

# PowerShell Tools for IR Forensics Collection

Doug Metz

# Enterprise Pulse – Q&A

## Magnet Forensics Discord Server

Join the conversation live!

**#EnterprisePulse2021** is offering live discussion on the **Magnet Forensics Discord Server**

<https://discord.gg/fMkHuYybSb>



## Whoami:

Incident Response Manager for  
Fortune 200 Company

Incident Response & Forensics for 13  
years spanning multiple verticals  
including consulting, private sector  
and DoD

### Certs:

MCFE, GCIH, GCFA, GCFE, GCTI,  
CISSP

### Affiliations:

SANS Advisory Board  
DFIR Review  
FIRST  
HTCIA

ND Alumni #Golrish

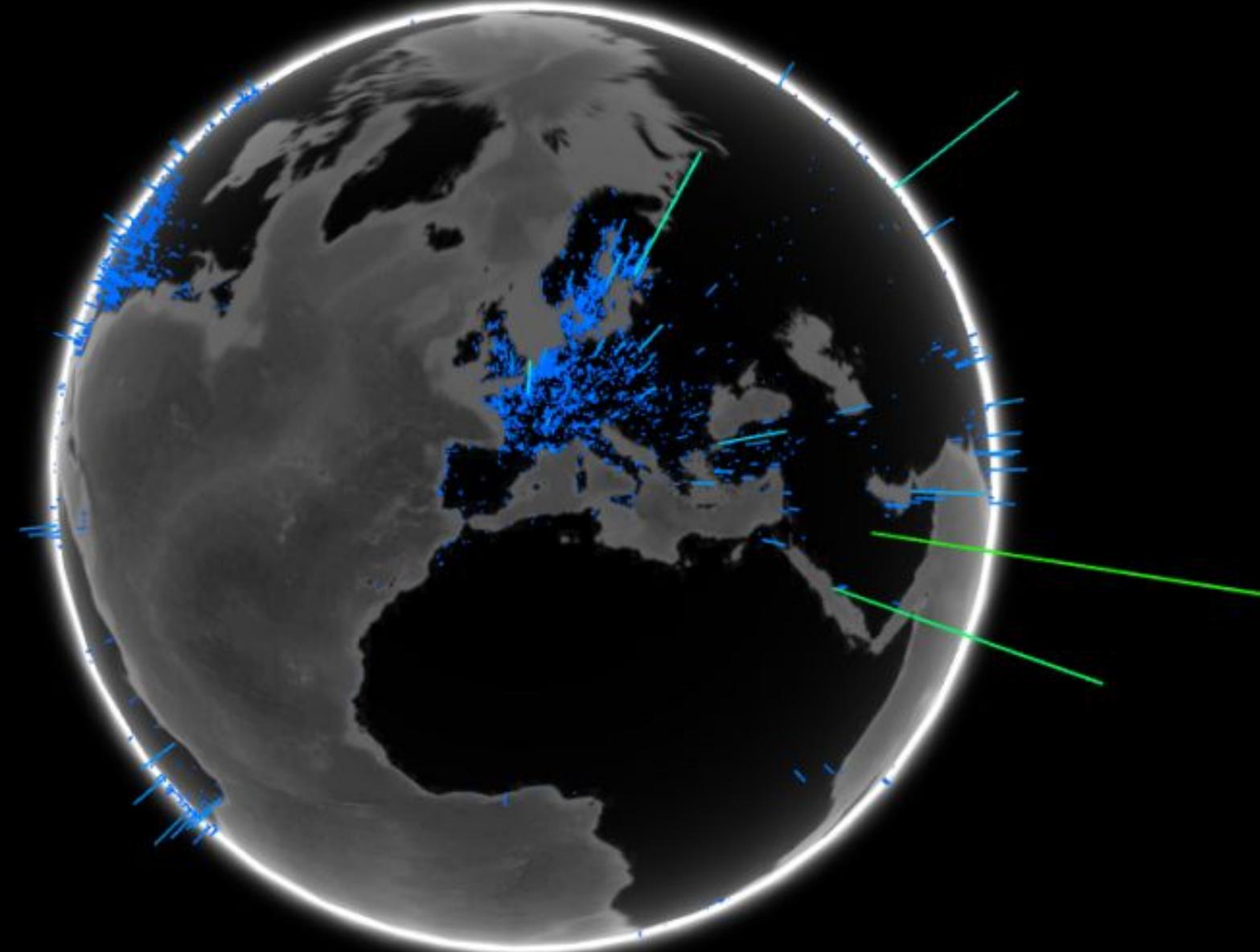
<http://bakerstreetforensics.com>

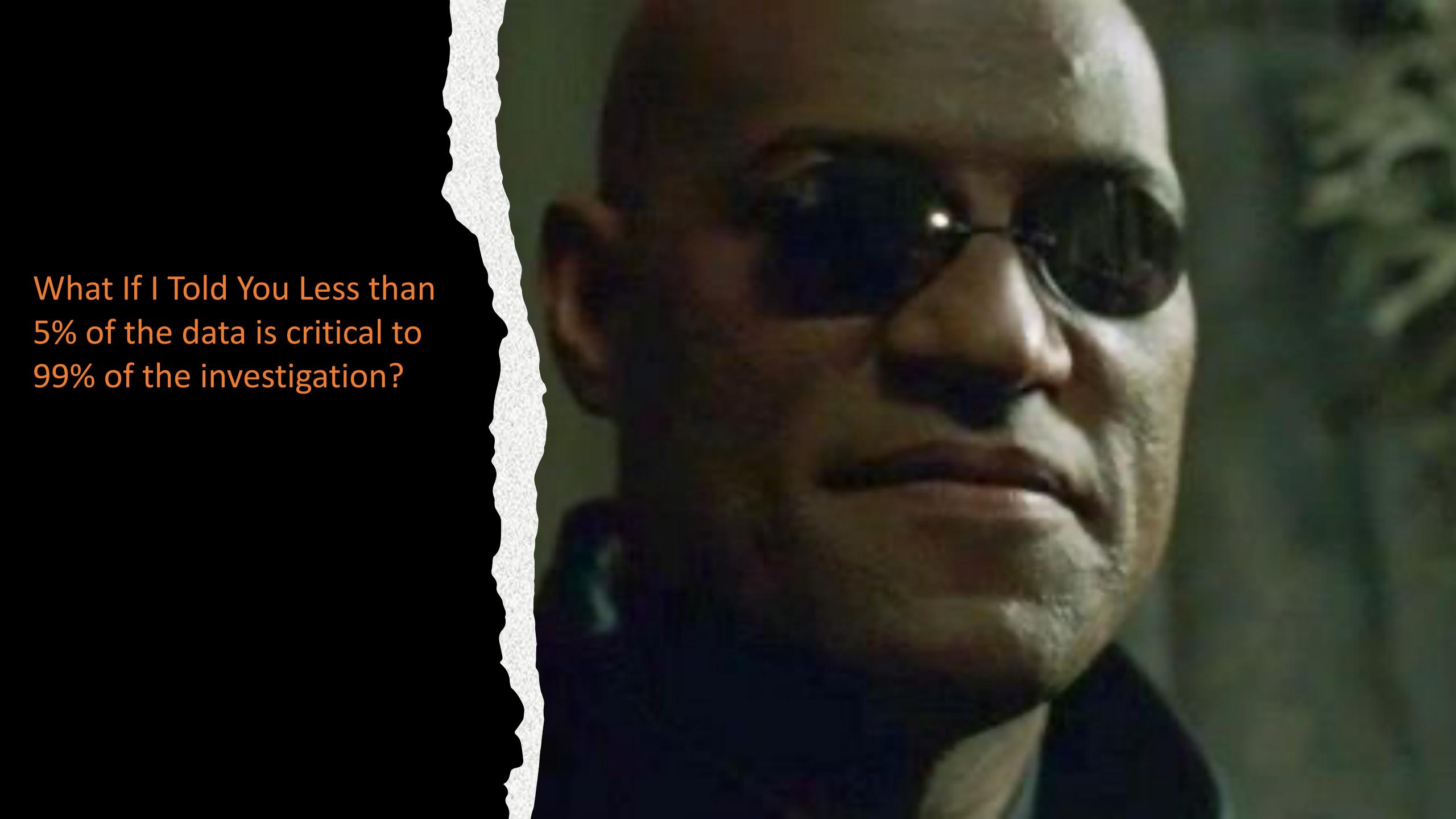
@dwmetz



## Challenges. Opportunities:

- Geographic disbursement of assets
- Bandwidth limitations in particular regions
- Limited resources on staff with forensic experience
- Magnitude of assets to be collected
- ? Unreachable



A close-up profile view of a man's face. He is wearing dark sunglasses and a dark suit jacket. His gaze is directed towards the right side of the frame. The background is blurred.

What If I Told You Less than  
5% of the data is critical to  
99% of the investigation?

## The Toolbox:

- PowerShell (CSIRT-Collect.ps1)
- KAPE (Kroll Artifact Parser & Extractor)
- Winpmem
- 7zip
- Arsenal Image Mounter
- Magnet Axiom



## CSIRT-Collection.PS1: (1)

- Maps to existing network drive -  
Subdir 1 : "Memory" – Winpmem and  
7zip executables
- Subdir 2: "KAPE" – directory copied  
from local install
- Creates a local directory on asset
- Copies the Memory exe files to local  
directory
- Captures memory with Winpmem
- When complete, ZIPS the memory  
image
- Renames the zip file based on hostname
- Documents the OS Build Info (no need  
to determine profile for Volatility)
- Compressed image is copied to network  
directory and deleted from host after  
transfer complete

```
15
16 ## map the network drive and change to that directory
17 Write-Host -Fore Green "Mapping network drive..."
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
38 #Remove-PSDrive -Name X
39 #New-PSDrive -Name X -PSProvider FileSystem -Root "\Synology\Collections"
40
41 # create local memory directory
42 Write-Host -Fore Green "Setting up local directory..."
43 mkdir C:\temp\IR -Force
44 Set-Location C:\temp\IR
45 Write-Host -Fore Green "Copying tools..."
46 robocopy "\Synology\Collections\Memory" *.exe
47 ## capture memory image
48 Write-Host -Fore Green "Capturing memory..."
49 .\winpmem.exe memdump.raw
```

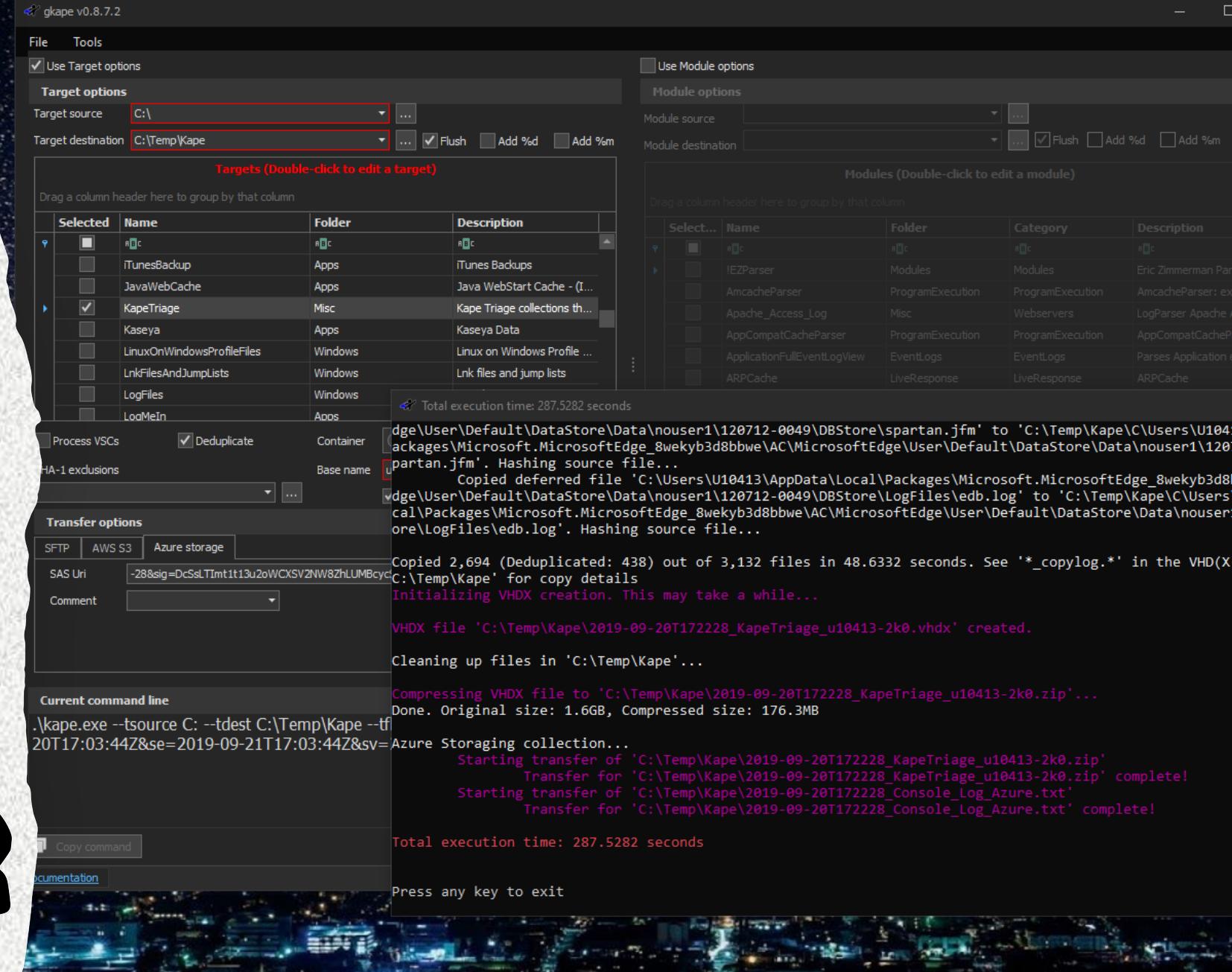
# KAPE:

KAPE has two primary components,  
Targets & Modules.

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

Modules are processing routines that  
can be run on what is collected  
(parse, convert to CSV, more)

If there is a command line interface  
available for an application, a KAPE  
module can be written for it



## CSIRT-Collection.ps1: (2)

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

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

## Size Matters:

Complete Hard Drive:

250 GB

Targeted Collection:

2 GB

Collection Compressed:

688 MB

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)



## Deployment Options:

- SOC
- Help Desk
- Field Support
- Group Policy
- SOAR (Automation)
- EDR (Endpoint Detection and Response)
- USB Media \*



# CSIRT-Collect.ps1

Demo

The screenshot shows a file explorer window with a dark theme. The path is 'synology > Collections > MORIARTY'. The 'Organize' ribbon tab is selected, showing icons for Move to, Copy to, Delete, Rename, New folder, New item, Open, Properties, Select all, Select none, and Invert selection. Below the ribbon is a search bar 'Search MORIARTY'. The file list contains the following items:

	Name	Date modified	Type	Size
1	2021-01-14T192147_ConsoleLog.txt	1/14/2021 2:24 PM	Text Document	94 KB
2	2021-01-14T192147_MORIARTY.zip	1/14/2021 2:24 PM	Compressed (zipp...)	151,594 KB
3	MORIARTY.7z	1/14/2021 2:20 PM	7Z File	1,551,643 KB
4	MORIARTY.txt	1/14/2021 2:20 PM	Text Document	1 KB
5	transfer-complete.txt	1/14/2021 2:24 PM	Text Document	1 KB

The screenshot shows a Notepad++ window titled '\\synology\Collections\MORIARTY\MORIARTY.txt - Notepad++'. The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, Macro, Run, Plugins, Window, and Help. The toolbar has various icons for file operations. The status bar at the bottom shows 'Normal text file', 'length : 95 lines : 5', and 'Ln : 5'. The content of the file is:

```
1
2 Major Minor Build Revision
3 -----
4 10 0 18363 0
5
```

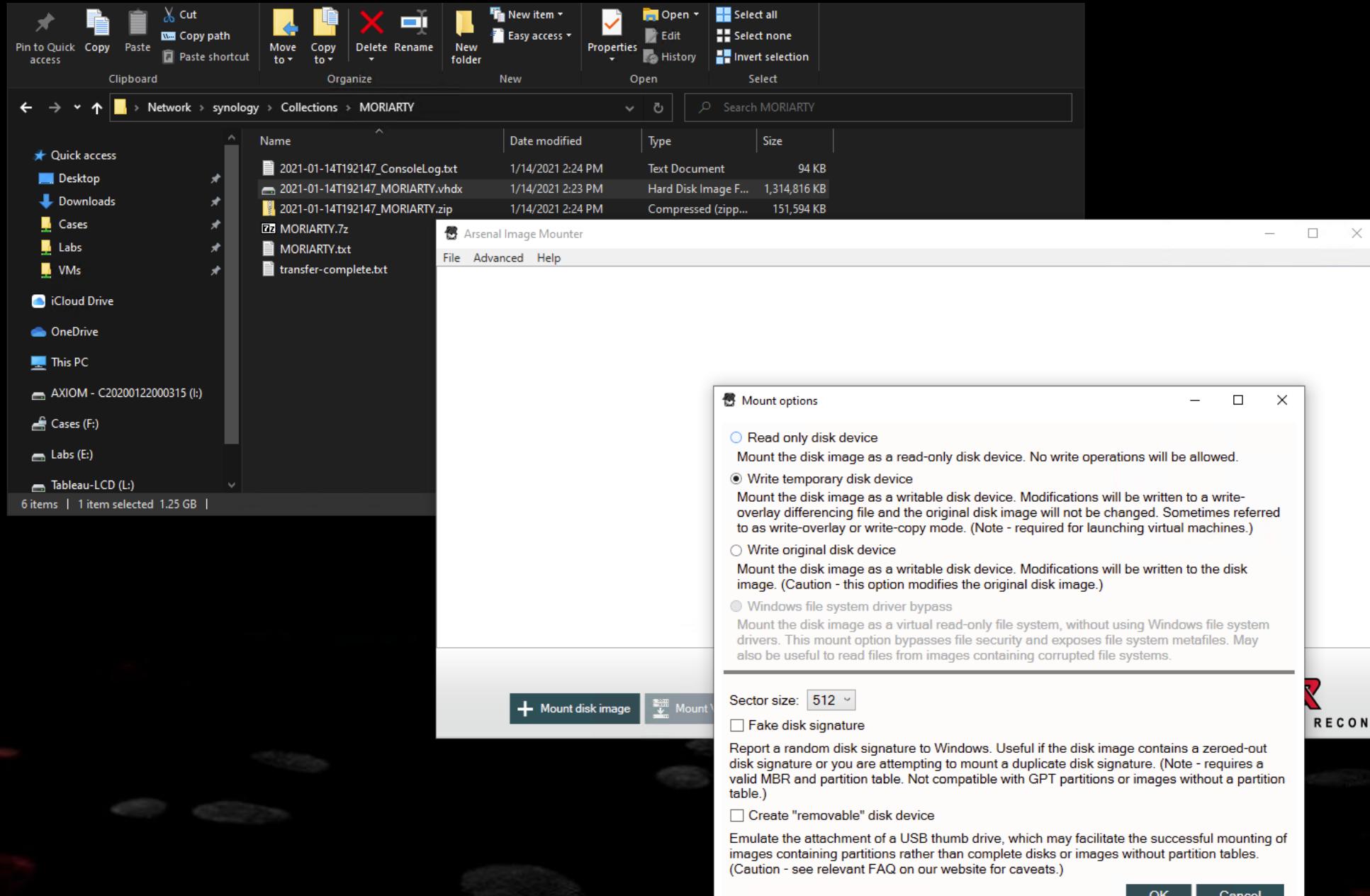
## Reviewing the Output

- 1 – KAPE Console Log
- 2 – zip file of KAPE .vhdx
- 3 – 7zip memory image
- 4 – OS Build info for Volatility
- 5 – “Transfer Complete” signal

The screenshot shows a Notepad++ window titled '\\synology\Collections\MORIARTY\transfer-complete.txt - Notepad++'. The menu bar includes File, Edit, Search, View, Encoding, Language, Settings, Tools, Macro, Run, Plugins, Window, and Help. The toolbar has various icons for file operations. The status bar at the bottom shows 'Normal text file', 'length : 95 lines : 5', and 'Ln : 5'. The content of the file is:

```
5 Transfer complete: 1/14/2021 2:24:17 PM
```

# Mount the VMDK with Arsenal Image Mounter



# AQUIRE the mounted image with Axiom Process

The screenshot shows the Magnet AXIOM Process 4.8.1.22785 software interface. The main window displays the following sections:

- EVIDENCE SOURCES**: Shows a list of files and artifacts:
  - 2021-01-14T192147\_ConsoleLog.txt (1/14/2021 2:24 PM)
  - 2021-01-14T192147\_MORIARTY.vhdx (1/14/2021 2:23 PM)
  - 2021-01-14T192147\_MORIARTY.vhdx.diff (1/14/2021 5:15 PM)
  - 2021-01-14T192147\_MORIARTY.zip (1/14/2021 2:24 PM)
  - MORIARTY.7z (1/14/2021 2:20 PM)
  - MORIARTY.vbt (1/14/2021 2:20 PM)
  - transfer-complete.txt (1/14/2021 2:24 PM)
- CASE DETAILS**: Shows the case name: MORIARTY.
- PROCESSING DETAILS**: Includes options like "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", and "Find more artifacts".
- ARTIFACT DETAILS**: Shows 0 artifacts.
- ANALYZE EVIDENCE**: A large empty area for analysis.

At the bottom right of the software window are **BACK** and **NEXT** buttons. The background of the entire image features a dark theme with fingerprint patterns and a magnifying glass.

+ Mount disk image    Mount VSCs    Launch VM    Remove    Remove all    Refresh



## AQUIRE the mounted image with Axiom Process (2)

The screenshot shows two windows side-by-side. On the left is a Windows File Explorer window titled 'MORIARTY' showing files from a network location. On the right is the 'Magnet AXIOM Process' software interface.

**Magnet AXIOM Process 4.8.1.22785**

**EVIDENCE SOURCES**

**CASE DETAILS**

**EVIDENCE SOURCES** (selected)

**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**

- Computer artifacts
- Mobile artifacts
- Cloud artifacts

**ANALYZE EVIDENCE**

**SELECT DEVICE**

**COMPUTER**

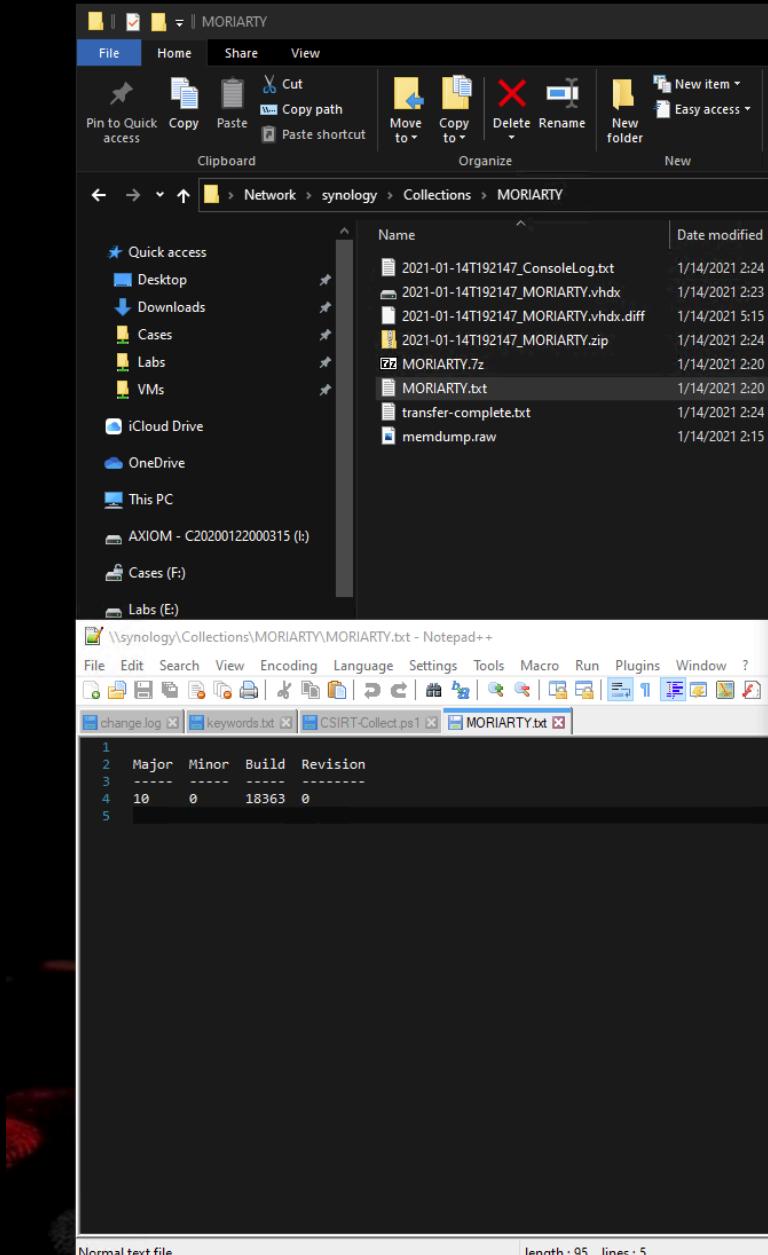
- PhysicalDrive6** USB Flash Disk USB Device (1.86 GB)  
Type: Removable Media  
Size: 1.86 GB  
Serial Number: C20200122000315
- PhysicalDrive1** Samsung SSD 850 PRO 1TB (953.87 GB)  
Type: Fixed hard disk media  
Size: 953.87 GB  
Serial Number: S252NXAG711528P
- PhysicalDrive7** Arsenal Virtual SCSI Disk Device (3.29 GB)  
Type: Fixed hard disk media  
Size: 3.29 GB  
Serial Number: {493d0e62-5693-11eb-a851-001a7dda7113}
- F: Entire Disk (9.1 TB)**  
Type:  
Size: 9.1 TB  
Serial Number: D0B580A85E1EB6C74872FFF665869C89:91877E00000

**BACK** **NEXT**

+ Mount disk image | Mount VSCs | Launch VM | Remove | Remove all | Refresh



# Use the Build Info .txt for Memory Profile



The screenshot shows a Windows File Explorer window titled "MORIARTY" and a Magnet AXIOM Process 4.8.1.22785 interface. The File Explorer displays several files including "2021-01-14T192147\_ConsoleLog.txt", "2021-01-14T192147\_MORIARTY.vhdx", "2021-01-14T192147\_MORIARTY.vhdx.diff", "2021-01-14T192147\_MORIARTY.zip", "MORIARTY.7z", "MORIARTY.txt", "transfer-complete.txt", and "memdump.raw". The Magnet AXIOM interface shows "EVIDENCE SOURCES" and "CASE DETAILS" sections. In the "SELECT PROFILE" section, the "Image profile" dropdown is set to "Win10x64 18362". A Notepad++ window is open, showing the contents of "MORIARTY.txt".

**EVIDENCE SOURCES**

**CASE DETAILS**

**EVIDENCE SOURCES** 1

**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** 188

- Computer artifacts 188 of 237
- Mobile artifacts
- Cloud artifacts

**ANALYZE EVIDENCE**

**WINDOWS SELECT PROFILE**

To process a memory image, you must provide the correct image profile, based on the operating system build number.

AXIOM Process can provide a list of recommended memory image profiles, which may take a while. You can also select a profile manually.

I want AXIOM Process to provide a list of recommended image profiles.  
 I want to select the image profile myself.

Select an image profile. Optionally, you can also provide the Kernel Debug (KDBG) address of the profile for faster memory analysis. On Windows 8+, Volatility reports this address as "KdCopyDataBlock (V)" and, on earlier Windows versions, as "Offset (V)."

**Image profile:** Win10x64 18362

**KDBG address:** [empty input field]

 Memory artifacts powered by Volatility

**BACK** **NEXT**

Normal text file length : 95 lines : 5 Ln : 5 Col : 1 Pos : 96 Windows (CR LF) UCS-2 LE BOM INS ...

Bring it all into Axiom

Combine Memory and  
Triage Collections in Axiom

Combine collections from  
multiple assets  
(Connections)

Timeline of activity for  
multiple assets

## EVIDENCE OVERVIEW

[ADD NEW EVIDENCE](#)

### KAPE Triage Collection (99,715)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number **KAPE Triage Collection**

Description

Location **KAPE Triage Collection.zip**

Platform **Computer**



[CHANGE PICTURE](#)

### Memory Collection (4,521)

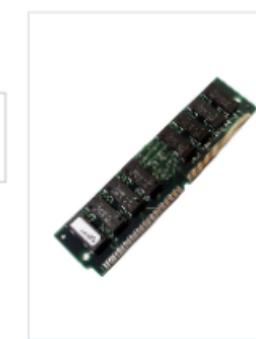
[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number **Memory Collection**

Description

Location **memdump.raw**

Platform **Computer**



[CHANGE PICTURE](#)

## PLACES TO START

### ARTIFACT CATEGORIES

[VIEW ALL ARTIFACT CATEGORIES](#)

Evidence source **All**

Number of artifacts **104,236**

Operating System

Web Related **6,783**

Media **1,053**

Refined Results **429**

Custom **31**

Documents **8**

### TAGS AND COMMENTS

### MAGNET.AI CATEGORIZATION

### KEYWORD MATCHES

### PROFILES

## Under the KAPE

KAPE: 1.3GB Collection >  
100,000+ Artifacts

Customize KAPE to collect  
what only what you need for  
investigation

- Desktop “Triage” Collection
- Web Server (IIS, Apache)
- Logs & Registry

Magnet AXIOM Examine v4.8.1.22785 - CSIRT-Collect Demo

Tools Process Help

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

REFINED RESULTS 320

- Classifieds URLs 2
- Cloud Services URLs 2
- Facebook URLs 5
- Identifiers - Device 44
- Identifiers - People 41
- Locally Accessed Files and Folders 14
- Parsed Search Queries 17
- Passwords and Tokens 4
- Rebuilt Desktops - Windows 1
- Social Media URLs 5
- Tax Site URLs 185

RELATED 3,957

MEDIA 336

DOCUMENTS 6

PEER TO PEER 4

OPERATING SYSTEM 95,089

- \$LogFile Analysis 4,690
- AmCache Device Containers 2
- AmCache Driver Binaries 351
- AmCache Driver Packages 21
- AmCache File Entries 588
- AmCache Pnp Devices 117
- AmCache Program Entries 56
- AmCache Shortcuts 50
- AutoRun Items 687
- Feature Usage 17

MATCHING RESULTS (99,715 of 104,236)

Item	Type	Artifact c...	Date...	Location
ZIP	File System Information	Operating System		
525385	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
11416	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
5240	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
5264	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
1160	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
9184	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
1136	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
1288	Pictures	Media		
1024	Pictures	Media		
1024	Pictures	Media		
1152	Pictures	Media		
1040	Pictures	Media		
1040	Pictures	Media		
1032	Pictures	Media		
1032	Pictures	Media		
1032	Pictures	Media		
1192	Pictures	Media		

## The Need for Speed

Triage collections can be collected and processed in minutes versus hours

RAM is worth the time

\*Typical collections average 10-15 minutes

Ability to leverage Azure cloud storage for even faster transfer of data from remote sites

☺ Supports bandwidth or regulatory concerns

From Acquisition to Evidence Analysis in 90 minutes or less



## Links

Arsenal Image Mounter:  
<https://arsenalrecon.com>

KAPE:  
<https://www.kroll.com/en/insights/publications/cyber/kroll-artifact-parser-extractor-kape>

Winpmem:  
<https://github.com/Velocidex/WinPmem/releases/tag/v4.0.rc1>

7zip: <https://www.7-zip.org/download.html>

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

Magnet Axiom:  
<https://www.magnetforensics.com>

FOR498 – Battlefield Forensics & Acquisition:  
<https://www.sans.org/cyber-security-courses/battlefield-forensics-and-data-acquisition/>

Blog: <https://bakerstreetforensics.com>



Connect

@dwmetz

dwmetz@gmail.com



[https://github.com/dwmetz/CSIRT-  
Collect](https://github.com/dwmetz/CSIRT-Collect)

<http://bakerstreetforensics.com>