

# Free Tools for Triage Collections

Doug Metz

Professional Services Consultant, Magnet Forensics



# 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®

The screenshot shows a web browser window displaying the 'FREE TOOLS' section of the MAGNET Forensics support website. The URL in the address bar is https://support.magnetforensics.com/s/free-tools. The page features a dark header with the MAGNET Forensics logo and navigation links for HOME, KNOWLEDGE BASE, TECH SUPPORT, ARTIFACT EXCHANGE, and More. Below the header, the page title 'FREE TOOLS' is displayed in a large, bold, blue font. A sub-header states: 'We're proud to offer a number of free tools to help give you new ways to find evidence in your investigations. Help yourself to what's available and try it in your next examination.' The main content area contains three tool descriptions: 'MAGNET ACQUIRE' (version 2.47.0.28714, release date 2022-01-25), 'MAGNET SHIELD' (described as empowering frontline officers to collect and report on fleeting digital evidence), and 'MAGNET CHROMEBOOK ACQUISITION ASSISTANT' (version 1.06, release date 2021-11-21). Each tool entry includes a 'DOWNLOAD' button, a 'RELEASE NOTES' link, and a 'System Requirements' dropdown. To the right of the tools, there is a 'TOP ARTICLES' sidebar with links to 'FREE TOOLS' articles like 'Generate wordlists with the AXIOM Wordlist Generator' and 'Acquire Memory with MAGNET RAM Capture'. There is also a 'View All (20+)' link.

https://support.magnetforensics.com/s/free-tools

**FREE TOOLS**

We're proud to offer a number of free tools to help give you new ways to find evidence in your investigations. Help yourself to what's available and try it in your next examination.

**MAGNET ACQUIRE**  
VERSION: 2.47.0.28714 , RELEASE DATE: 2022-01-25

Magnet ACQUIRE helps you quickly and easily acquire forensic images of any iOS or Android device, hard drives, and removable media.

[DOWNLOAD](#)

[RELEASE NOTES](#)

[System Requirements](#)

---

**MAGNET SHIELD**

Empower frontline officers to collect and report on fleeting digital evidence. Maintain privacy and build trust with the public while capturing crucial but fleeting digital evidence from consenting victims and witnesses.

[DOWNLOAD](#)

[LEARN MORE](#)

---

**MAGNET CHROMEBOOK ACQUISITION ASSISTANT**  
VERSION: 1.06 , RELEASE DATE: 2021-11-21

The Magnet Chromebook Acquisition Assistant (MCAA) helps you acquire a logical image from a Chromebook, without requiring it to be in developer mode.

**TOP ARTICLES**

[FREE TOOLS](#)

[Generate wordlists with the AXIOM Wordlist Generator](#)

[Acquire Memory with MAGNET RAM Capture](#)

[System requirements: Magnet ACQUIRE](#)

[Prepare iOS devices for acquisition](#)

[Magnet ACQUIRE supported Android devices](#)

[View All \(20+\)](#)

# 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



The screenshot shows the KAPE v1.1.0.1 graphical user interface. The left side of the window is titled "Targets" and contains a table of collected artifacts. The right side is titled "Modules" and contains a table of processing routines. Both sections have dropdown menus for "Target source" and "Target destination" (or "Module destination") and various checkboxes for "Flush", "Add %d", "Add %m", and "Zip".

**Targets (Double-click to edit a target)**

Selected	Name	Folder	Description
<input checked="" type="checkbox"/>	Kali	WSL	Kali on Windows Subsystem
<input checked="" type="checkbox"/>	KapeTriage	Compound	Kape Triage collections th...
<input type="checkbox"/>	Kaseya	Apps	Kaseya Data
<input type="checkbox"/>	LinuxOnWindowsProfileFiles	Windows	Linux on Windows Profile ...
<input type="checkbox"/>	LNKFilesAndJumpLists	Windows	LNK Files and jump lists
<input type="checkbox"/>	LogFiles	Windows	LogFiles (includes SUM)
<input type="checkbox"/>	LogMeIn	Apps	LogMeIn Data
<input type="checkbox"/>	MacriumDefect	Apps	Macrium Defect

**Modules (Double-click to edit a module)**

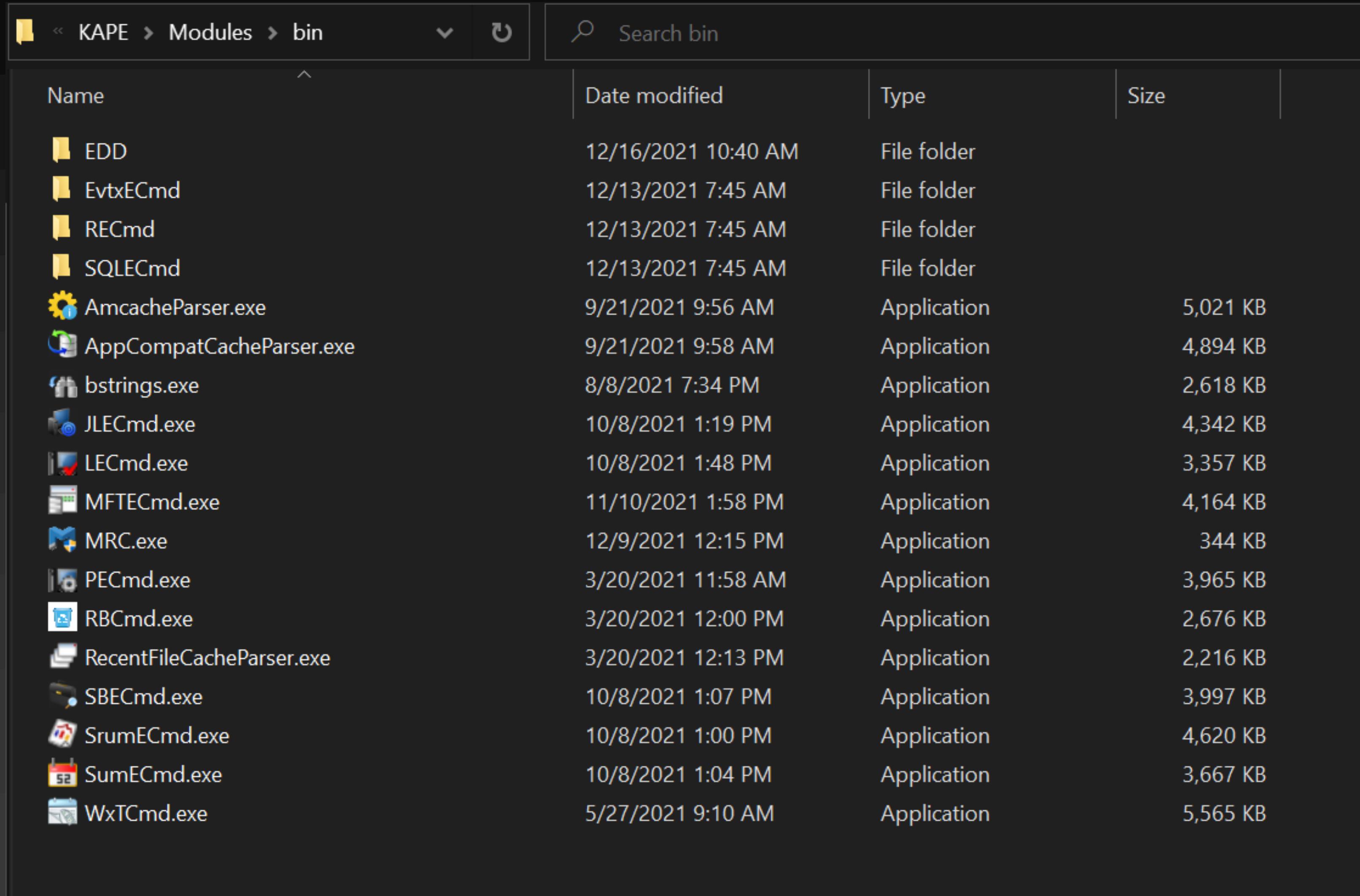
Selected	Name	Folder	Category	Description
<input checked="" type="checkbox"/>	MagnetForensics_EDD	Apps	LiveResponse	Checks the local physi...
<input type="checkbox"/>	MagnetForensics_RAMCapture	Apps	Memory	Magnet RAM Capture ...

**Current command line**

```
.\kape.exe --tsource C: --tdest D:\KAPE-OUT --target KapeTriage --mdest D:\KAPE-OUT\DECRYPT --mflush --module MagnetForensics_EDD --gui
```

Buttons at the bottom include "Copy command", "Sync with GitHub", and "Execute!"

# Tools in the /bin - BYOE



The screenshot shows a file explorer window with the following details:

- Path: KAPE > Modules > bin
- Search bar: Search bin
- File list:

Name	Date modified	Type	Size
EDD	12/16/2021 10:40 AM	File folder	
EvtxECmd	12/13/2021 7:45 AM	File folder	
RECmd	12/13/2021 7:45 AM	File folder	
SQLECmd	12/13/2021 7:45 AM	File folder	
AmcacheParser.exe	9/21/2021 9:56 AM	Application	5,021 KB
AppCompatCacheParser.exe	9/21/2021 9:58 AM	Application	4,894 KB
bstrings.exe	8/8/2021 7:34 PM	Application	2,618 KB
JLECmd.exe	10/8/2021 1:19 PM	Application	4,342 KB
LECmd.exe	10/8/2021 1:48 PM	Application	3,357 KB
MFTECmd.exe	11/10/2021 1:58 PM	Application	4,164 KB
MRC.exe	12/9/2021 12:15 PM	Application	344 KB
PECmd.exe	3/20/2021 11:58 AM	Application	3,965 KB
RBCmd.exe	3/20/2021 12:00 PM	Application	2,676 KB
RecentFileCacheParser.exe	3/20/2021 12:13 PM	Application	2,216 KB
SBECmd.exe	10/8/2021 1:07 PM	Application	3,997 KB
SrumECmd.exe	10/8/2021 1:00 PM	Application	4,620 KB
SumECmd.exe	10/8/2021 1:04 PM	Application	3,667 KB
WxTCmd.exe	5/27/2021 9:10 AM	Application	5,565 KB

# 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

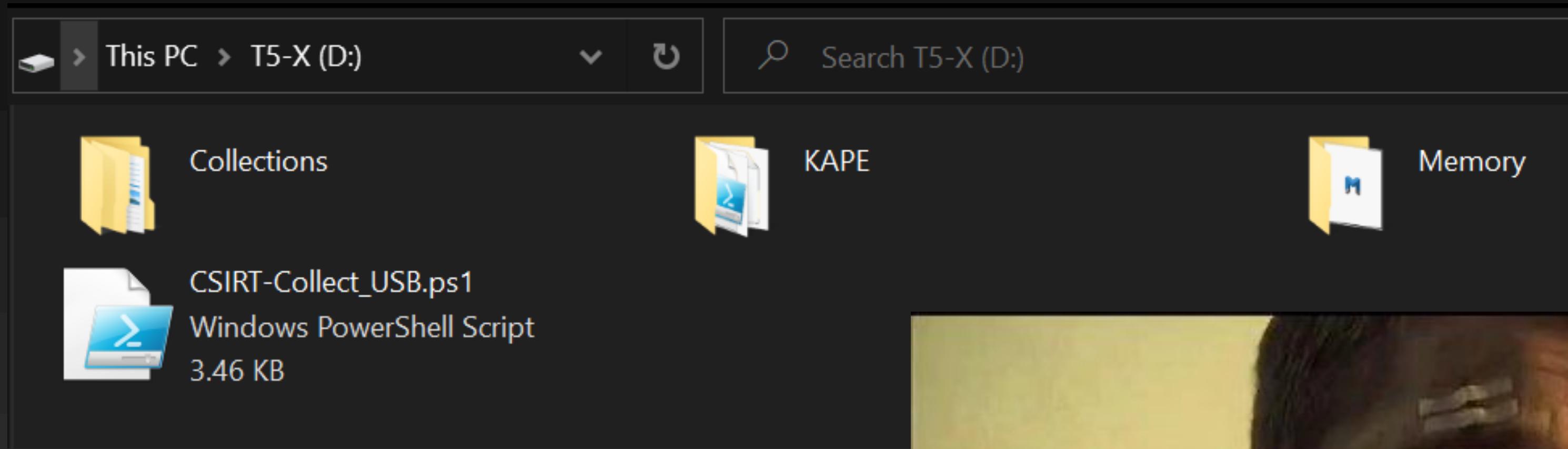
# Place "EDDv310.exe", "EDDv310.exe.config" files into "Modules\bin\EDD"

Reload Generate GUID

KAPE > Modules > Apps

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

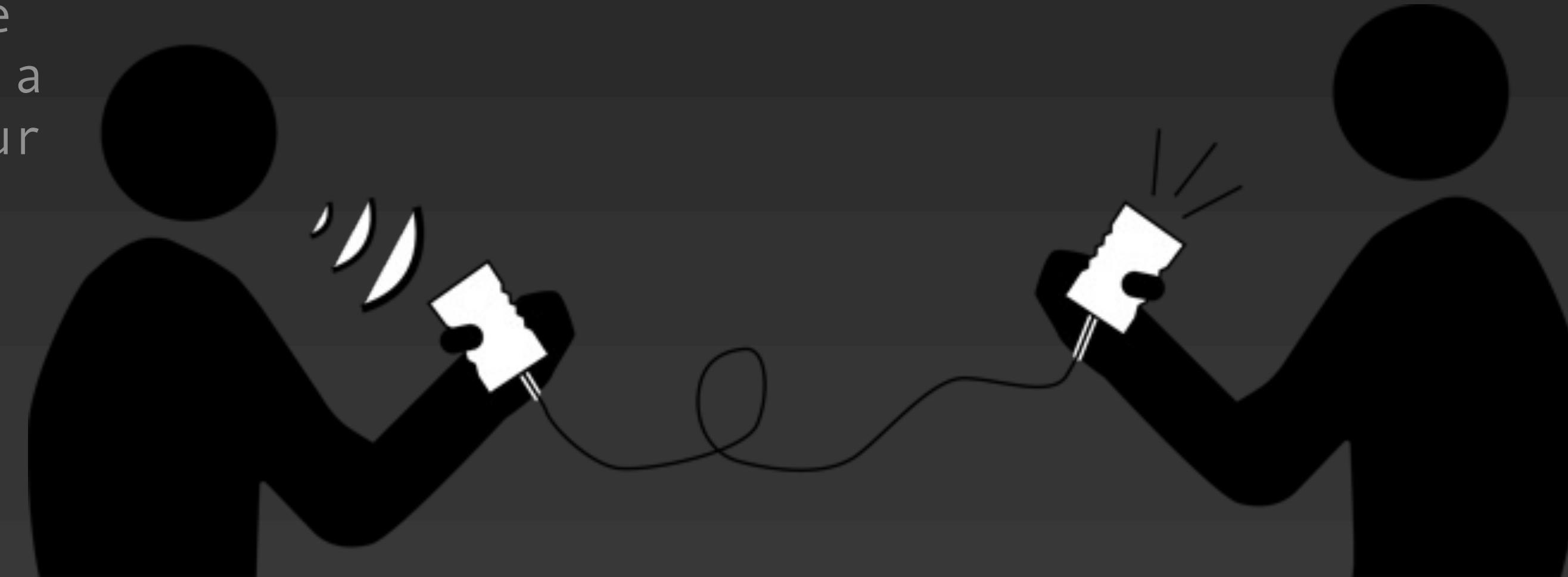
# Folder Layout



# 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 change 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 ## transfer evidence to share
84 Set-Location C:\Temp\Kape
85 robocopy . "\\\Synology\Collections\$env:COMPUTERNAME"
86
87 ## delete the local directory and contents
88 Write-Host -Fore Green "Removing temporary files"
89 Set-Location C:\TEMP
90 Remove-Item -LiteralPath "C:\temp\KAPE" -Force -Recurse
91 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

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

Collection Compressed:  
688MB

~6 GB

Full memory acquisition:  
16 GB

Data management on endpoints helps to preserve disk space

Compressed memory image:  
5 GB

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



# CSIRT-Collect [USB]

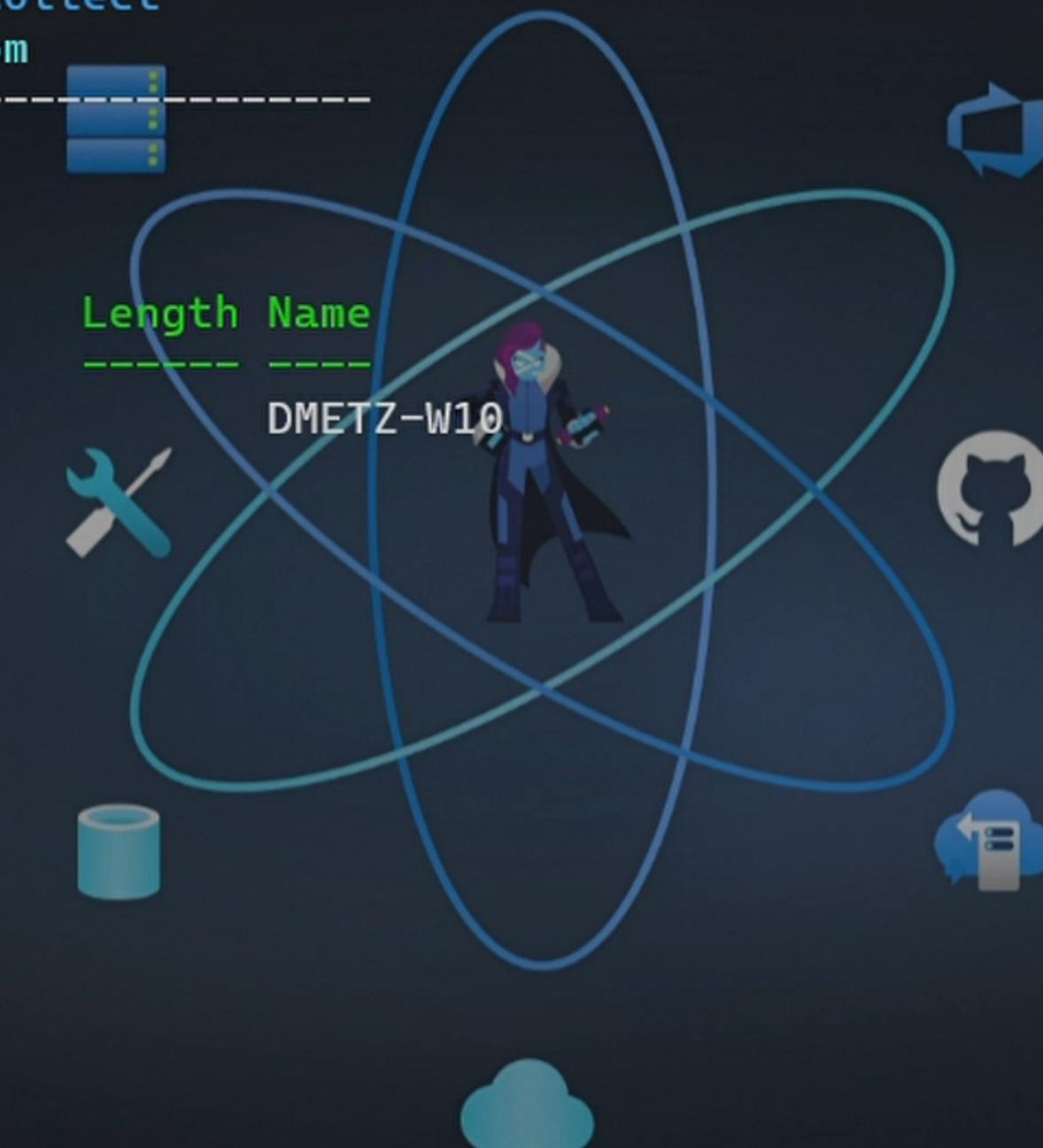
*Script Walk Through*

# Memory Collection

Administrator: PowerShell

```
PS D:\> & '.\CSIRT-Collect USB.ps1'

-----  
CSIRT IR Collection Script - USB, v2.2  
https://github.com/dwmetz/CSIRT-Collect  
@dwmetz | bakerstreetforensics.com  
-----  
Directory: D:\Collections  
Mode           LastWriteTime  
----           -----  
d--- 2/11/2022  2:34 PM  
Initiating Magnet Ram Capture.  
Capturing memory...  
This process may take several minutes...
```



# Build Info >>> KAPE Triage

```
0.56%: Files remaining to be cop X + ▾ - □ ×  
-----  
Directory: D:\Collections  
  
Mode           LastWriteTime  
----  
d---          2/11/2022 2:34 PM  
Initiating Magnet Ram Capture.  
Capturing memory...  
This process may take several minutes...  
Determining OS build info...  
Cleaning up memory collection...  
Collecting OS artifacts...  
KAPE version 1.1.0.1 Author: Eric Zimmerman (kapec@kroll.com)  
  
KAPE directory: D:\Kape  
Command line: --tsource C: --tdest Collections\DMETZ-W10 --target KapeTriage --vhdx DMETZ-W10 --zv false --module Magnet  
Forensics_EDD --mdest Collections\DMETZ-W10\Decrypt  
  
System info: Machine name: DMETZ-W10, 64-bit: True, User: dmetz OS: Windows10 (10.0.19044)  
  
Using Target operations  
Found 14 targets. Expanding targets to file list...  
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!  
Found 1,261 files in 7.074 seconds. Beginning copy...
```

# KAPE Modules (EDD) >>> .vhdx

```
Preparing VHDX container... × + ▾ - □ ×

df84\ActivitiesCache.db-shm' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\AAD.9b34a
814-50a1-4e9e-a5e6-f03b6c21df84\ActivitiesCache.db-shm'. Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\AAD.9b34a814-50a1-4e9e-a5e6-f03b6c21
df84\ActivitiesCache.db-wal' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\AAD.9b34a
814-50a1-4e9e-a5e6-f03b6c21df84\ActivitiesCache.db-wal'. Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db'
to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db'.
Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db-
shm' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.
db-shm'. Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db-
wal' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.
db-wal'. Hashing source file...

Copied 1,160 (Deduplicated: 101) out of 1,261 files in 76.7647 seconds. See '*_CopyLog.csv' in the VHD(X)/Zip located in
'D:\Collections\DMETZ-W10' for copy details

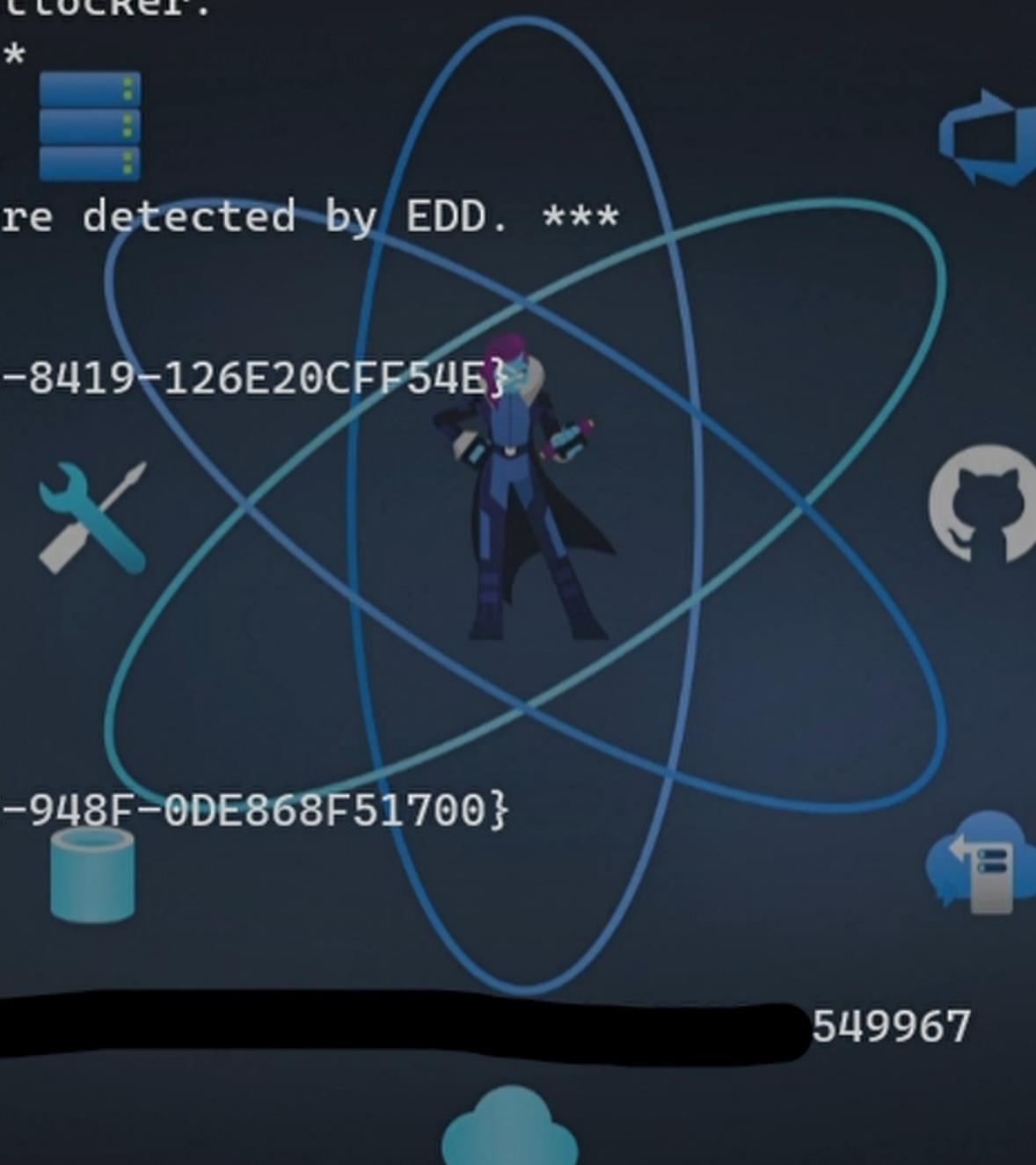
Using Module operations
Setting --msource to 'D:\Collections\DMETZ-W10' since --msource was not provided
Creating module destination directory 'D:\Collections\DMETZ-W10\Decrypt'
Found processor 'Executable: EDD\EDDv302.exe, Cmd line: /batch >> %destinationDirectory%, Export: txt, A
ppend: False'!
Discovered 1 processor to run.
Executing modules with file masks...
Executing remaining modules...
Running 'EDD\EDDv302.exe': /batch >> D:\Collections\DMETZ-W10\Decrypt\LiveResponse
Executed 1 processor in 2.6672 seconds
Initializing VHDX creation. This may take a while...
```

# Encrypted Disk Detector (EDD)

```
Administrator: PowerShell + - X
VHDX file 'D:\Collections\DMETZ-W10\2022-02-11T193611_DMETZ-W10.vhdx' created.
Cleaning up files in 'D:\Collections\DMETZ-W10'...
Total execution time: 122.9963 seconds

Encrypted Disk Detector v3.0.2
Copyright (c) 2009-2021 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is governed by the End User License Agreement available at www.magnetforensics.com/legal. //
* Checking physical drives on system... *
Checking PhysicalDrive1 - Samsung Portable SSD T5 SCSI Disk Device (1,000 GB) - Status: OK
Checking PhysicalDrive2 - USB Flash Disk USB Device (2 GB) - Status: OK
Checking PhysicalDrive0 - SKHynix_HFS512GDE9X081N (512 GB) - Status: OK
* Completed checking physical drives on system. *
* Now checking logical volumes on system... *
Drive C: [Label: Windows] (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 511 GB, Free Space: 78 GB
Drive D: [Label: T5-X] (PhysicalDrive1), Drive Type: Fixed, Filesystem: exFAT, Size: 1,000 GB, Free Space: 828 GB
Drive F: [Label: AXIOM - C20200122001664] (PhysicalDrive2), Drive Type: Removable, Filesystem: NTFS, Size: 2 GB, Free Space: 2 GB
* Completed checking logical volumes on system. *
* Running Secondary Bitlocker Check... *
Volume C: [Windows] is encrypted using Bitlocker.
* Completed Secondary Bitlocker Check... *
* Checking for running processes... *
* Completed checking running processes. *
*** Encrypted volumes and/or processes were detected by EDD. ***
Retrieving BitLocker Keys
```

# Bitlocker Recovery Key Extraction



```
Administrator: PowerShell
ace: 2 GB
* Completed checking logical volumes on system. *
* Running Secondary Bitlocker Check... *
Volume C: [Windows] is encrypted using Bitlocker.
* Completed Secondary Bitlocker Check... *
* Checking for running processes... *
* Completed checking running processes. *
*** Encrypted volumes and/or processes were detected by EDD. ***
Retrieving BitLocker Keys

KeyProtectorId      : {185E68FA-7B39-4908-8419-126E20CFF54E}
AutoUnlockProtector :
KeyProtectorType    : Tpm
KeyFileName         :
RecoveryPassword   :
KeyCertificateType :
Thumbprint          :

KeyProtectorId      : {6F0700E7-557A-464C-948F-0DE868F51700}
AutoUnlockProtector :
KeyProtectorType    : RecoveryPassword
KeyFileName         :
RecoveryPassword   : 64841[REDACTED]549967
KeyCertificateType :
Thumbprint          :

** Process Complete **

PS D:\> |
```

# Collection Output

Collections > DMETZ-W10			
Name	Date modified	Type	Size
Decrypt	2/15/2022 8:27 AM	File folder	
2022-02-15T132640_ConsoleLog.txt	2/15/2022 8:28 AM	Text Document	106 KB
2022-02-15T132640_DMETZ-W10.vhdx	2/15/2022 8:28 AM	Hard Disk Image File	4,329,472 KB
collection-complete.txt	2/15/2022 8:28 AM	Text Document	1 KB
DMETZ-W10_20220215_082500.raw	2/15/2022 8:26 AM	RAW File	18,341,888 KB
DMETZ-W10_build.txt	2/15/2022 8:26 AM	Text Document	1 KB

Decrypt > LiveResponse			
Name	Date modified	Type	
DMETZ-W10_recovery.txt	2/15/2022 8:28 AM	Text Document	
EDD.txt	2/15/2022 8:27 AM	Text Document	

# 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

Magnet AXIOM Process 5.2.0.25407

File Tools Help

**EVIDENCE SOURCES**

**WINDOWS SELECT EVIDENCE SOURCE**

	DRIVE	IMAGE	FILES & FOLDERS	VOLUME SHADOW COPY	MEMORY
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					

**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

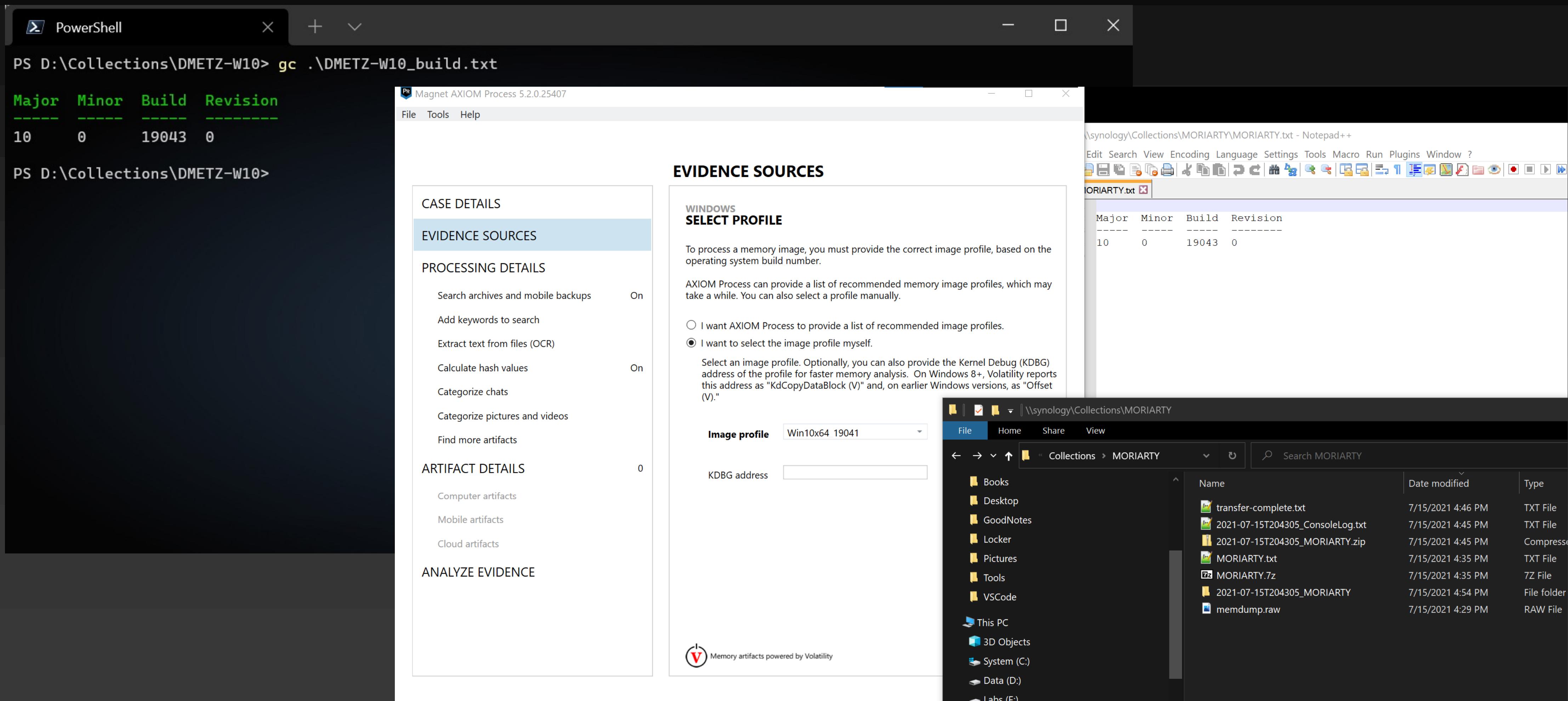
Cloud artifacts

**ANALYZE EVIDENCE**

BACK      NEXT

# Memory Processing

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



# Memory Artifacts from Volatility

« Artifacts ▾

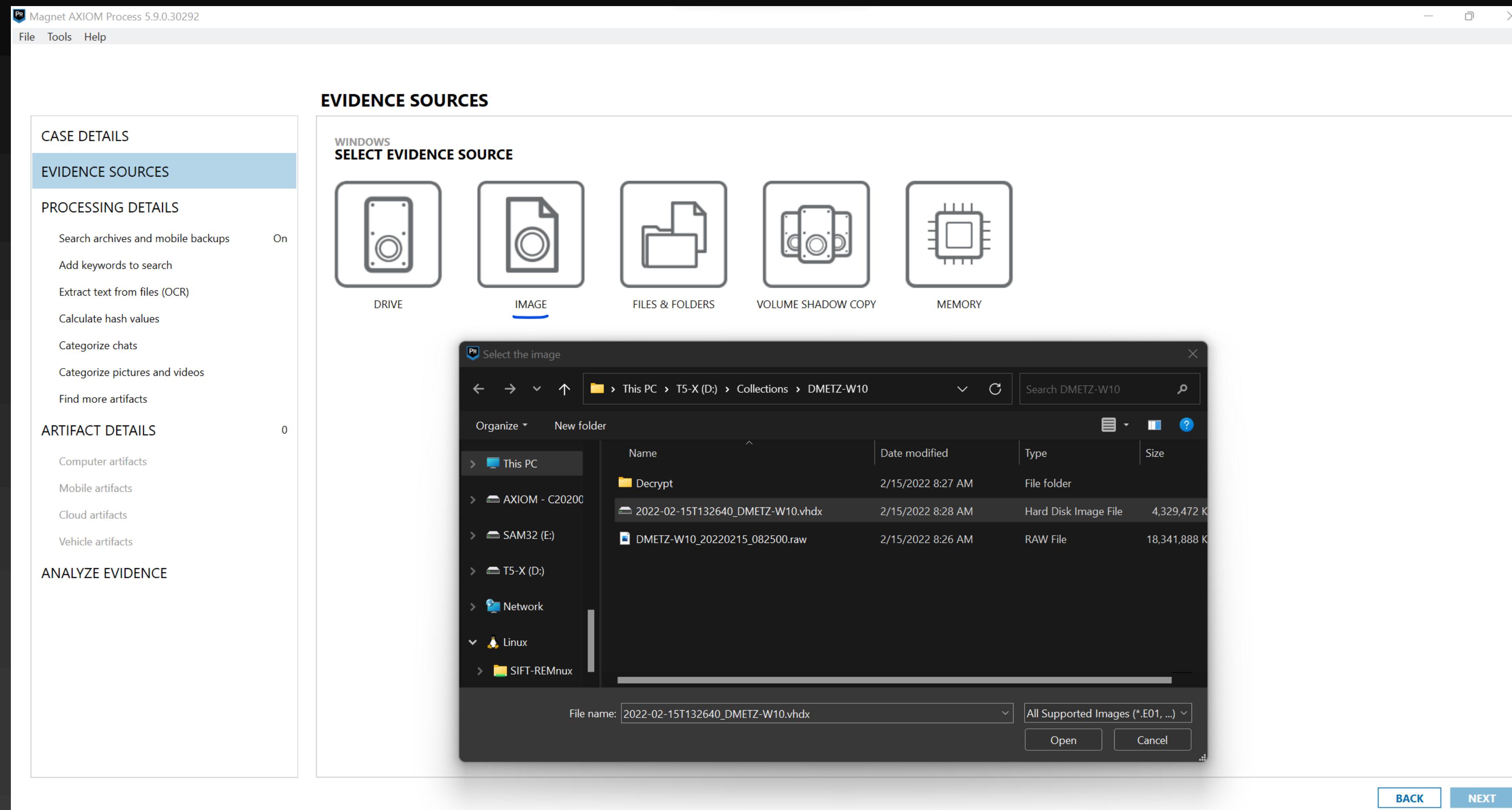
### MATCHING RESULTS (56 of 56)

Column view ▾

	Prot...	Local IP Ad...	Remote IP...	State	Proc...	Owner	Created Date/T...	Artifact type
TCPv4	0.0.0.0:49666	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:	*:*			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:	*:*			3284	dasHost.exe	7/13/2021 6:33:00 PM	Network Info (ne
TCPv4	0.0.0.0:5040	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		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:	*:*			3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
UDPv4	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:	*:*			3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
UDPv4	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		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		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		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:	*:*			3064	svchost.exe	7/15/2021 8:28:59 PM	Network Info (ne
UDPv4	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)

The screenshot displays two windows of Magnet AXIOM Examine software, version v5.2.0.25407, showing artifacts from a triage image (VMDK).

**CASE OVERVIEW**

**EVIDENCE OVERVIEW**

**MATCHING RESULTS (306,038 of 475,436)**

Item	Type
import.png	MRU Recent Files &
flightupdates2021	MRU Recent Files &
Pictures	MRU Recent Files &
tumblr_mrastq8t0Q1rnqlk4o1_1280.jpg	MRU Recent Files &
2766498.jpg	MRU Recent Files &
MORIARTY	MRU Recent Files &
collection-complete.txt	MRU Recent Files &
T5-X (D:)	MRU Recent Files &
CSIRT-Collect_USB.ps1	MRU Recent Files &
USB-stages.ps1	MRU Recent Files &
Collections	MRU Recent Files &
.txt	MRU Recent Files &
D:\	MRU Recent Files &
remnux-WSL.png	MRU Recent Files &
edit?isTemporary=true&source=screenclip&sharedA...	MRU Recent Files &
crown.jpg	MRU Recent Files &
connecteddevices	MRU Recent Files &
Scripts	MRU Recent Files &
CSIRT-Collect	MRU Recent Files &
Default	MRU Recent Files &

# PowerShell History

Magnet AXIOM Examine v5.9.0.30292 - CSIRT USB W11

File Tools Process Help

FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone Type a search term... GO ADVANCED

**EVIDENCE (2,033)**

Column view

Order	Command List (UTF8)	Command List (Raw)	Artifact type
1787	.\\kape.exe --sync	b'\\kape.exe --sync'	PowerShell H
1788	ls	b'ls'	PowerShell H
1789	.\\KAPE-EZToolsAncillaryUpdater.ps1	b'\\KAPE-EZToolsAncillaryUpdater.ps1'	PowerShell H
1790	ls	b'ls'	PowerShell H
1791	cd ..	b'cd ..'	PowerShell H
1792	ls	b'ls'	PowerShell H
1793	cd .\\volatility3\\	b'cd .\\volatility3\\'	PowerShell H
1794	ls	b'ls'	PowerShell H
1795	.\\vol.py -h	b'\\vol.py -h'	PowerShell H
1796	python --version	b'python --version'	PowerShell H
1797	python .\\vol.py -h	b'python .\\vol.py -h'	PowerShell H
1798	\$LogicalDisk = @()	b'\$LogicalDisk = @()'	PowerShell H
1799	Get-WmiObject Win32_LogicalDisk -filter "DriveTy...	b'Get-WmiObject Win32_LogicalDisk -filter "DriveTy..."	PowerShell H
1800	\$LogicalDisk += @(\$_   Select @{n="Name";e={...}}`n)	b'\$LogicalDisk += @(\$_   Select @{n="Name";e={...}}`n)	PowerShell H
1801	@{n="Volume Label";e={\$_.VolumeName}}`n	b'@{n="Volume Label";e={\$_.VolumeName}}`n	PowerShell H
1802	@{n="Size (Gb)";e={"(0:N2)" -f (\$_.Size/1GB)}}`n	b'@{n="Size (Gb)";e={"(0:N2)" -f (\$_.Size/1GB)}}`n	PowerShell H
1803	@{n="Used (Gb)";e={"(0:N2)" -f ((\$_.Size/1GB) - ...)} `n	b'@{n="Used (Gb)";e={"(0:N2)" -f ((\$_.Size/1GB) - ...)} `n	PowerShell H
1804	@{n="Free (Gb)";e={"(0:N2)" -f (\$_.FreeSpace/1G...)} `n	b'@{n="Free (Gb)";e={"(0:N2)" -f (\$_.FreeSpace/1G...)} `n	PowerShell H
1805	@{n="Free (%)" ;e={(if(\$_.Size) {"(0:N2)" -f (\$_.Fre...)} `n	b'@{n="Free (%)" ;e={(if(\$_.Size) {"(0:N2)" -f (\$_.Fre...)} `n	PowerShell H
1806	)`n	b' )`n	PowerShell H
1807	\$LogicalDisk   Format-Table -AutoSize   Out-String	b'\$LogicalDisk   Format-Table -AutoSize   Out-String'	PowerShell H
1808	Invoke-RestMethod -Uri ('https://ipinfo.io/')	b'Invoke-RestMethod -Uri ('https://ipinfo.io/')	PowerShell H
1809	python .\\vol.py -h	b'python .\\vol.py -h'	PowerShell H
1810	cd /	b'cd /'	PowerShell H
1811	cd .\\Users\\dmetz\\Downloads\\	b'cd .\\Users\\dmetz\\Downloads\\'	PowerShell H
1812	.\ConsoleHost_history.txt	b'.\\ConsoleHost_history.txt'	PowerShell H

1

**2022-02-15T132640\_DMETZ-W10.vhdx**

**DETAILS**

Order 1

Command List (UTF8) python --version

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

Artifact type PowerShell History

Item ID 586032

**ARTIFACT INFORMATION**

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

Recovery method Parsing

Deleted source

Location n/a

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

**EVIDENCE INFORMATION**

TAGS, COMMENTS & PROFILES

# Firewall Events

Magnet AXIOM Examine v5.9.0.30292 - CSIRT USB W11

File Tools Process Help

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

Type a search term... GO ADVANCED

**EVIDENCE (1,403)**

Column view

	Event ID	Created Date/Timestamp	Event Type	Event Description Summary	Rule ID
2004	2/14/2022 8:53:04 PM	307	A rule has been added to the Windows Firewall exce...	{8B724E29-6C65-4399-B1C8}	
2004	2/14/2022 8:53:04 PM	308	A rule has been added to the Windows Firewall exce...	{A8E695EF-27BD-4830-B3AF}	
2004	2/14/2022 8:53:04 PM	309	A rule has been added to the Windows Firewall exce...	{3B65252B-EB81-4B31-B91C}	
2004	2/14/2022 8:53:04 PM	310	A rule has been added to the Windows Firewall exce...	{E344DFB1-72BC-43AF-B0A1}	
2004	2/14/2022 8:53:04 PM	311	A rule has been added to the Windows Firewall exce...	{57D99815-6AF3-41B1-8B24}	
2004	2/14/2022 8:53:17 PM	312	A rule has been added to the Windows Firewall exce...	{80F1EA52-4FED-40F1-98E7}	
2004	2/14/2022 8:53:17 PM	313	A rule has been added to the Windows Firewall exce...	{FC968866-F413-4D1B-A0C2}	
2006	2/14/2022 8:54:33 PM	314	A rule has been deleted in the Windows Firewall exc...	{3B65252B-EB81-4B31-B91C}	
2006	2/14/2022 8:54:33 PM	315	A rule has been deleted in the Windows Firewall exc...	{A8E695EF-27BD-4830-B3AF}	
2004	2/14/2022 8:49:31 PM	10	A rule has been added to the Windows Firewall exce...	{884168A9-58A1-4719-A111}	
2004	2/14/2022 8:49:31 PM	13	A rule has been added to the Windows Firewall exce...	{47E0E03C-07D3-417E-933A}	
2004	2/14/2022 8:49:31 PM	12	A rule has been added to the Windows Firewall exce...	{FC8AEA85-1A02-459A-98FA}	
2006	2/14/2022 8:49:31 PM	14	A rule has been deleted in the Windows Firewall exc...	{FC8AEA85-1A02-459A-98FA}	
2004	2/14/2022 8:49:31 PM	11	A rule has been added to the Windows Firewall exce...	{167FD499-2C58-437E-B2FF}	
2006	2/14/2022 8:49:31 PM	15	A rule has been deleted in the Windows Firewall exc...	{167FD499-2C58-437E-B2FF}	
2006	2/14/2022 8:49:31 PM	16	A rule has been deleted in the Windows Firewall exc...	{884168A9-58A1-4719-A111}	
2006	2/14/2022 8:49:31 PM	17	A rule has been deleted in the Windows Firewall exc...	{47E0E03C-07D3-417E-933A}	
2004	2/14/2022 8:49:31 PM	18	A rule has been added to the Windows Firewall exce...	{2337CE28-2973-4EA5-96EB}	
2004	2/14/2022 8:49:31 PM	19	A rule has been added to the Windows Firewall exce...	{9864DEDA-F8CA-4990-9BC}	
2004	2/14/2022 8:49:31 PM	20	A rule has been added to the Windows Firewall exce...	{6E024BF2-B25F-46E7-9203}	
2004	2/14/2022 8:49:31 PM	21	A rule has been added to the Windows Firewall exce...	{8A6E7D10-A9D4-44AE-B2B}	
2006	2/14/2022 8:51:10 PM	29	A rule has been deleted in the Windows Firewall exc...	{3daa47ad-4db9-45b8-8f97-}	
2006	2/14/2022 8:51:10 PM	30	A rule has been deleted in the Windows Firewall exc...	{88d76b46-70a0-47be-ad62-}	
2004	2/14/2022 8:51:10 PM	31	A rule has been added to the Windows Firewall exce...	{8044754e-571c-414a-b91b-}	
2004	2/14/2022 8:51:10 PM	32	A rule has been added to the Windows Firewall exce...	{7f42be00-bd25-41f9-ba12-a}	
2006	2/14/2022 8:51:10 PM	33	A rule has been deleted in the Windows Firewall exc...	{15090595-6681-4544-96CD}	

**2004**

DMETZ-W10\_20220215\_082500.raw

**DETAILS**

**ARTIFACT INFORMATION**

Event ID **2004**  
Created Date/Time **2/14/2022 8:53:17 PM**  
Event Record ID **313**  
Event Description Summary **A rule has been added to the Windows Firewall exception list.**  
Rule ID **{FC968866-F413-4D1B-A0C2-90F0F0EFA02}**  
Rule Name **OneDrive**  
Modifying User **S-1-5-80-3088073201-146472863  
0-1879813800-1107566885-8232  
18052**  
Modifying Application **C:\WINDOWS\System32  
svchost.exe**  
Direction **Outbound**  
Event Data **<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">  
<System>  
<Provider Name="Microsoft-Windows-Windows Firewall With Advanced Security" Guid="d1bc9aff-2abf-4d71-9146-ecb2a986eb85" />  
<EventID>2004</EventID>  
<Version>0</Version>  
<Level>4</Level>  
<Task>0</Task>  
<Opcode>0</Opcode>  
<Keywords>0x8000020000000000**

**TAGS, COMMENTS & PROFILES**

Time zone UTC+0:00

# System Resource Usage Monitor (SRUM)

Magnet AXIOM Examine v5.9.0.30292 - CSIRT USB W11

File Tools Process Help

FILTERS Evidence Artifacts Content types Date and time Tags and comments Profiles Partial results Keyword lists Skin tone Type a search term... GO ADVANCED

EVIDENCE (69,398)

18630

Column view FILES EXPLORE

Application Name Full Path

Entr...	Application Name	Full Path
70970	SMB	System\S
28271	SMB	System\S
71080	SMB	System\S
80279	teams.exe	\device\h
73746		
37402		
73739	teams.exe	\device\h
60863	SMB	System\S
61649		
73557		
55880	SMB	System\S
73550	teams.exe	\device\h
37535	SMB	System\S
62551		
55904	SMB	System\S
61640	teams.exe	\device\h
56705		
62543	teams.exe	\device\h
56695	teams.exe	\device\h
81459		
87369		
87388	powerpnt.exe	\device\h
55927	SMB	System\S
51669		
70966	onedrive.exe	\device\harddiskvolume3\program files\microsoft o...
51666	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...

INDUSTRY NEWS OCTOBER 5, 2022

What is SRUM?

Table of Contents

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

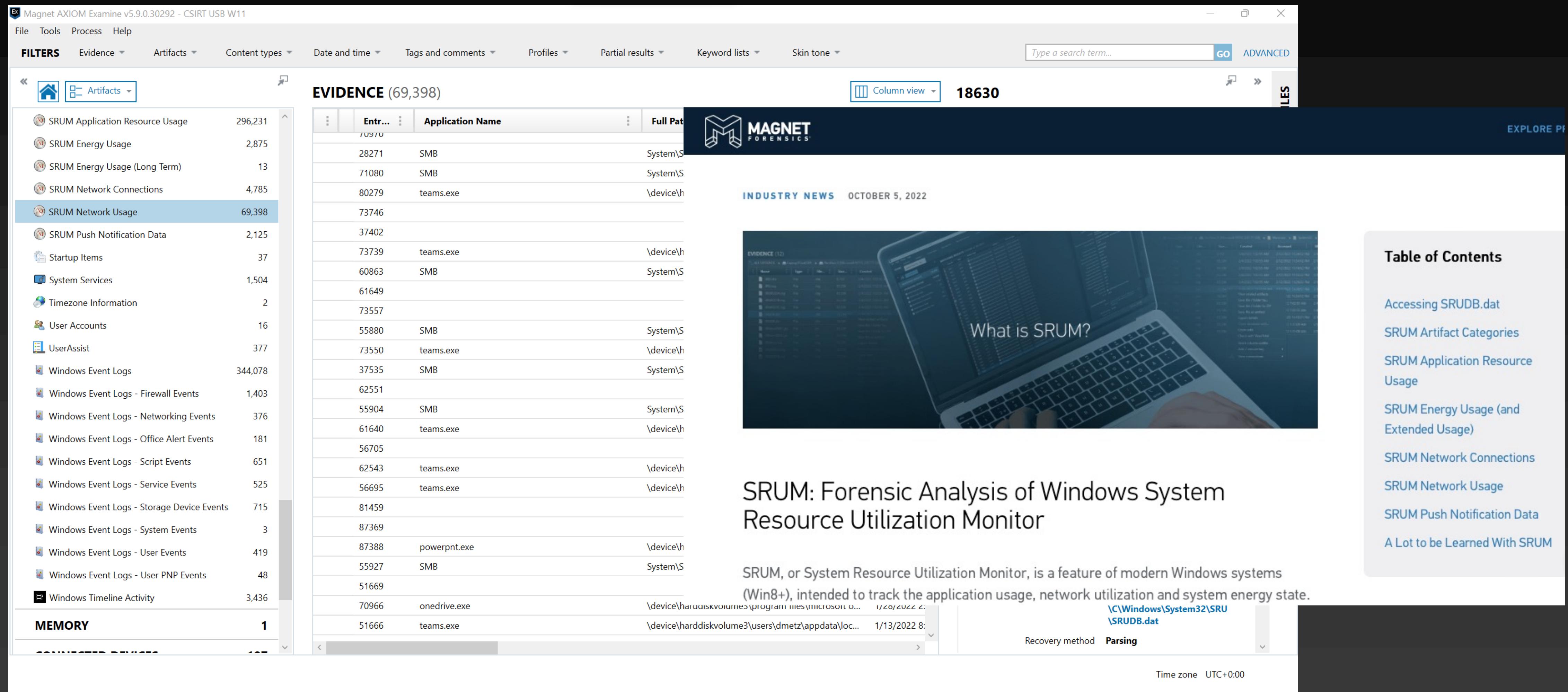
SRUM: Forensic Analysis of Windows System Resource Utilization Monitor

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

\C\Windows\System32\SRU\SRUDB.dat

Recovery method Parsing

Time zone UTC+0:00



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

# Offline Collections Processed - What's Next?

Magnet AXIOM Examine v5.9.0.30292 - CSIRT USB W11

File Tools Process Help

Case dashboard

## CASE OVERVIEW

### 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: CSIRT USB W11

SCAN 2

Scanned by: Doug Metz

Scan date/time - local time: 2/15/2022 2:26:42 PM

Scan description:

[VIEW SCAN SUMMARY](#)

SCAN 1

Scanned by: Doug Metz

Scan date/time - local time: 2/15/2022 11:37:50 AM

Scan description:

[VIEW SCAN SUMMARY](#)

### 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](#)

## EVIDENCE OVERVIEW

### 2022-02-15T132640\_DMETZ-W10.vhdx (782,246)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number: 2022-02-15T132640\_DMETZ-W10.vhdx

Description:

Location: 2022-02-15T132640\_DMETZ-W10.vhdx

Platform: Computer



[CHANGE PICTURE](#)

### DMETZ-W10\_20220215\_082500.raw (33,040)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number: DMETZ-W10\_20220215\_082500.raw

Description:

Location: DMETZ-W10\_20220215\_082500.raw

Platform: Computer



[CHANGE PICTURE](#)

## PLACES TO START

### ARTIFACT CATEGORIES

[VIEW ALL ARTIFACT CATEGORIES](#)

Evidence source: All

Number of artifacts: 815,286

Category	Count
Operating System	746,938
Web Related	54,323
Refined Results	7,887
Media	3,339
Custom	2,082
Application Usage	375
...	...

### TAGS AND COMMENTS

### MAGNET.AI CATEGORIZATION

### KEYWORD MATCHES

### 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 IMEIs.

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](#)

Time zone: UTC+0:00

# Collecting More with Axiom Cyber

Magnet AXIOM Process 6.0.0.31091

EVIDENCE SOURCES

SELECT EVIDENCE SOURCE

- COMPUTER
- MOBILE
- CLOUD
- VEHICLE
- REMOTE COMPUTER

EVIDENCE SOURCES ADDED TO CASE

Type	Image - location name	Evidence number	Search type	Status
Computer artifacts				

Magnet AXIOM Process 6.0.0.31091

EVIDENCE SOURCES

REMOTE COMPUTER DEPLOY AGENT

Provide information about the remote computer that you want to deploy the agent to.

Remote computer IP address: moriarty

User name: dwmetz

Password: \*\*\*\*\*

Agent location on remote computer: C:\

DEPLOY AGENT

Magnet AXIOM Process 6.0.0.31091

EVIDENCE SOURCES

REMOTE COMPUTER SELECT ITEMS TO DOWNLOAD

Computer name: MORIARTY  
User name: dwmetz  
Local end point: 192.168.4.181  
Computer status: Connected Downloading the file system structure and metadata

STOP AND DELETE AGENT

REVIEW AND SELECT THE DATA FROM THE TARGET COMPUTER

Review the files and folders on the remote computer and select the drives, files, folders, and memory that you want to download. To save time searching the complete list of files and folders, select Targeted locations to view a list of typical files and folders that you might want to download.

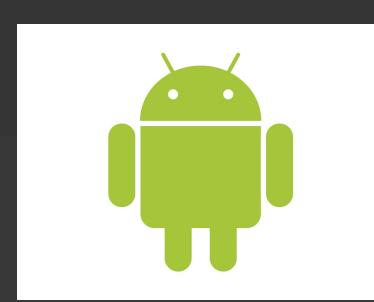
TARGETED LOCATIONS FILES AND DRIVES MEMORY

ITEMS TO DOWNLOAD

The selected items will be saved to an AFF4-L container EDIT

Item	Download start date/time	Items downloaded

BACK NEXT



# 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/cape>

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

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

Blog: <https://bakerstreetforensics.com>

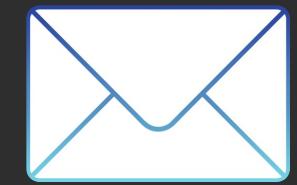
# Thank You



<https://github.com/dwmetz>



@dwmetz



doug.metz@magnetforensics.com



<https://bakerstreetforensics.com>



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