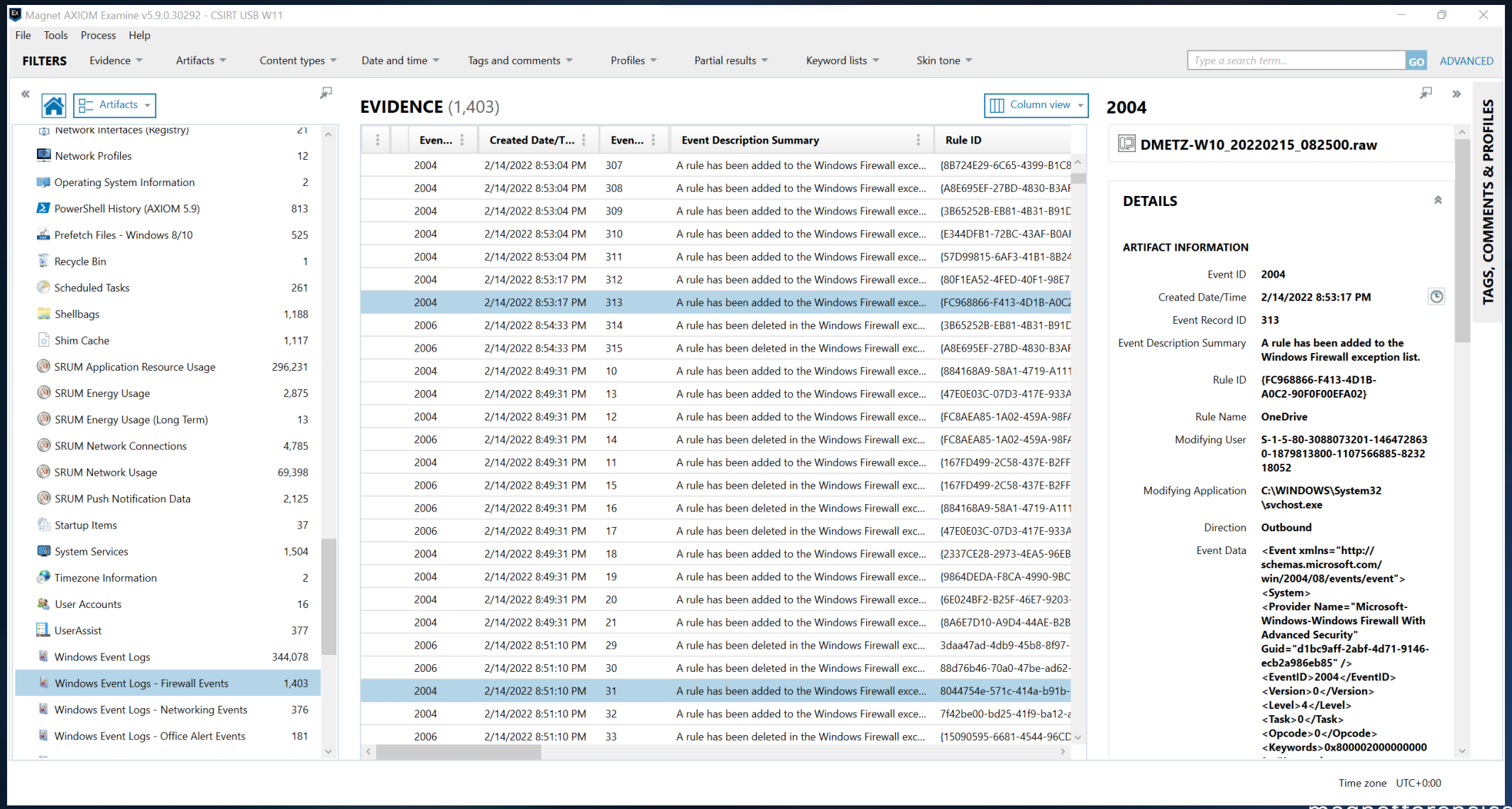
POWERSHELL HISTORY



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

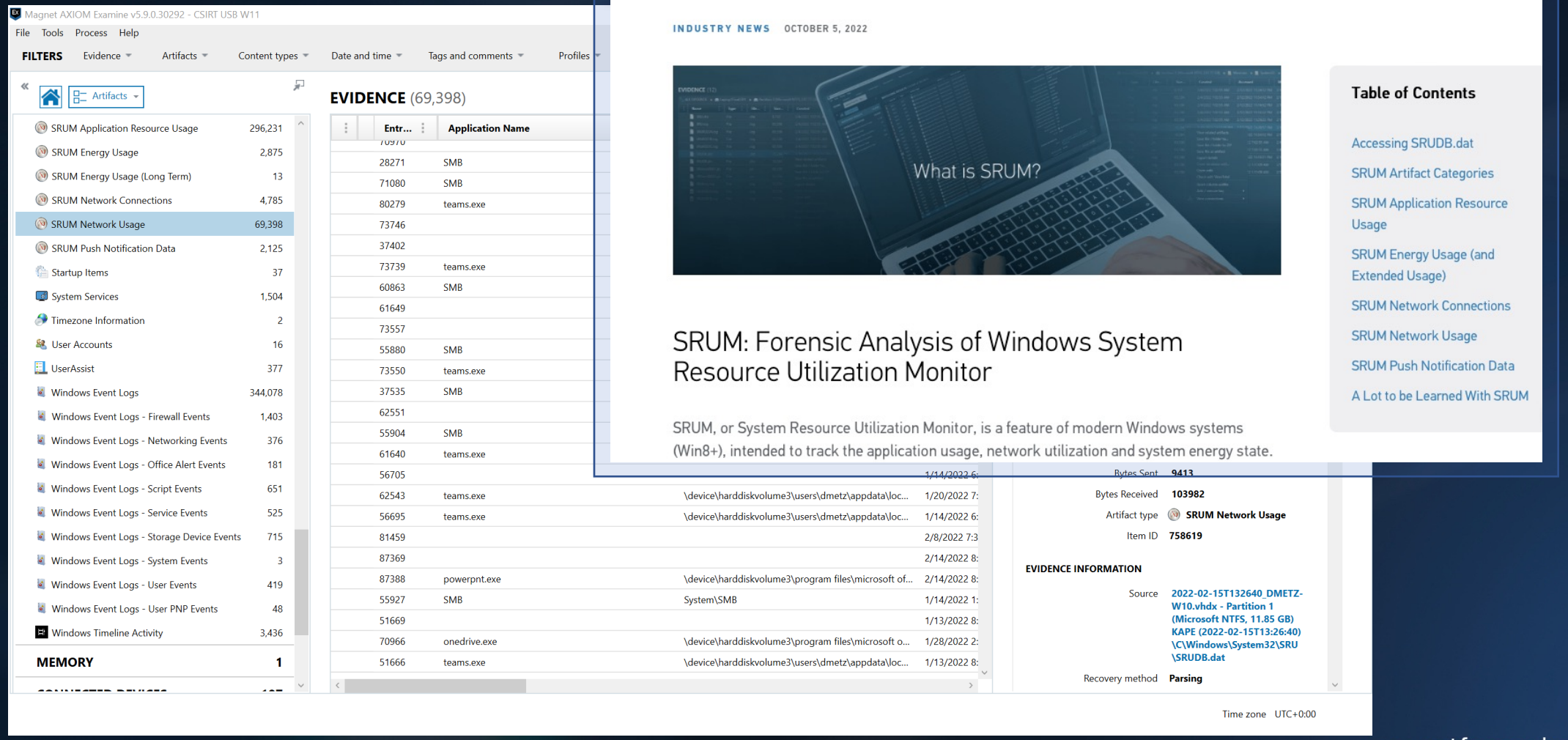
FIREWALL EVENTS



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

SYSTEM RESOURCE USAGE MONITOR (SRUM)

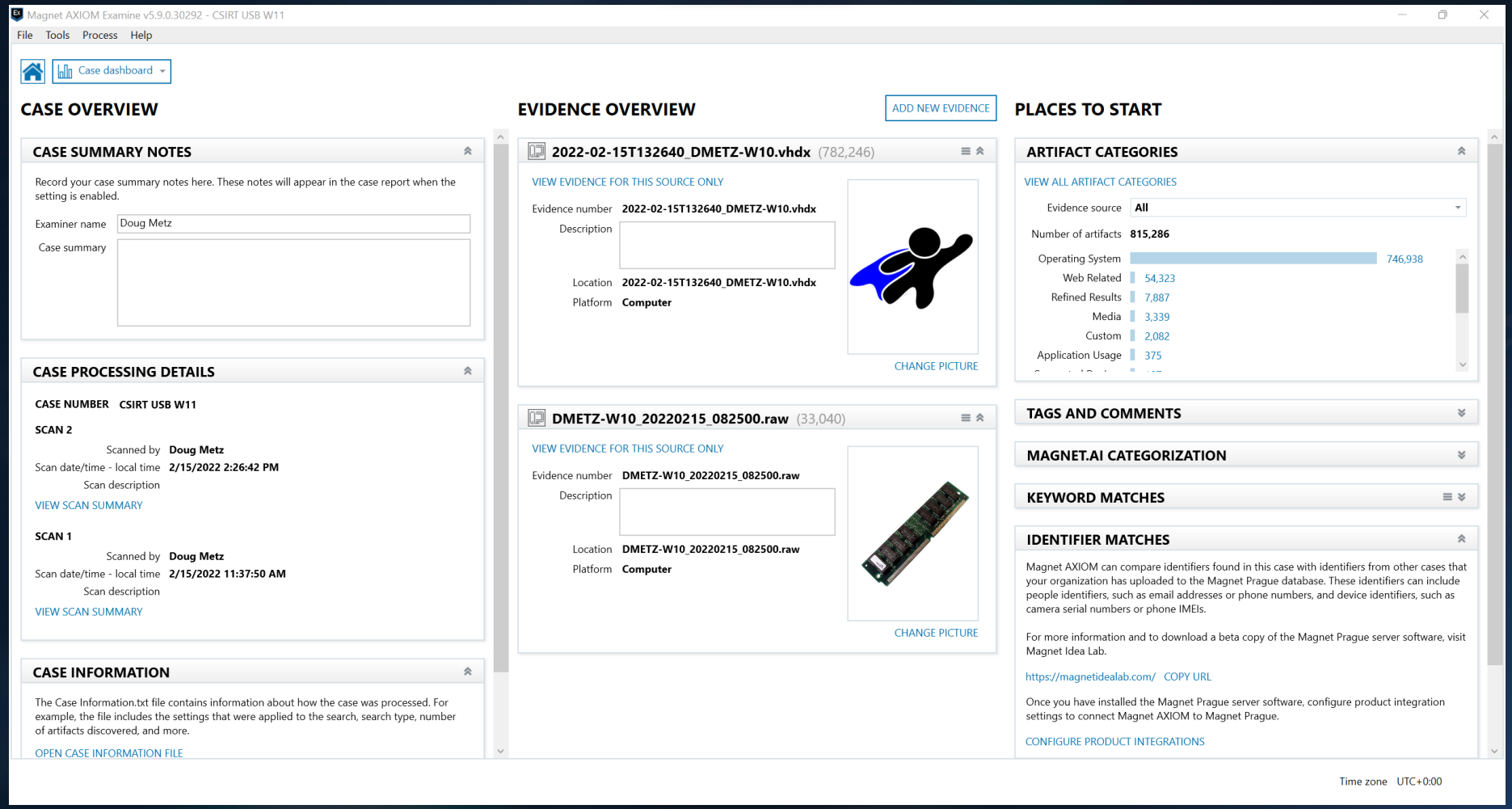


https://www.magnetforensics.com/blog/srum-forensic-analysis-of-windows-system-resource-utilization-monitor/

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

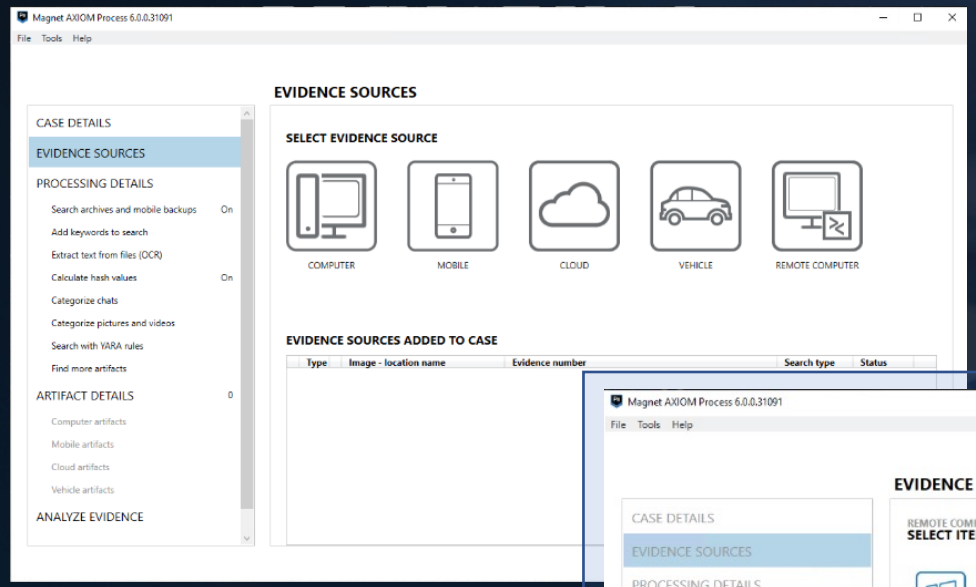
OFFLINE COLLECTIONS PROCESSED – WHAT'S NEXT?

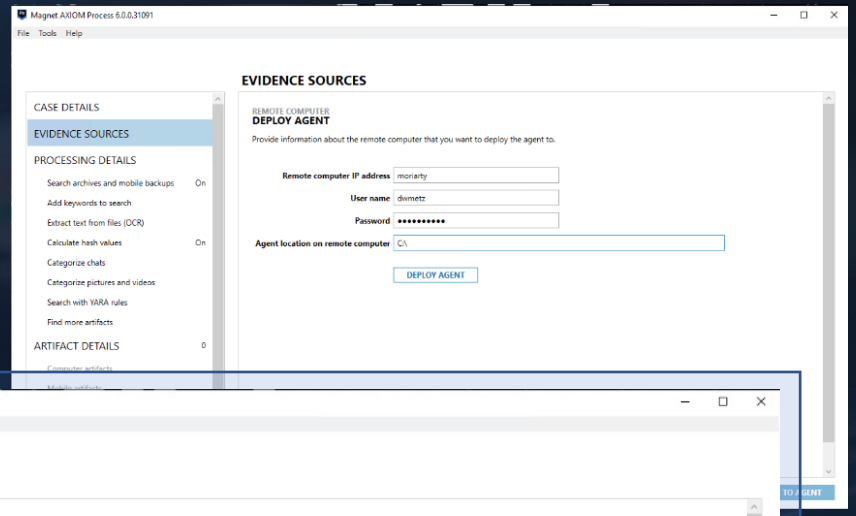


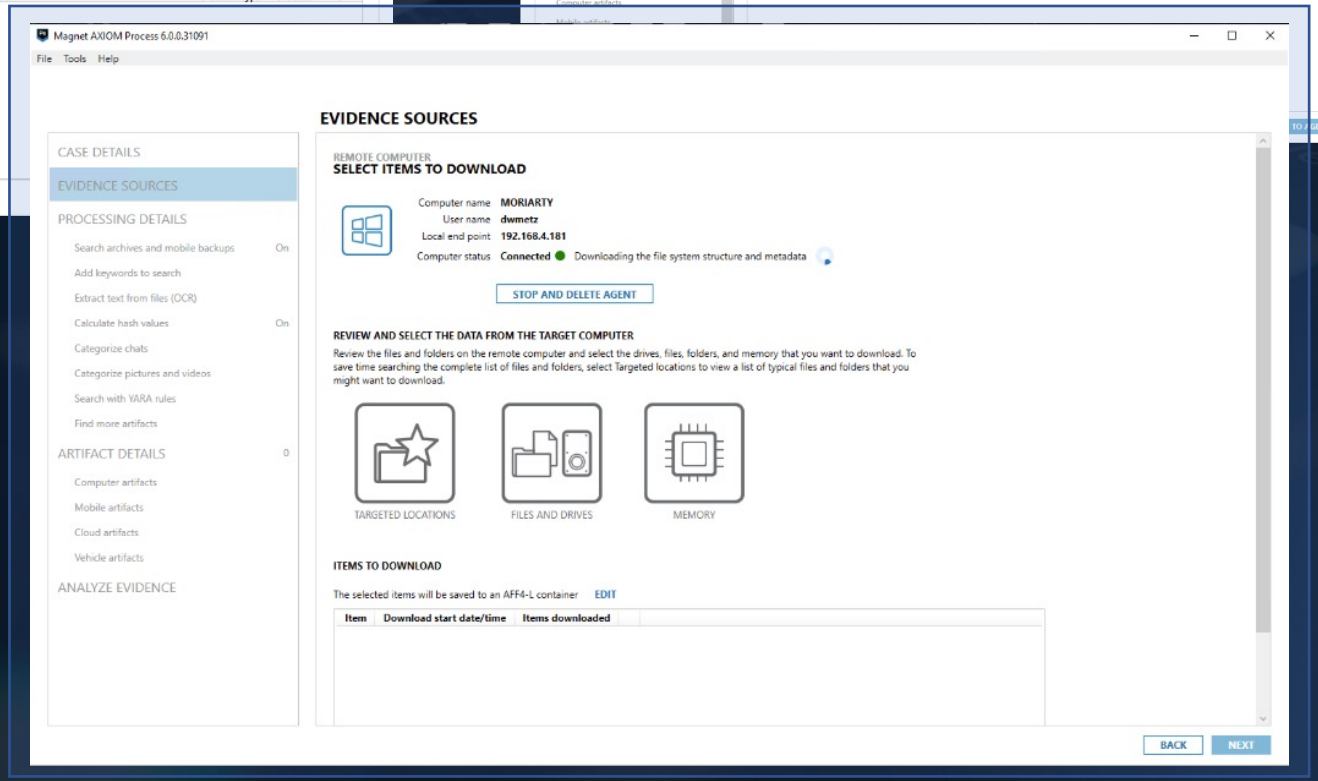
SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

COLLECTING MORE WITH AXIOM CYBER







Office 365

iOS

aws

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

RESOURCES

CyberPipe: https://github.com/dwmetz/CyberPipe

Magnet DumpIt for Windows: https://support.magnetforensics.com/s/free-tools

Magnet Encrypted Disk Detector (EDD): https://support.magnetforensics.com/s/free-tools

KAPE: https://www.sans.org/tools/kape

My Other PowerShell Scripts: https://github.com/dwmetz

Magnet RESPONSE:

Magnet AXIOM: https://www.magnetforensics.com/products/magnet-axiom-cyber/

Blog: https://bakerstreetforensics.com

THANK YOU

https://github.com/dwmetz

https://bakerstreetforensics.com

doug.metz@magnetforensics.com

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

https://infosec.exchange/@dwmetz

@dwmetz

SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNET FORENSICS®

magnetforensics.com