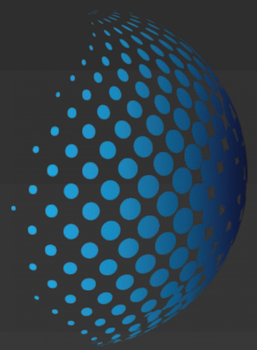
Free Tools for Triage Collections

Doug Metz

Professional Services Consultant, Magnet Forensics



HTCIA

Tech Tuesday Series
1 November 2022

Who Am I

PS /Users/dwmetz/Documents> gc ./whoami.txt

I started in security in the days of Windows 98 and Google priced at $85/share.

Nearly 20 years of DFIR experience supporting government, private sector and academic institutions - from building and protecting secure networks, to defending them, to identifying and responding to compromises, internal and external.

Prior to Magnet I was the Incident Response Manager and forensics lead for a Fortune 200, leading a small global team of incident responders and 24x7 SOC.

HTCIA Delaware Valley-Philly Chapter
Volunteer for The Magnet Auxtera Project
PowerShell Fanboy
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

BAKER STREET FORENSICS

D . F . I . R .

WHERE IRREGULARS ARE PART OF THE GAME

Agenda

- CSIRT-Collect & Use Cases
- Magnet Ram Capture, EDD, & KAPE
- Hardware Choices
- Script Output
- Additional PowerShell Utilities
- Tips for Effective Evidence Processing

CSIRT-Collect PowerShell

CSIRT-Collect is a PowerShell script for Incident Response investigations that captures RAM and disk artifacts to a network share.

CSIRT-Collect_USB is a variant of the script intended to be run direct from a USB device.

CSIRT-Collect	CSIRT-Collect USB
Magnet RAM Capture	Magnet RAM Capture
KAPE (Disk Triage)	KAPE (Disk Triage)
Compression	[omitted in USB edition]
Network Share	USB Device
	Encrypted Disk Detector (EDD)
	BitLocker Key Recovery

Deployment Options

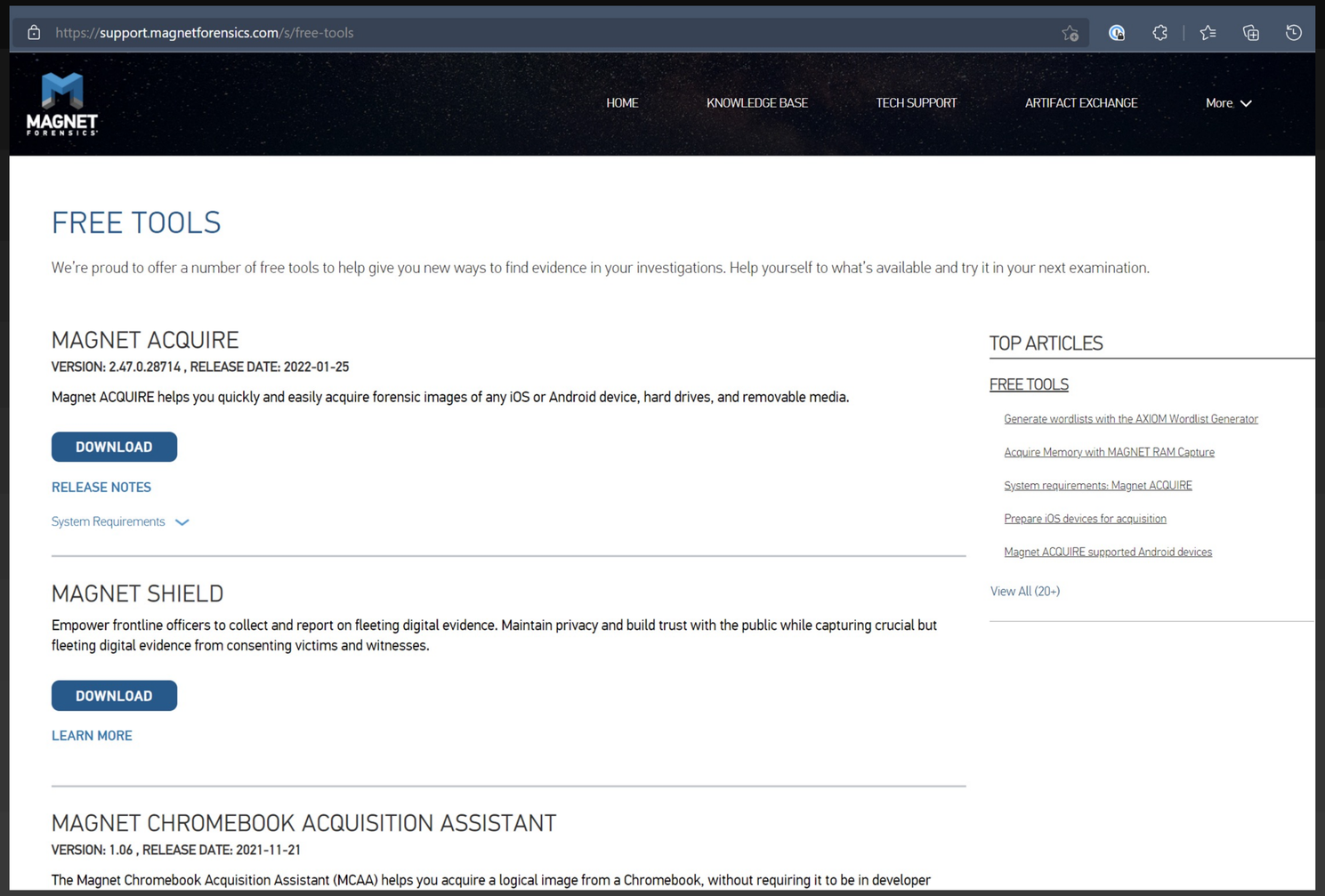
- SOC (Security Operations Center)
- Help Desk
- Field Support / Local IT
- Group Policy
- SOAR (Automation)
- EDR (Endpoint Detection and Response)
- USB Media *

[USB] Collect from Network Isolated Assets

- Ransomware response
- Airgap; Manufacturing / Medical / ICS
- Enterprise resources not available
- BOGHOK (Boots on Ground, Hands on Keyboard)

MAGNET Free Tools

- Magnet RAM Capture
- Encrypted Disk Detector (EDD)



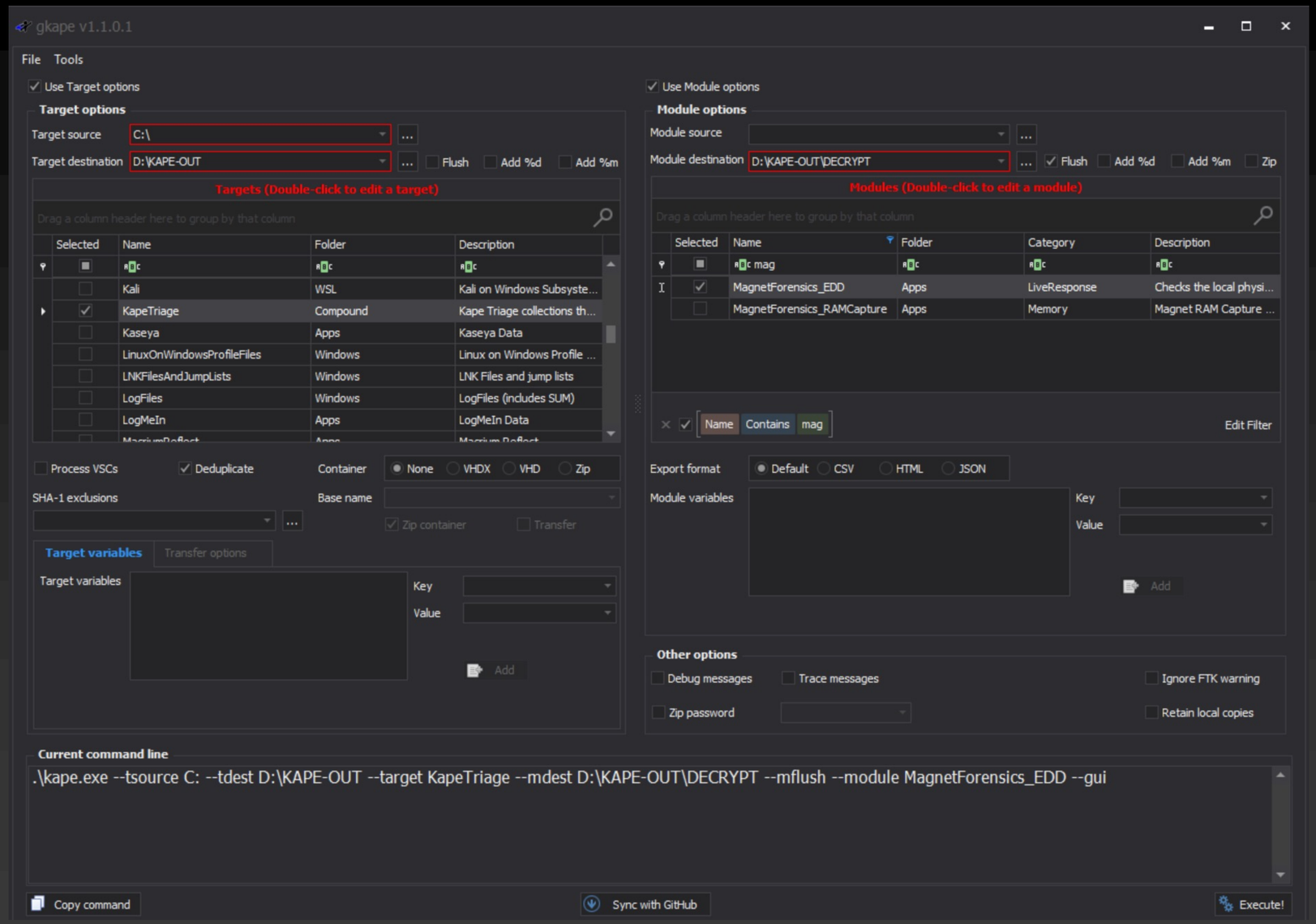
MAGNET FORENSICS®

KAPE

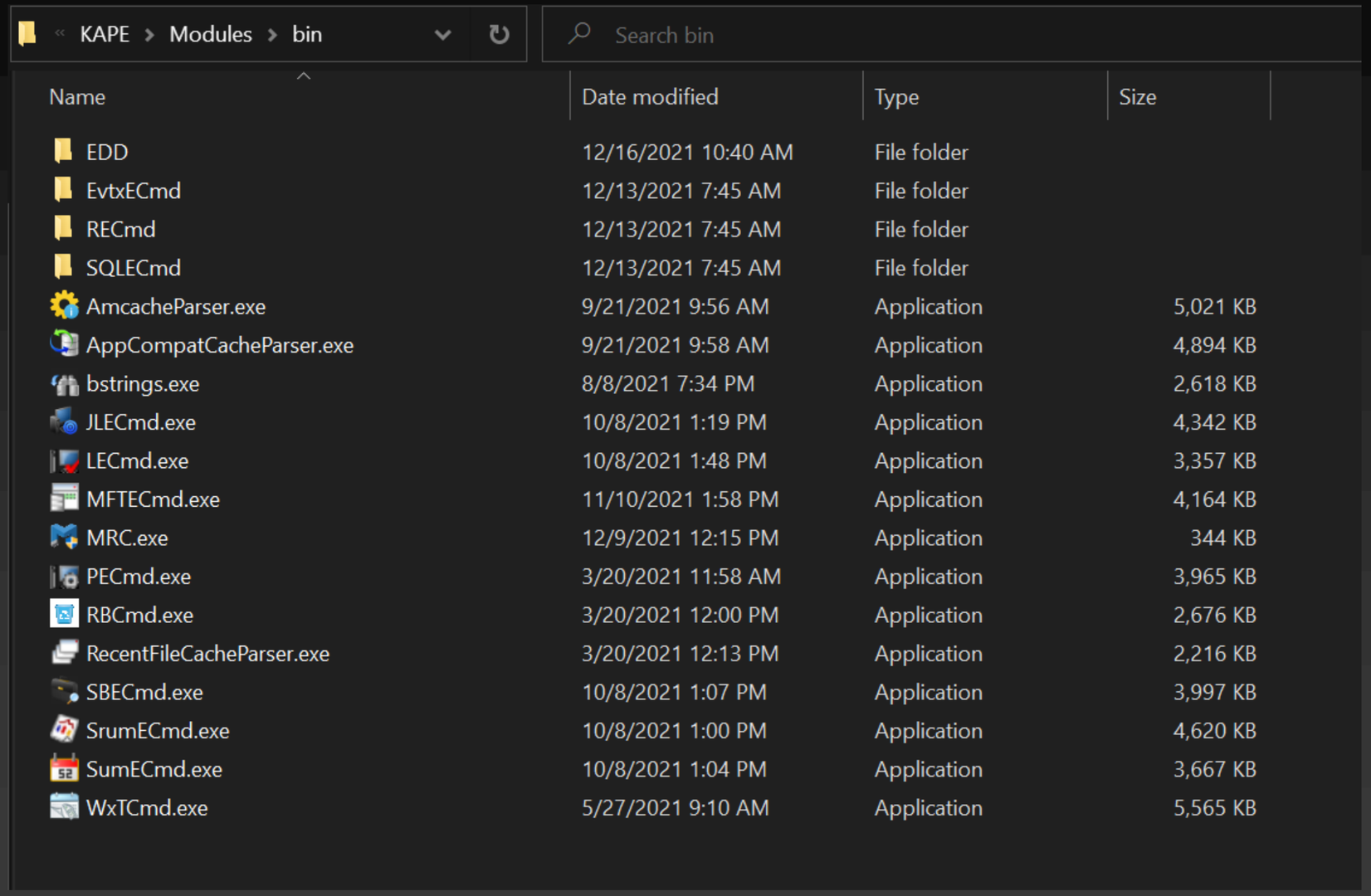
Targets: categories of artifacts that can be collected (registry, event logs, browser activity…)

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

GUI and Command Line



Tools in the /bin - BYOE



Check your binaries

Editor: MagnetForensics_EDD

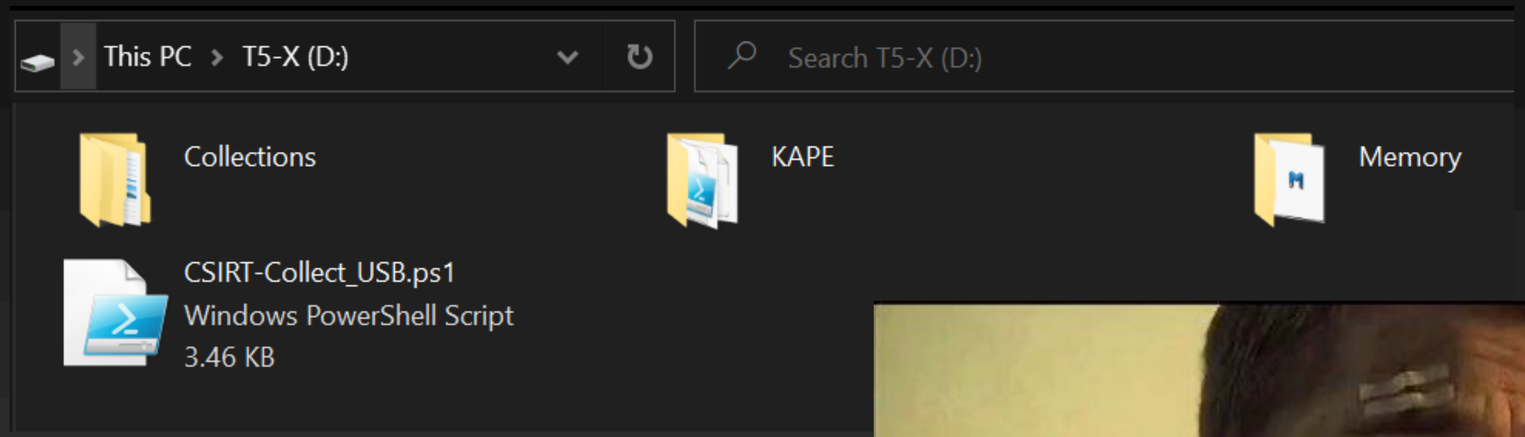
```
Description: Checks the local physical drives on a system for TrueCrypt, PGP, VeraCrypt, SafeBoot, or Bitlocker encrypted volumes
Category: LiveResponse
Author: Mohamed El-Hadidi
Version: 1.1
Id: c7212da1-ed41-4560-95f7-1a2d99acc1f8
BinaryUrl: https://www.magnetforensics.com/resources/encrypted-disk-detector/
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"
```

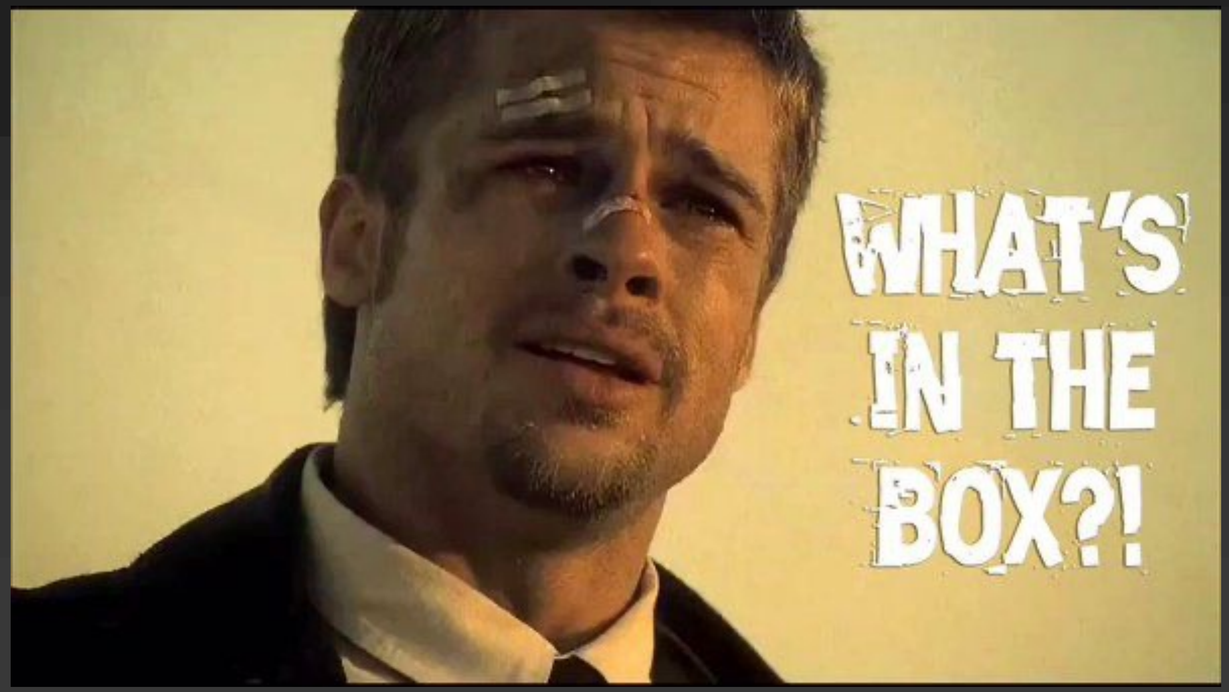
Reload Generate GUID

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

Folder Layout

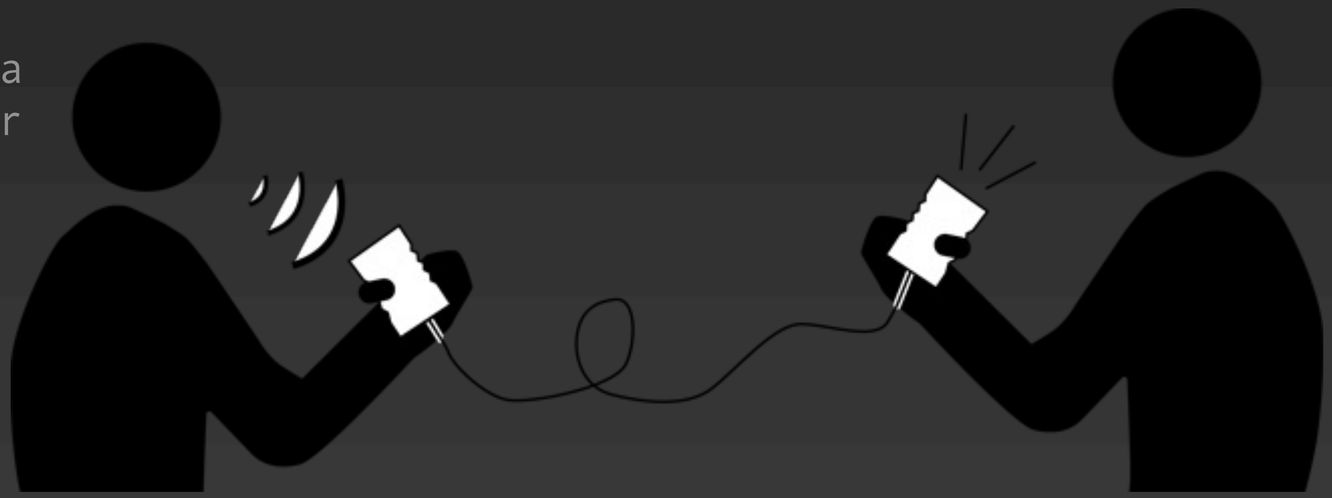




The Handoff

“I need you to do a forensic capture of the RAM and active processes and then proceed with a triage collection of host artifacts. Then check if encrypted disks are present. If so, validate recovery key can be retrieved before powering off. And keep a detailed log of all your actions.”

“1. Plug in USB device
2. Open PowerShell as Admin
3. Execute CSIRT-Collect_USB.ps1”



CSIRT-Collect

Stage 1

[Network]

Maps to existing network drive
Subdir 1 : “Memory” – MRC and 7zip exe’s
Subdir 2: ”KAPE” – directory copied from local install

Creates a local directory on asset

Copies the Memory exe files to local directory

[Network & USB]

Captures memory with Magnet RAM Capture

When complete, ZIPs the memory image [Network]

Renames the zip file based on hostname

Documents the OS Build Info for later memory processing

Compressed image is copied to network directory and deleted from host after transfer complete [Network]

```
15  ## map the  (parameter) -Fore  hange to that directory
16  Write-Host -Fore Green "Mapping network drive..."
17
18
19  $Networkpath = "X:\"
20
21
22  If (Test-Path -Path $Networkpath) {
23      Write-Host -Fore Green "Drive Exists already"
24  }
25  Else {
26      #map network drive
27      (New-Object -ComObject WScript.Network).MapNetworkDrive("X:","\\Synology\Collections",
28
29      #check mapping again
30      If (Test-Path -Path $Networkpath) {
31          Write-Host -Fore Green "Drive has been mapped"
32      }
33      Else {
34          Write-Host -For Red "Error mapping drive"
35      }
36  }
37  #Remove-PSDrive -Name X
38  #New-PSDrive -Name X -PSProvider FileSystem -Root "\\Synology\Collections"
39
40  # create local memory directory
41  Write-Host -Fore Green "Setting up local directory..."
42  mkdir C:\temp\IR -Force
43  Set-Location C:\temp\IR
44  Write-Host -Fore Green "Copying tools..."
45  robocopy "\\Synology\Collections\Memory" . *.exe
46  ## capture memory image
47  Write-Host -Fore Green "Capturing memory..."
48  .\winpmem.exe memdump.raw
49  ## zip the memory image
50  Write-Host -Fore Green "Zipping the memory image..."
51  .\7za a -t7z memdump.7z memdump.raw -mx1
52  ## delete the raw file
53  Remove-Item memdump.raw
```

CSIRT-Collect
Stage 2

- New directory for KAPE output
- KapeTriage collection is run using VHDX as output format [$hostname.vhdx]
- VHDX transfers to network [Network]
- Removes the local KAPE directory after completion [Network]
- Writes a “Process complete” text file to signal investigators that collection is ready for analysis

```
57  [System.Environment]::OSVersion.Version > C:\Temp\IR\windowsbuild.txt
58  Write-Host -Fore Green "Renaming file..."
59  Get-ChildItem -Filter "*windowsbuild*" -Recurse | Rename-Item -NewName {$_.name -replace
60
61  ## create output directory on "Collections" share
62  mkdir X:\$env:COMPUTERNAME
63
64  Write-Host -Fore Green "Copying memory image to network..."
65
66  ## copy memory image to network
67  robocopy . "\\Synology\Collections\$env:COMPUTERNAME" *.7z *.txt
68
69  ## delete the directory and contents
70  Write-Host -Fore Green "Removing temporary files"
71  Set-Location C:\TEMP
72  Remove-Item -LiteralPath "C:\temp\IR" -Force -Recurse
73
74  ## create the KAPE directory on the client
75  Write-Host -Fore Green "Creating KAPE directory on host..."
76  mkdir C:\Temp\KAPE -Force
77
78  ## execute the KAPE "OS" collection
79  Write-Host -Fore Green "Collecting OS artifacts..."
80  Set-Location X:\KAPE
81  .\kape.exe --tsource C: --tdest C:\Temp\KAPE --target !SANS_Triage --vhdx $env:COMPUTERN
82
83
84  ## transfer evidence to share
85  Set-Location C:\Temp\Kape
86  robocopy . "\\Synology\Collections\$env:COMPUTERNAME"
87
88  ## delete the local directory and contents
89  Write-Host -Fore Green "Removing temporary files"
90  Set-Location C:\TEMP
91  Remove-Item -LiteralPath "C:\temp\KAPE" -Force -Recurse
92  Set-Content -Path X:\$env:COMPUTERNAME\transfer-complete.txt -Value "Transfer complete:
```

Size Matters

Sample: Laptop with 250GB Hard Drive and 16GB RAM

*Network version statistics

Targeted Collection: 2GB

Collection Compressed: 688MB

Full memory acquisition: 16 GB

Compressed memory image: 5 GB

266GB of data we want to collect is now reduced to ~6 GB

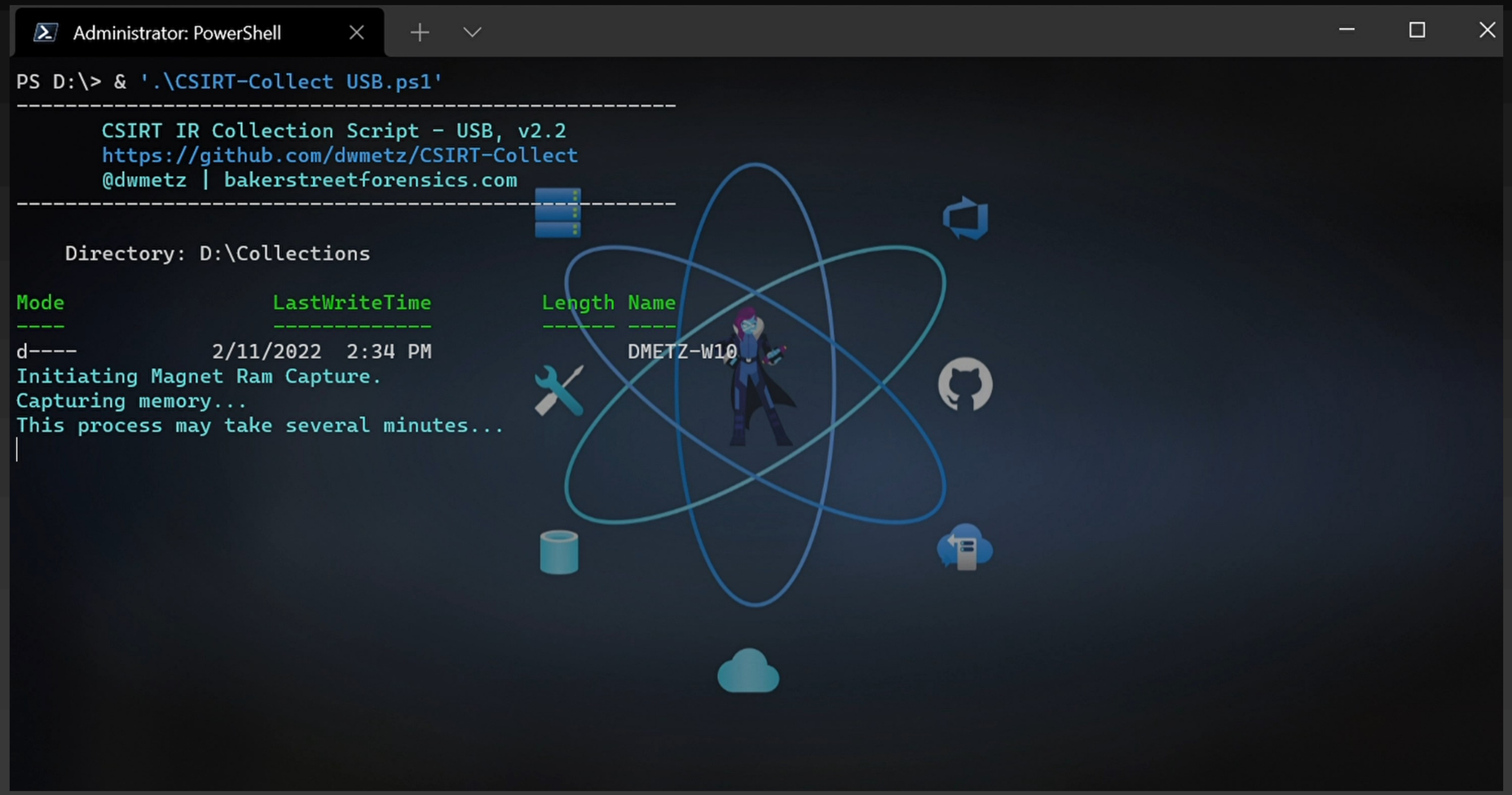
Data management on endpoints helps to preserve disk space

Easily portable (network share, USB, Azure/AWS)

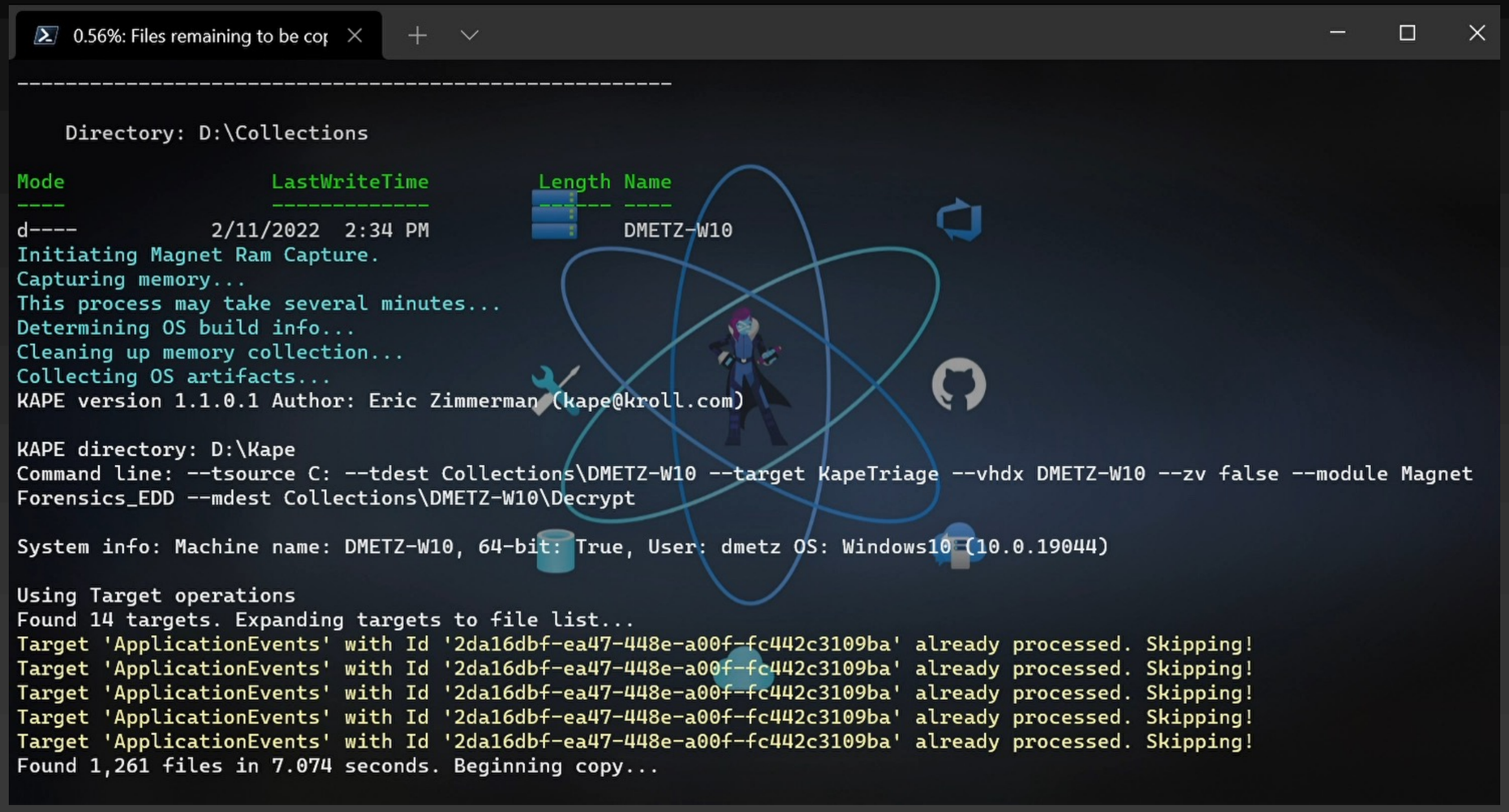
CSIRT-Collect [USB]

Script Walk Through

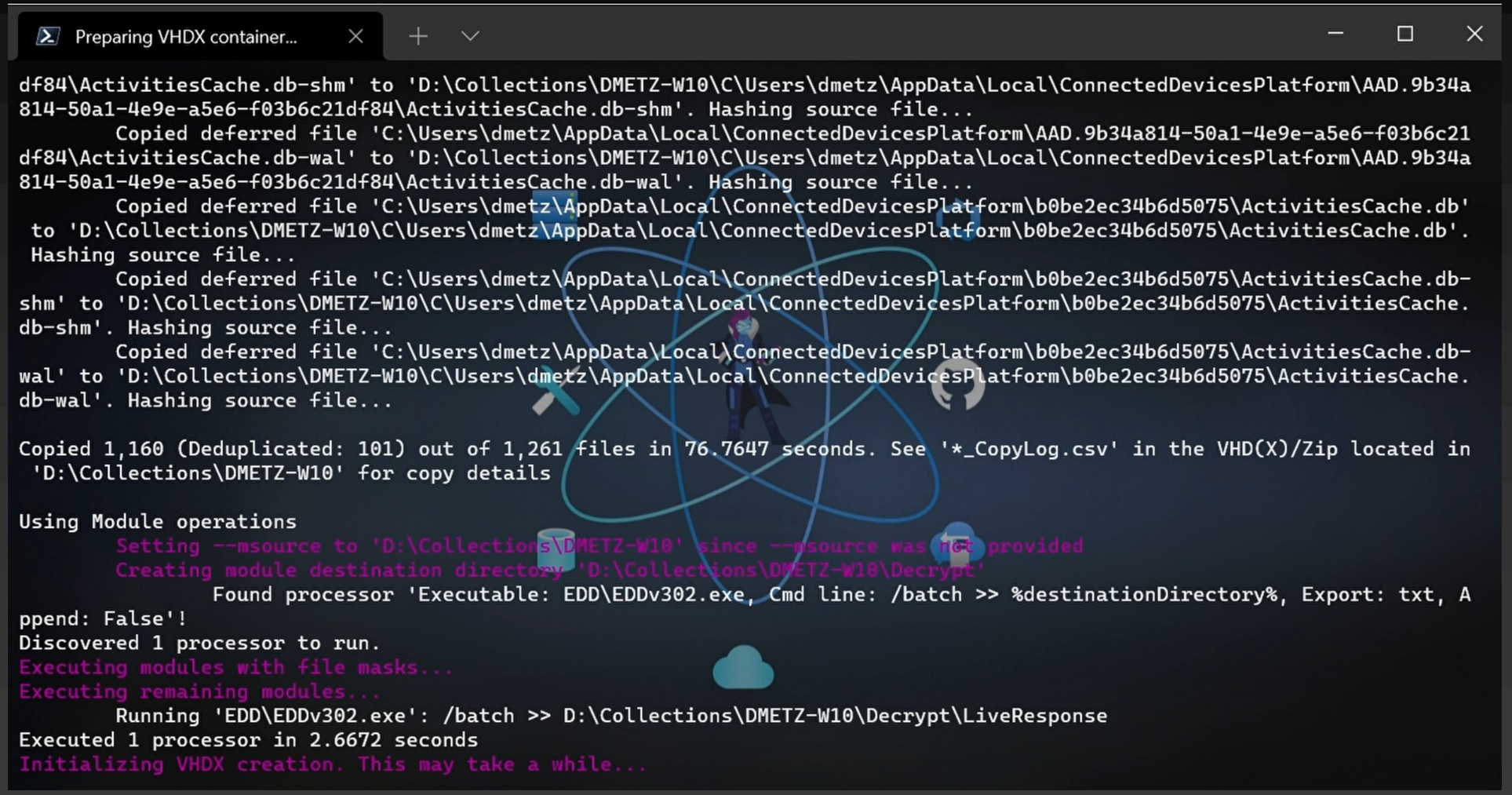
Memory Collection



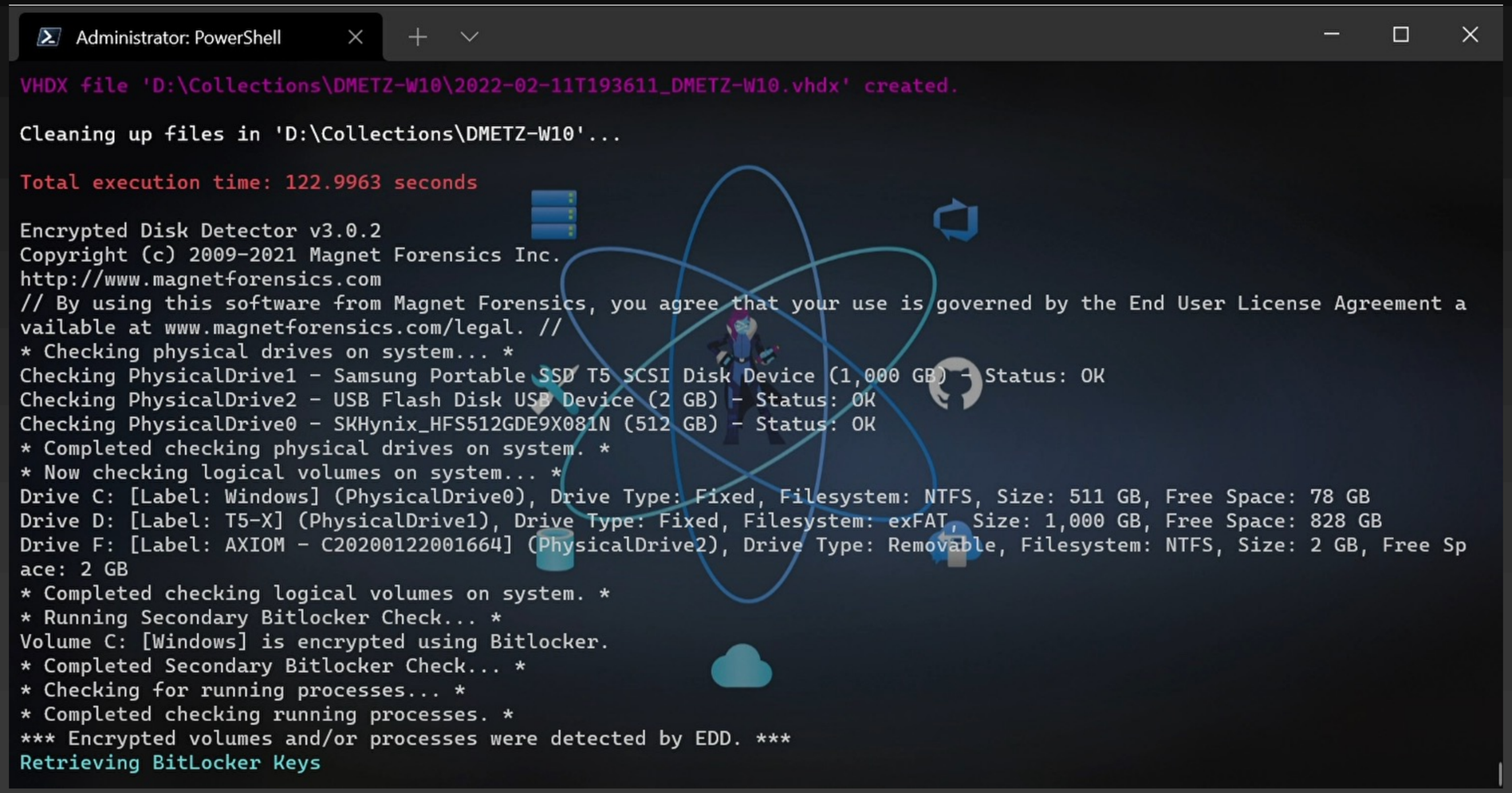
Build Info >>> KAPE Triage



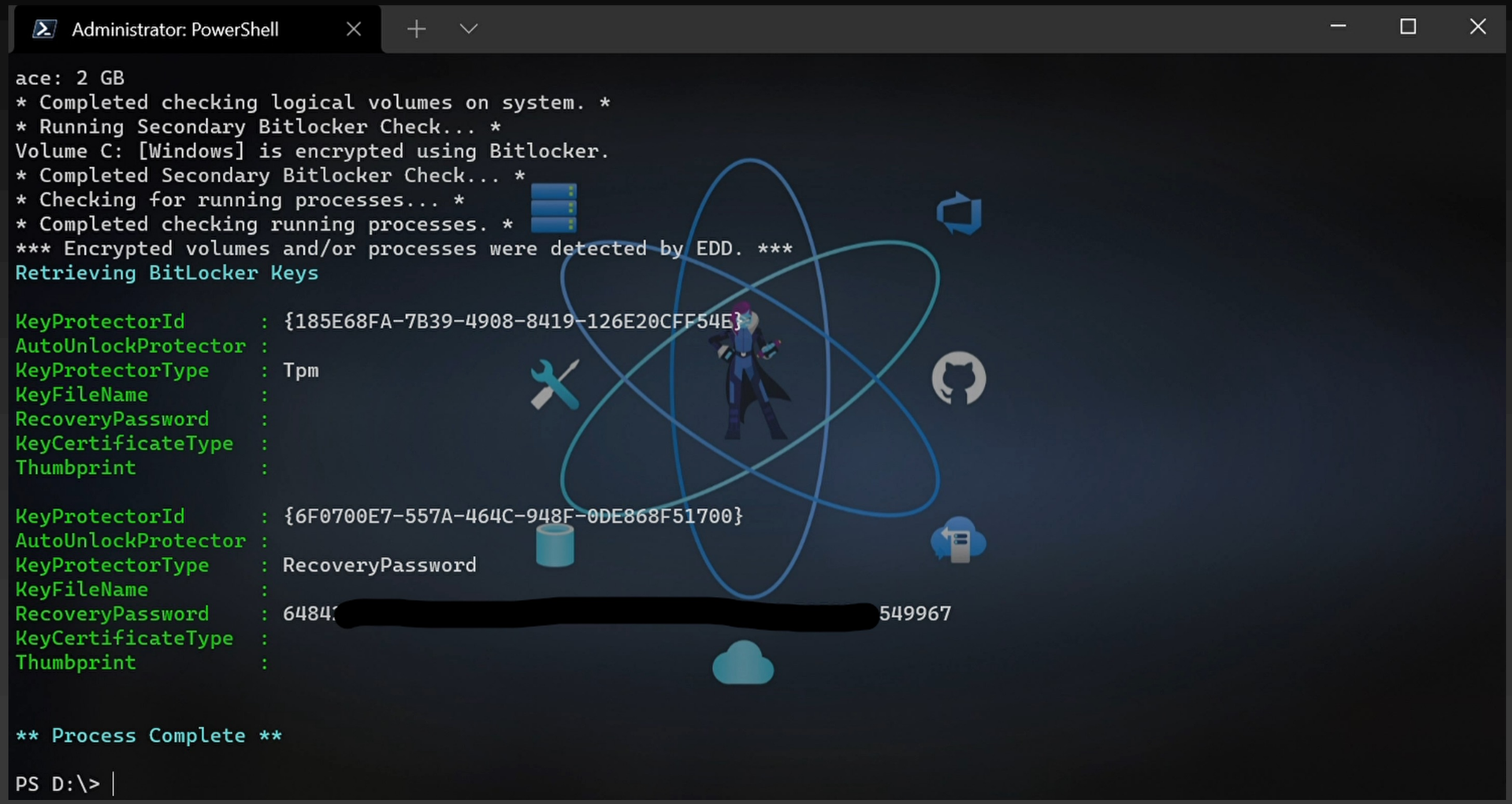
KAPE Modules (EDD) >>> .vhdx



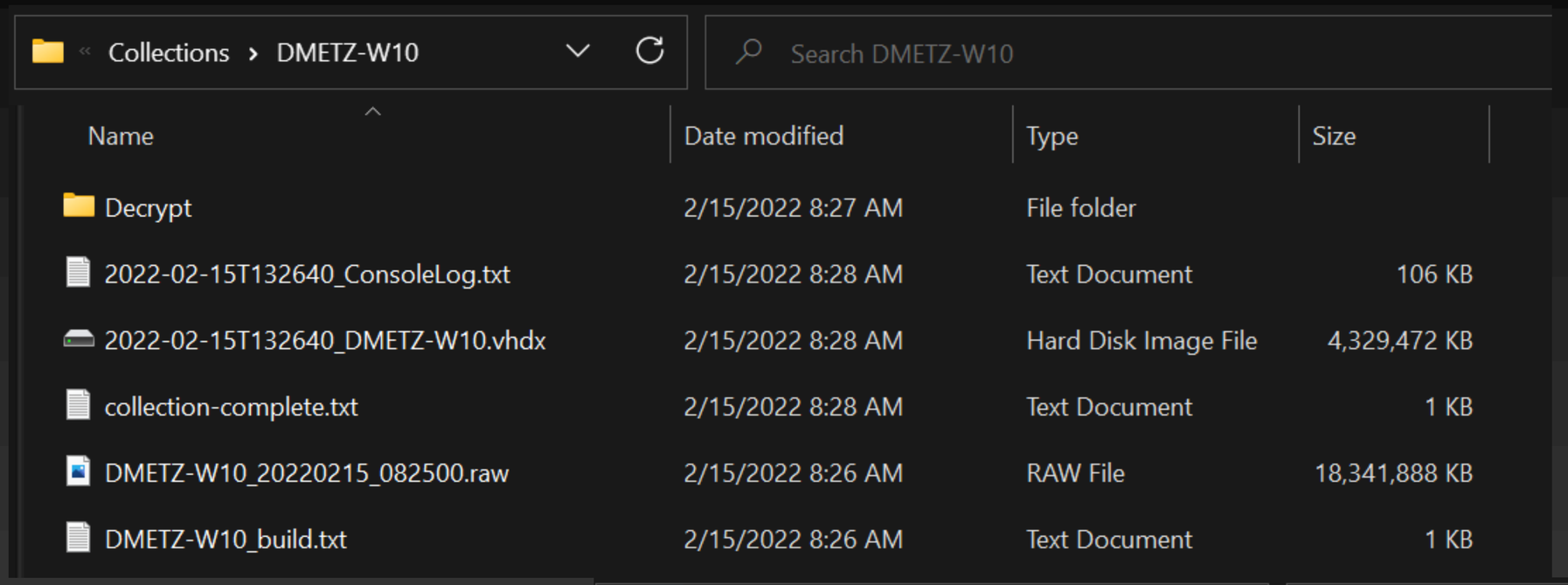
Encrypted Disk Detector (EDD)

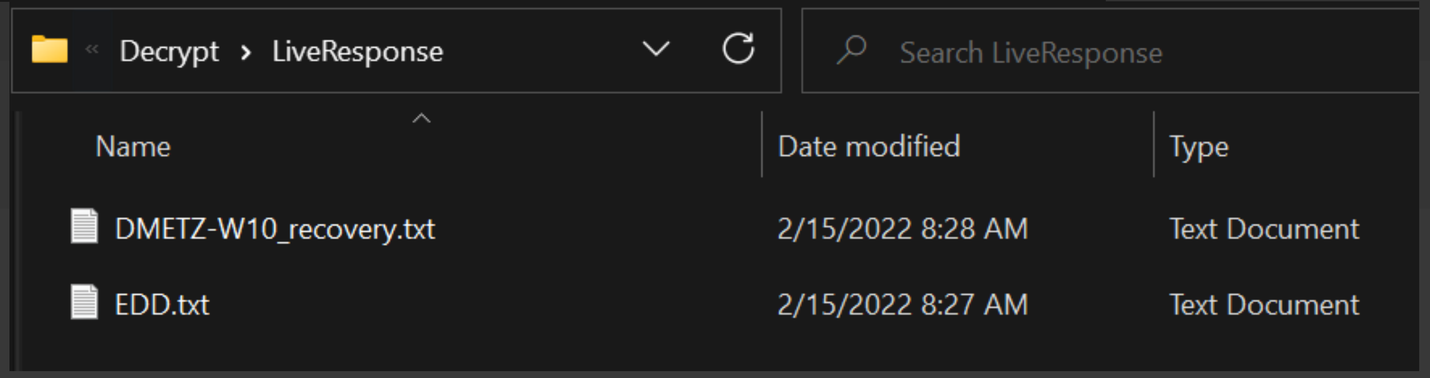


Bitlocker Recovery Key Extraction



Collection Output





Hardware Choices

15:30 Memory Acquisition

20:00 VHDX Created

25:48 Complete

1:45 Memory Acquisition

3:15 VHDX Created

3:55 Complete

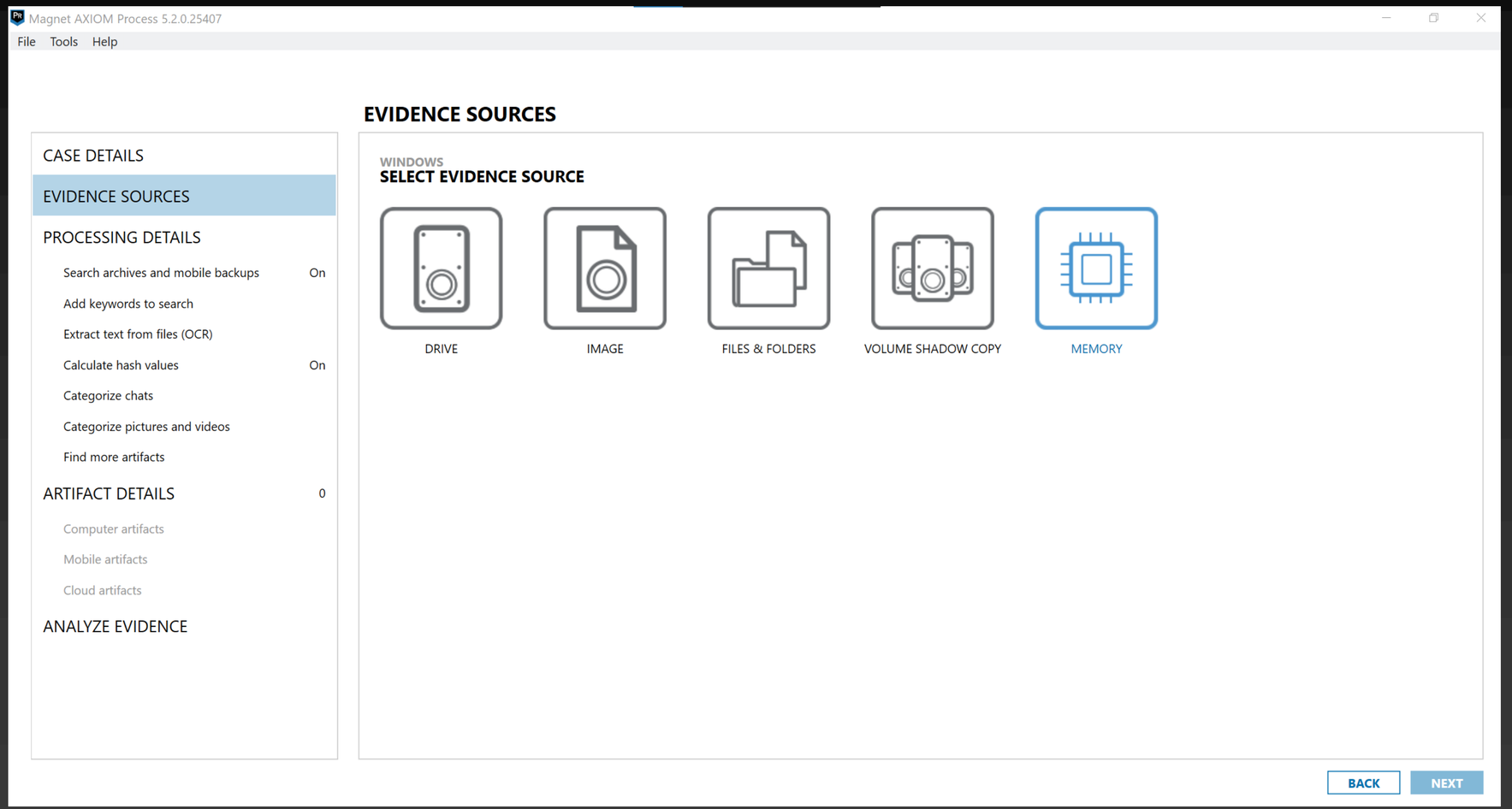
Additional PowerShell Resources

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.

MAGNET FORENSICS®

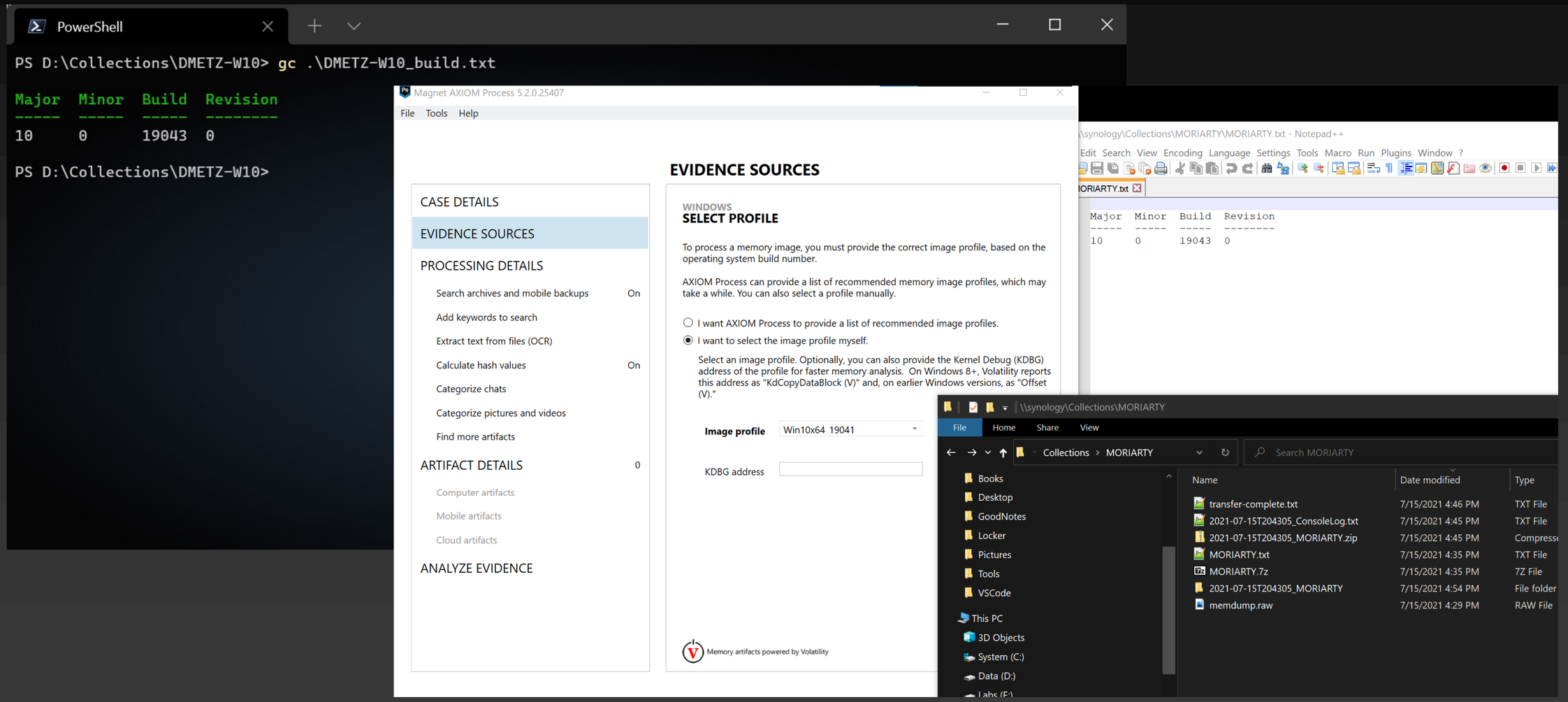
Evidence Processing Tips

Memory Processing

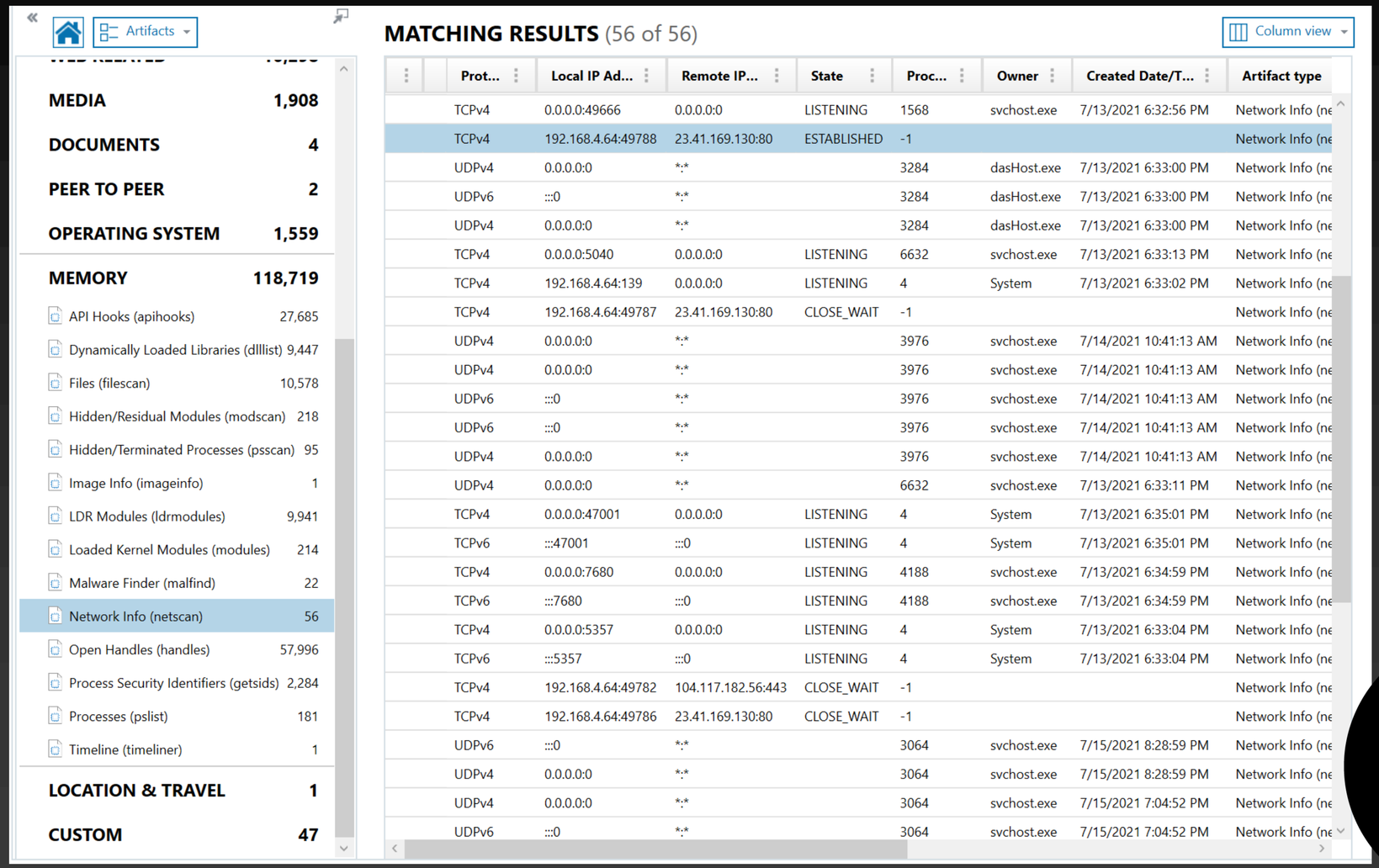


Memory Processing

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

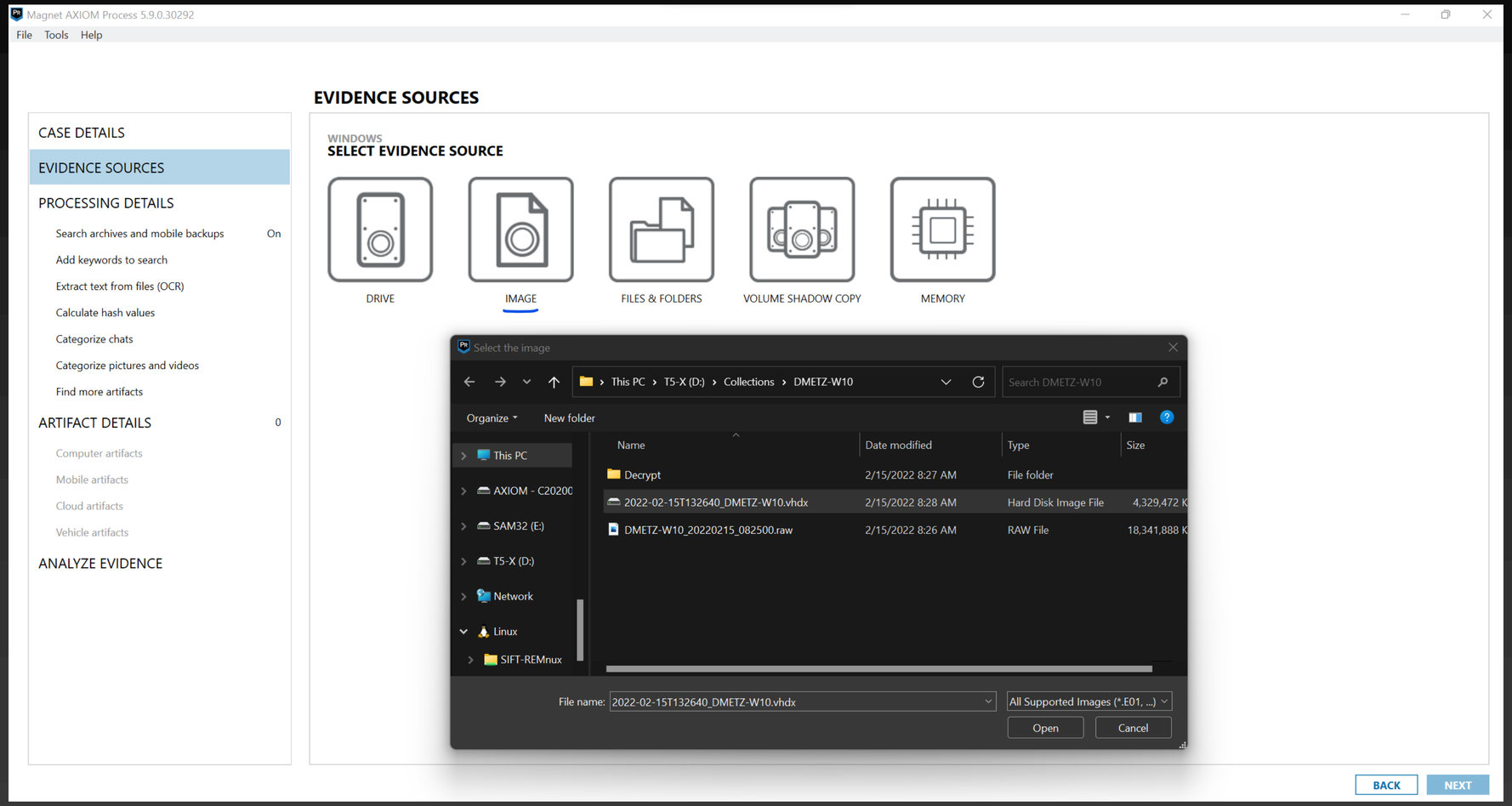


Memory Artifacts from Volatility



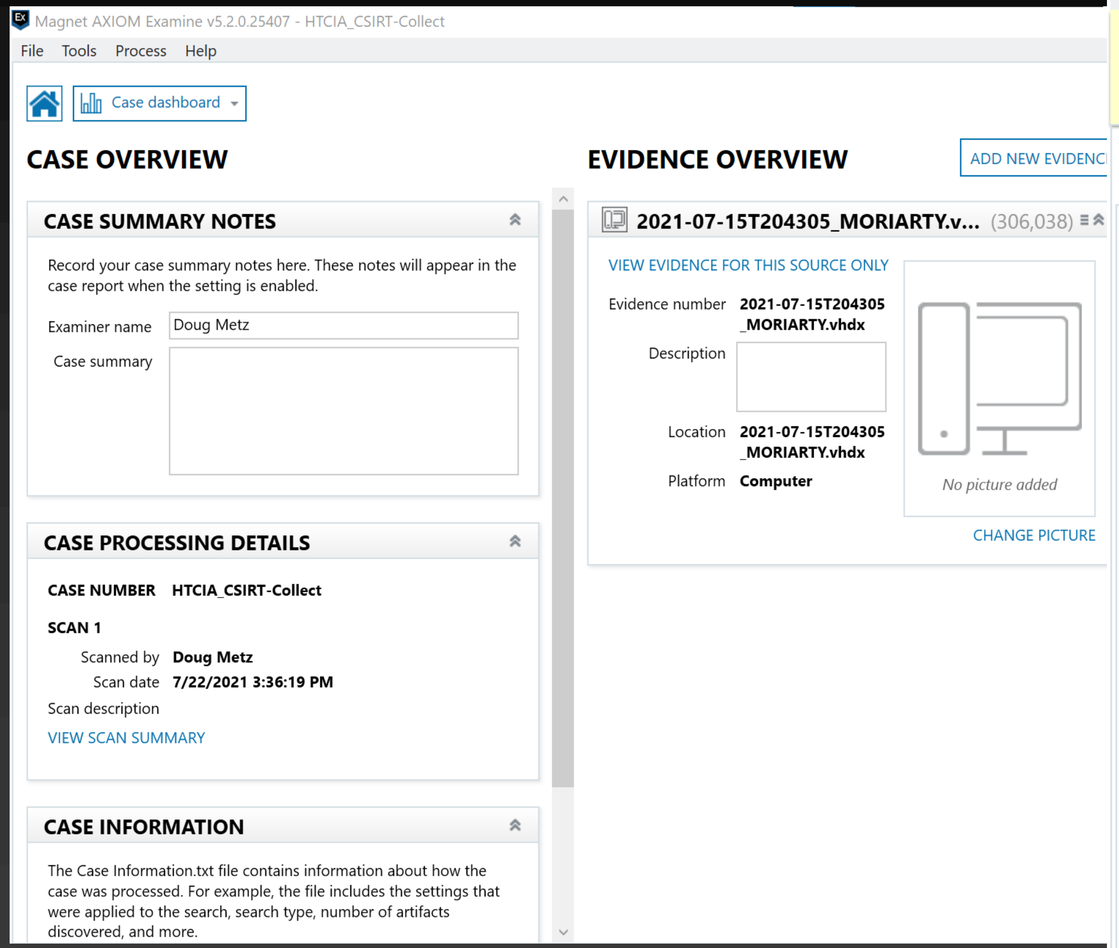
Prot...	Local IP Ad...	Remote IP...	State	Proc...	Owner	Created Date/T...	Artifact type
TCPv4	0.0.0.0:49666	0.0.0.0:0	LISTENING	1568	svchost.exe	7/13/2021 6:32:56 PM	Network Info (ne
TCPv4	192.168.4.64:49788	23.41.169.130:80	ESTABLISHED	-1			Network Info (ne
UDPv4	0.0.0.0:0	*:*		3284	dasHost.exe	7/13/2021 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 (ne
TCPv4	192.168.4.64:49786	23.41.169.130:80	CLOSE_WAIT	-1			Network Info (ne
UDPv6	:::0	*:*		3064	svchost.exe	7/15/2021 8:28:59 PM	Network Info (ne
UDPv4	0.0.0.0:0	*:*		3064	svchost.exe	7/15/2021 8:28:59 PM	Network Info (ne
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

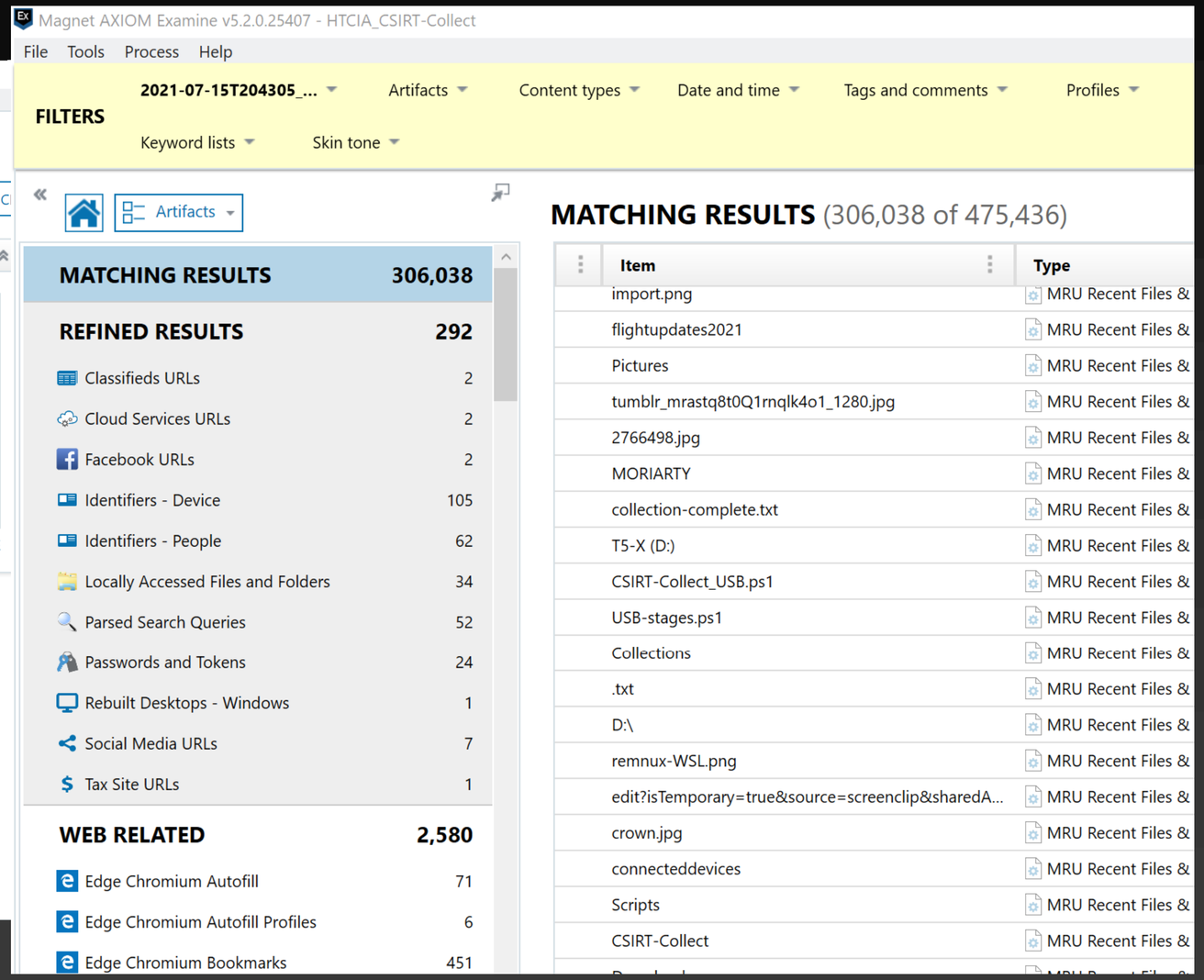
VMDK Image Processing



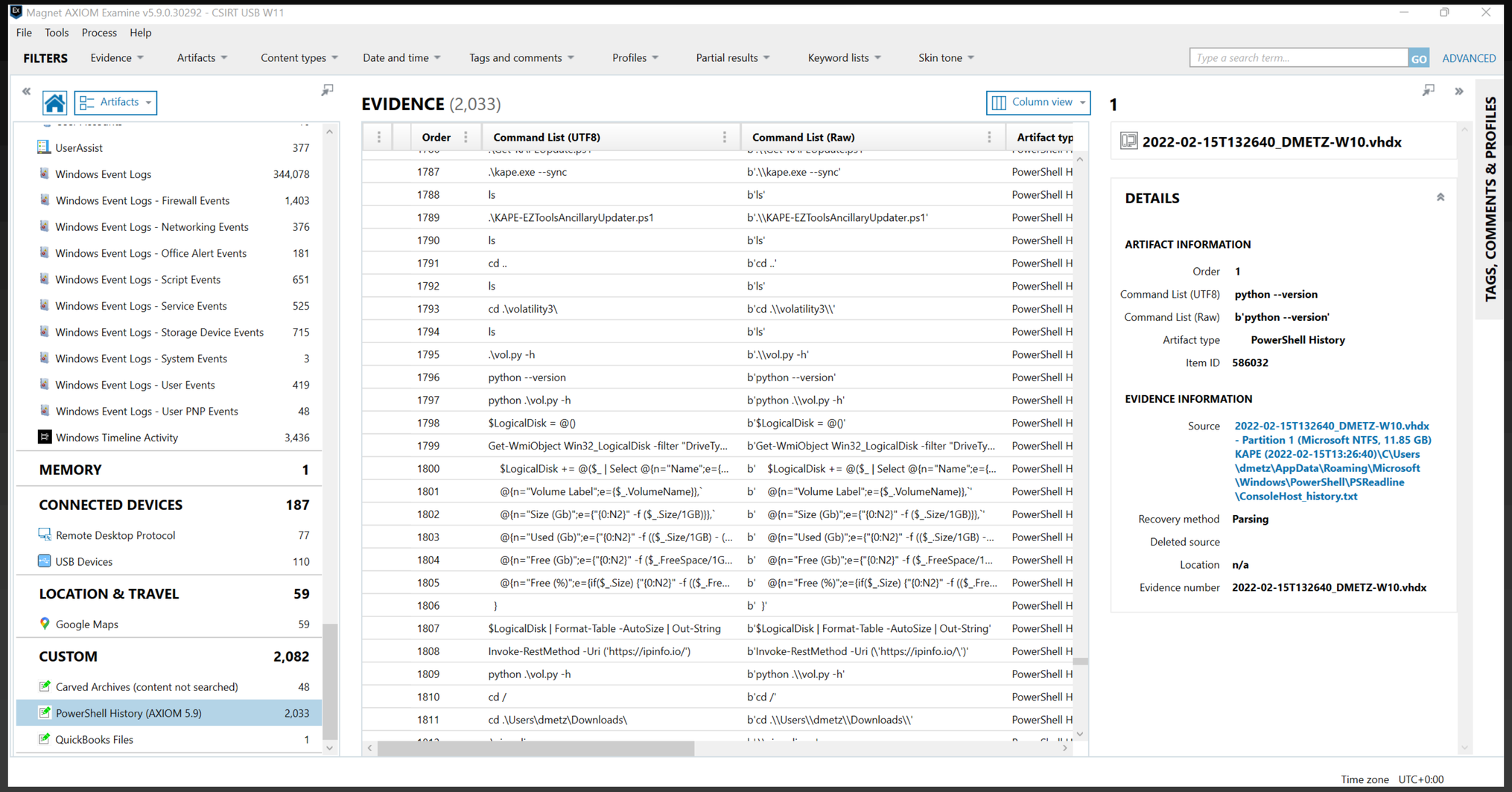
Computer > Windows > Load Evidence > IMAGE

Artifacts from Triage Image (VMDK)

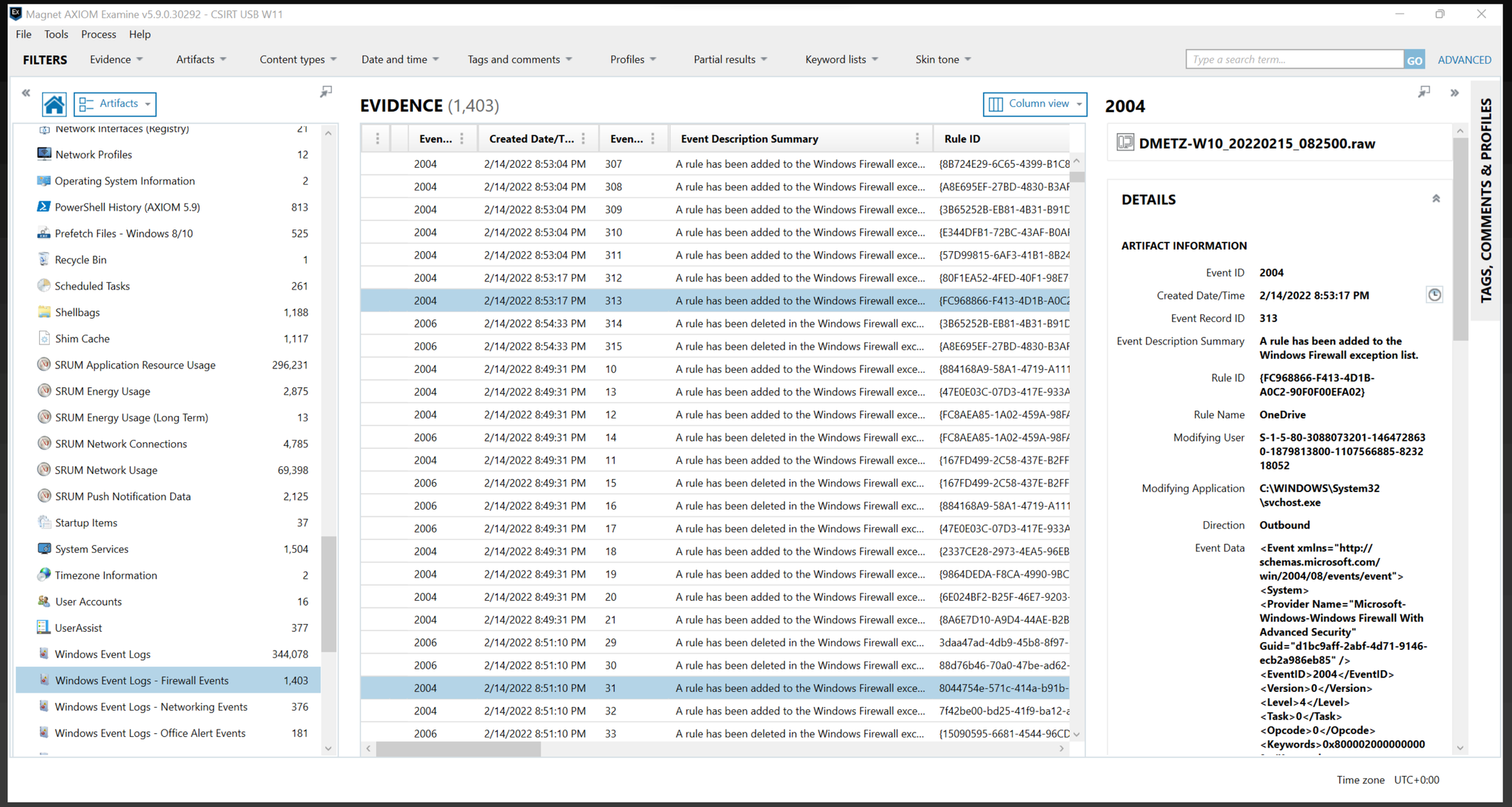




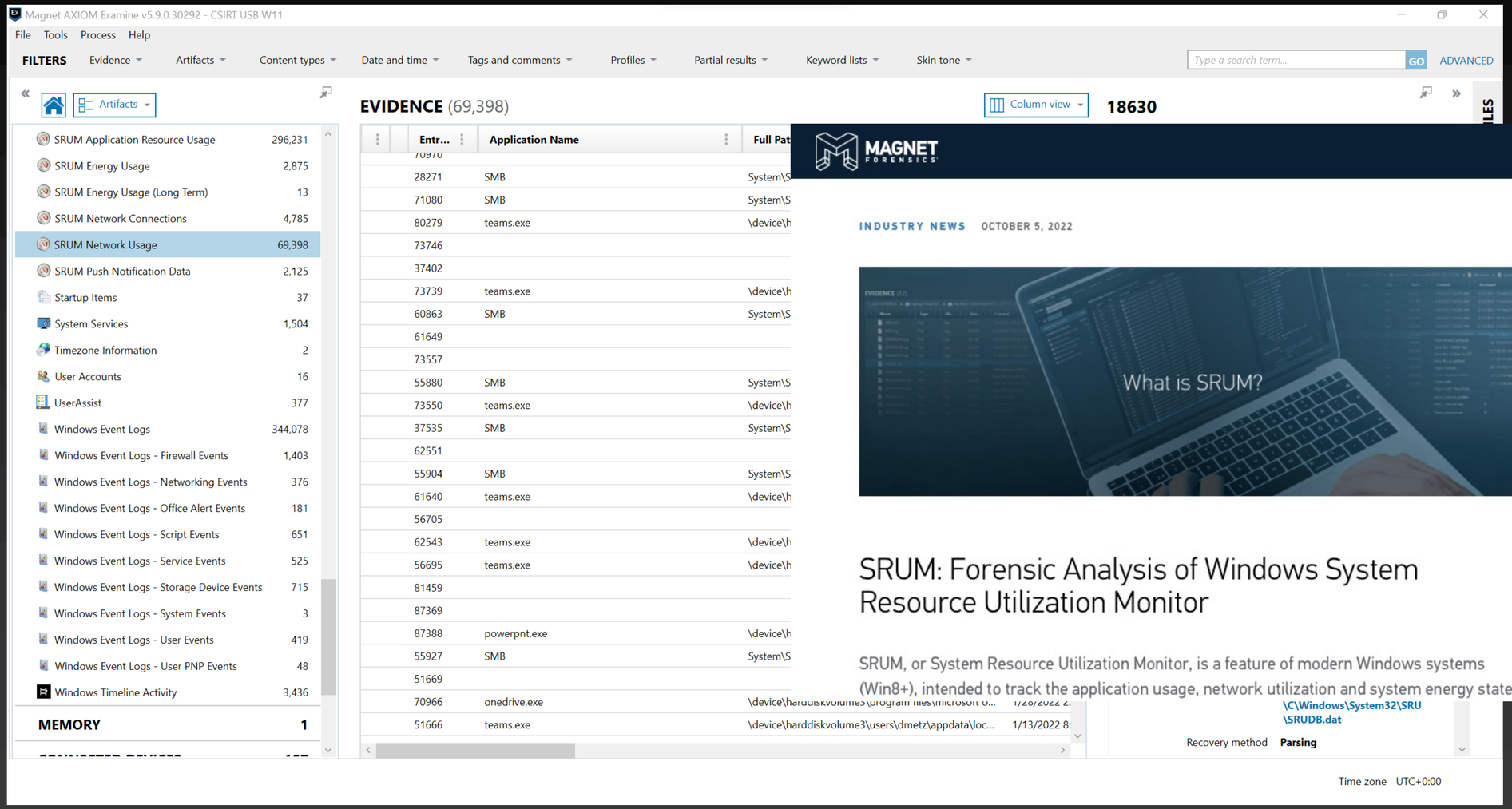
PowerShell History



Firewall Events

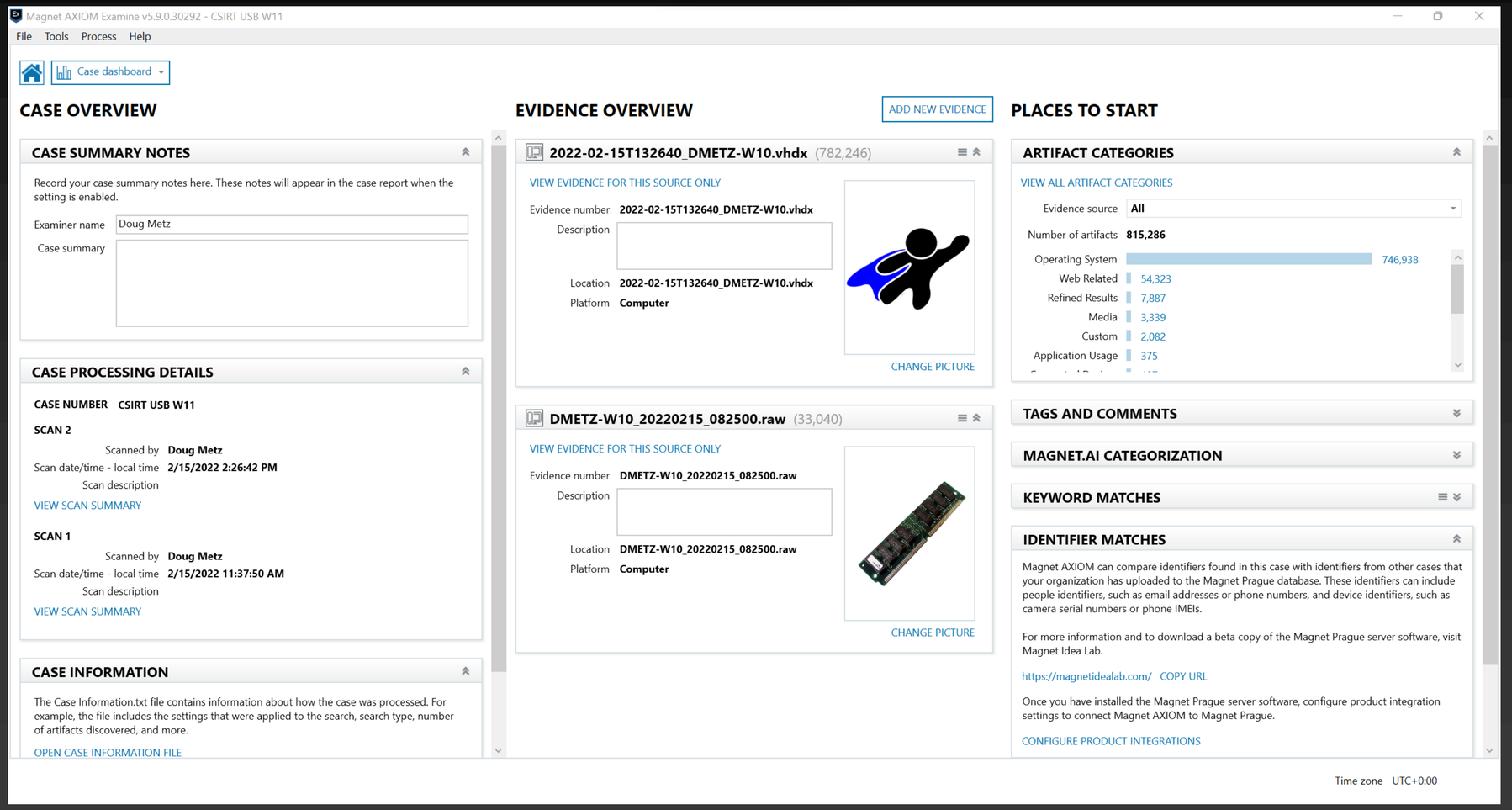


System Resource Usage Monitor (SRUM)

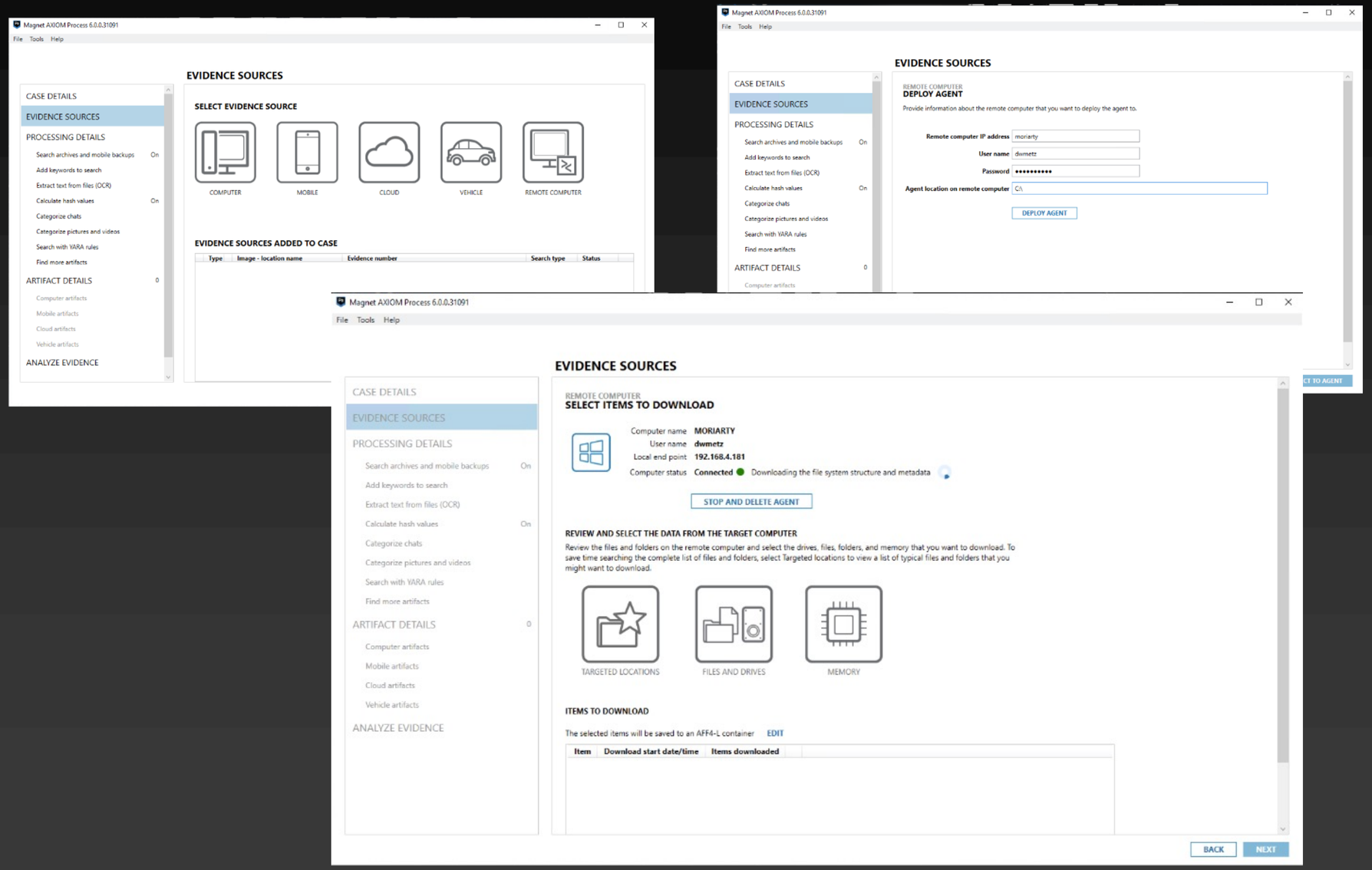


https://www.magnetforensics.com/blog/srum-forensic-analysis-of-windows-system-resource-utilization-monitor/

Offline Collections Processed – What's Next?



Collecting More with Axiom Cyber



Resources

CSIRT-Collect PowerShell: https://github.com/dwmetz/CSIRT-Collect

Magnet RAM Capture: 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

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

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

Blog: https://bakerstreetforensics.com

Thank You

https://github.com/dwmetz

@dwmetz

doug.metz@magnetforensics.com

https://bakerstreetforensics.com

https://infosec.exchange/@dwmetz