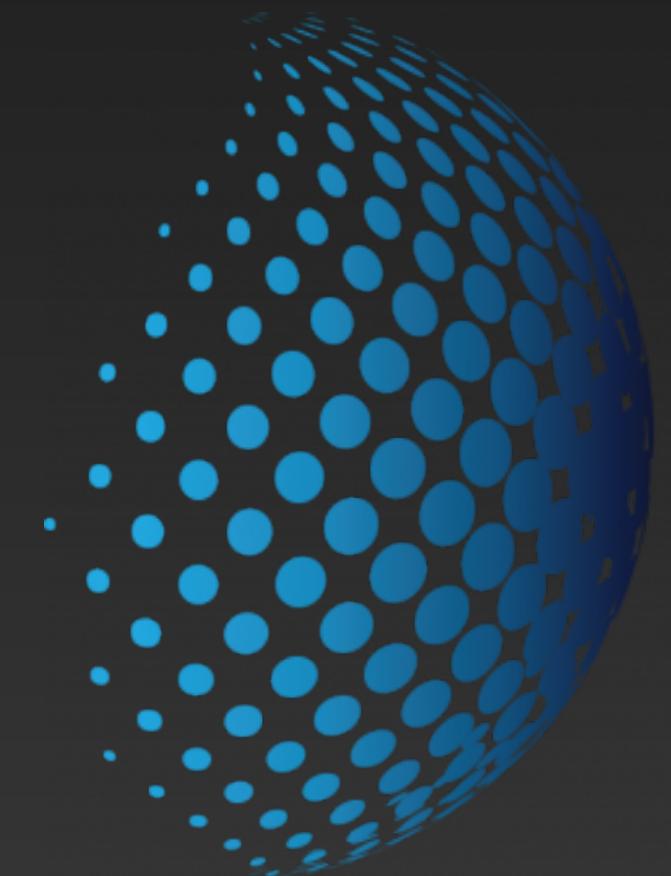


PowerShell Tools for IR

Forensics Collection

Doug Metz

Global Incident Manager



HTCIA

International Conference
September 2021

Who Am I

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

WHOAMI

Summary: Global Incident Response Manager for Fortune 200, leading a distributed team of DFIR analysts and 24x7 SOC

15 years Incident Response, Forensics and Consulting experience across Public, Private and DoD sectors.

PowerShell Fanboy

Certs: MCFE, GCIH, GCFA, GCFE, GCTI, CISSP

Affiliations:

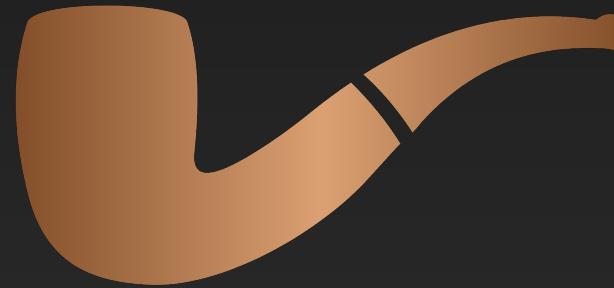
- HTCIA
- DFIR Review
- SANS Advisory Board
- FIRST

ND Alumni #GoIrish

Twitter: @dwmetz

Blog: <https://bakerstreetforensics.com>

Github: <https://github.com/dwmetz>



Baker Street Forensics

D . F . I . R .

We Need Forensic Data

“What’s the problem?”

- Geographic disbursement of assets
- Bandwidth limitations in remote regions
- Limited staff with forensic experience
- Magnitude of assets to be collected
- Budget
- Time



**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-Collect

Stage 1

Maps to existing network drive

Subdir 1 : "Memory" – Winpmem 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

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 ## map the [parameter] -Fore [range 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
```

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.



The screenshot shows the KAPE v0.8.7.2 software interface. The top menu bar includes File and Tools. Under Tools, there are checkboxes for 'Use Target options' (checked) and 'Use Module options' (unchecked). The 'Target options' section contains fields for 'Target source' (set to C:\), 'Target destination' (set to C:\Temp\Kape), and checkboxes for 'Flush', 'Add %d', and 'Add %m'. The 'Module options' section contains fields for 'Module source' and 'Module destination', with similar checkboxes for 'Flush', 'Add %d', and 'Add %m'. The main window is divided into two sections: 'Targets (Double-click to edit a target)' and 'Modules (Double-click to edit a module)'. Both sections feature tables with columns for Selected, Name, Folder, and Description. In the Targets section, 'KapeTriage' is selected. In the Modules section, several modules are listed under categories like Modules, ProgramExecution, and Webservers. A status bar at the bottom displays the total execution time as 287.5282 seconds and a message to press any key to exit.

CSIRT-Collect

Stage 2

- New temp Directory on asset for KAPE output
- KapeTriage 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

```
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

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

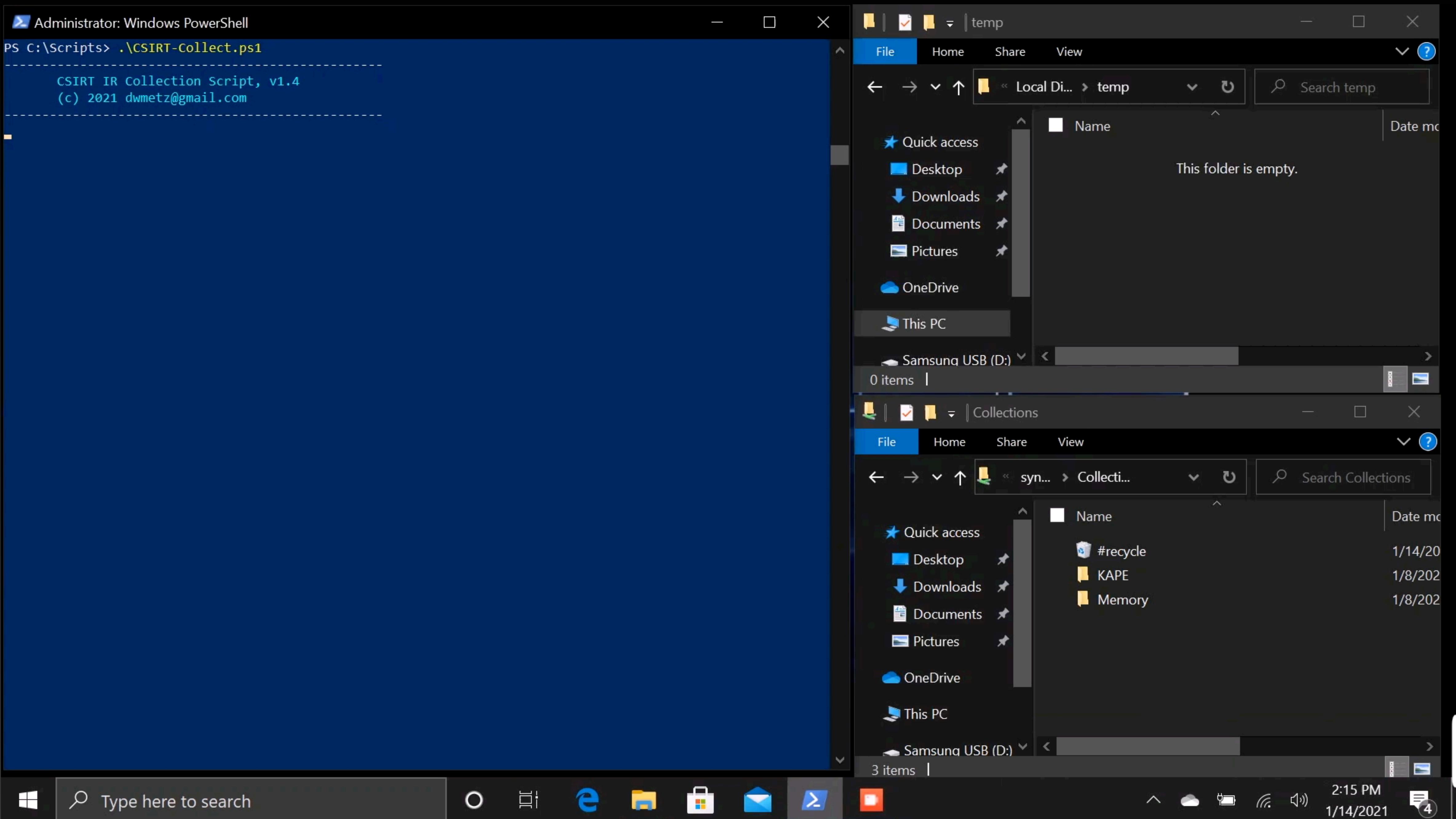


- SOC (Security Operations Center)
- Help Desk
- Field Support / Local IT
- Group Policy
- SOAR (Automation)
- EDR (Endpoint Detection and Response)
- USB Media *

CSIRT-Collect.ps1

Demo

May the Demo gods smile on us



Reviewing the Collection Output

The screenshot shows a Windows File Explorer window and a Notepad++ window side-by-side.

File Explorer Content:

- Path: \\synology\Collections\MORIARTY
- Files listed:
 - 1 2021-01-14T192147_ConsoleLog.txt
 - 2 2021-01-14T192147_MORIARTY.zip
 - 3 MORIARTY.7z
 - 4 MORIARTY.txt
 - 5 transfer-complete.txt

Notepad++ Content (MORIARTY.txt):

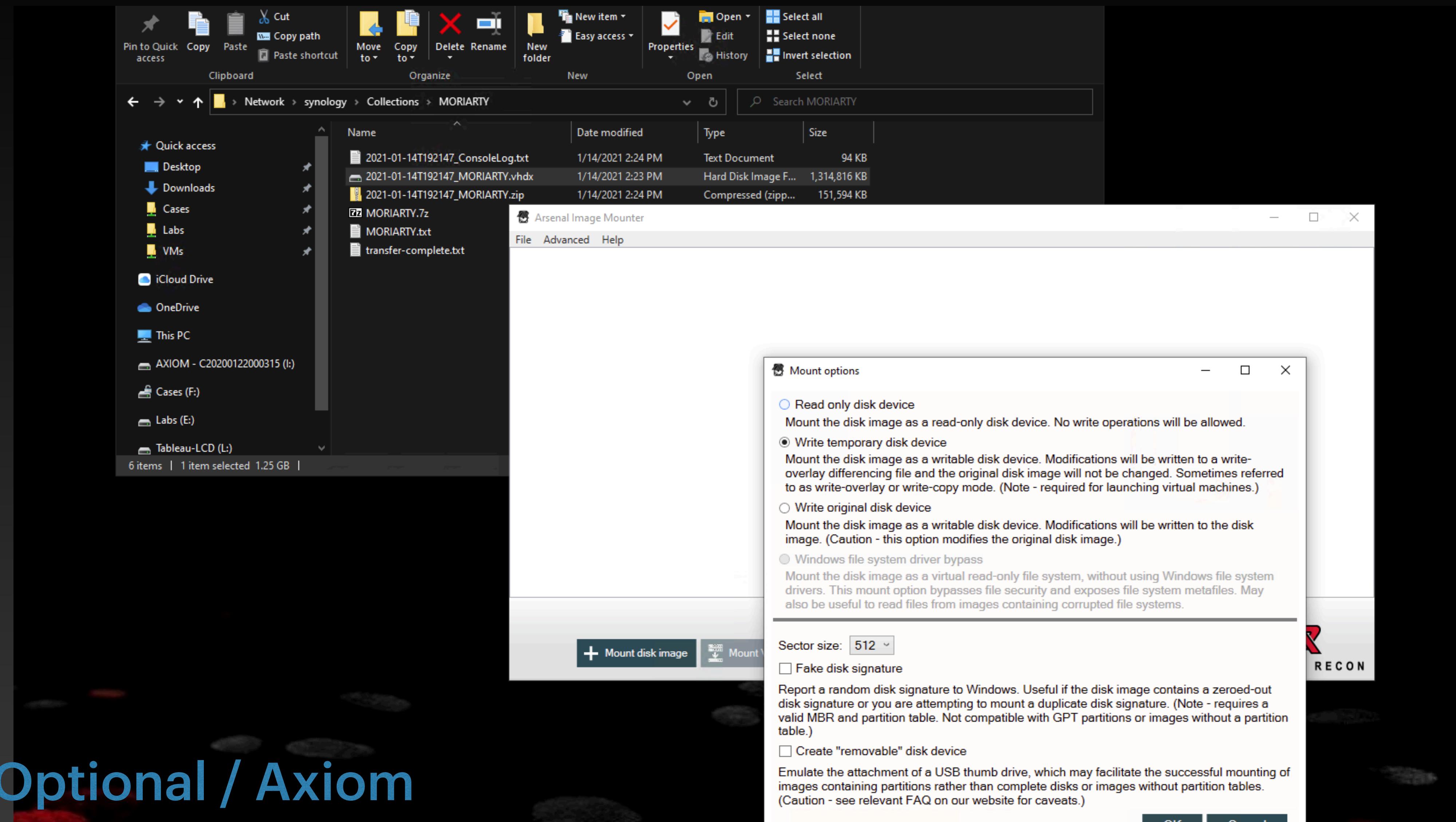
	Major	Minor	Build	Revision
1	10	0	18363	0
2				
3				
4				
5				

Notepad++ Content (transfer-complete.txt):

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

Evidence Processing Tips

Mount the VMDK with Arsenal Image Mounter



Process the VMDK

Magnet AXIOM Process 5.2.0.25407

File Tools Help

EVIDENCE SOURCES

WINDOWS SELECT EVIDENCE SOURCE

DRIVE IMAGE FILES & FOLDERS VOLUME SHADOW COPY MEMORY

Select the image

Organize New folder

Name	Date modified	Type	Size
2021-07-15T204305_MORIARTY.vhdx	7/15/2021 4:44 PM	Hard Disk Image F...	1,871,872 ...

Quick access
Desktop
Downloads
Documents
Cases
Labs
VMs

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

Computer > Windows > Load Evidence > IMAGE

Artifacts from VMDK

Magnet AXIOM Examine v5.2.0.25407 - HTcia_CSIRT-Collect

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: HTcia_CSIRT-Collect

SCAN 1

Scanned by: Doug Metz

Scan date: 7/22/2021 3:36:19 PM

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.

EVIDENCE OVERVIEW

2021-07-15T204305_MORIARTY.vhd (306,038)

ADD NEW EVIDENCE

Evidence number: 2021-07-15T204305_MORIARTY.vhd

Description: No picture added

Location: 2021-07-15T204305_MORIARTY.vhd

Platform: Computer

CHANGE PICTURE

PLACES TO START

ARTIFACT CATEGORIES

VIEW ALL ARTIFACT CATEGORIES

Evidence source: All

Number of artifacts: 306,038

Operating System: 302,838

Web Related: 2,580

Refined Results: 292

Media: 179

Connected Devices: 60

Application Usage: 55

TAGS AND COMMENTS

MAGNET.AI CATEGORIZATION

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

Under the KAPE

KAPE: 1.8GB Collection >
300,000+ Artifacts

Customize KAPE to
collect what only what
you need for
investigation

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

Magnet AXIOM Examine v5.2.0.25407 - HTCIA_CSIRT-Collect

File Tools Process Help

2021-07-15T204305_... Artifacts Content types Date and time Tags and comments Profiles

FILTERS Keyword lists Skin tone

Artifacts

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 &
...	MRU Recent Files &

MATCHING RESULTS 306,038

REFINED RESULTS 292

Category	Count
Classifieds URLs	2
Cloud Services URLs	2
Facebook URLs	2
Identifiers - Device	105
Identifiers - People	62
Locally Accessed Files and Folders	34
Parsed Search Queries	52
Passwords and Tokens	24
Rebuilt Desktops - Windows	1
Social Media URLs	7
Tax Site URLs	1

WEB RELATED 2,580

Category	Count
Edge Chromium Autofill	71
Edge Chromium Autofill Profiles	6
Edge Chromium Bookmarks	451

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

Add keywords to search

Extract text from files (OCR)

Calculate hash values

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

The screenshot shows the Magnet AXIOM Process interface. On the left, the 'EVIDENCE SOURCES' tab is selected under 'CASE DETAILS'. In the 'PROCESSING DETAILS' section, several options are listed with 'On' or 'Off' status indicators. The 'ARTIFACT DETAILS' section shows 0 artifacts. The 'ANALYZE EVIDENCE' section is currently empty.

In the center, the 'WINDOWS SELECT PROFILE' section guides the user through selecting a memory profile based on the operating system build number. It includes a note about AXIOM Process providing recommended profiles or allowing manual selection. Two radio button options are shown:

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

Below these options, there is a dropdown menu labeled 'Image profile' set to 'Win10x64 19041' and a text input field for 'KDBG address'.

On the right side of the interface, two windows are displayed:

- A Notepad++ window titled 'MORIARTY.txt' showing the contents of the file: \synology\Collections\MORIARTY\MORIARTY.txt. The file contains the following text:

Major	Minor	Build	Revision
10	0	19043	0
- A File Explorer window showing the directory structure and files within the 'MORIARTY' folder. The files listed are:

Name	Date modified	Type
transfer-complete.txt	7/15/2021 4:46 PM	TXT File
2021-07-15T204305_ConsoleLog.txt	7/15/2021 4:45 PM	TXT File
2021-07-15T204305_MORIARTY.zip	7/15/2021 4:45 PM	Compressed
MORIARTY.txt	7/15/2021 4:35 PM	TXT File
MORIARTY.7z	7/15/2021 4:35 PM	7Z File
2021-07-15T204305_MORIARTY	7/15/2021 4:54 PM	File folder
memdump.raw	7/15/2021 4:29 PM	RAW File

Bring it all together with 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](#)

PLACES TO START

ARTIFACT CATEGORIES

[VIEW ALL ARTIFACT CATEGORIES](#)

Evidence source: All

Number of artifacts: 475,436

Category	Count
Operating System	304,398
Memory	155,502
Web Related	12,878
Media	2,090
Refined Results	365
Connected Devices	60

TAGS AND COMMENTS

MAGNET.AI CATEGORIZATION

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

Evidence Overview Details:

Evidence Item	Description	Location	Platform
memdump.raw (169,398)	(empty)	memdump.raw	Computer
2021-07-15T204305_MORIARTY.vhd (306,038)	(empty)	2021-07-15T204305_MORIARTY.vhd	Computer

The Need for Speed

Triage collections can be collected and processed in minutes versus hours

RAM is worth the time

Typical collections averaging 10-15 minutes

From **Acquisition** to **Evidence Analysis** in 90 minutes or less



Wrap Up

Preparation:

People, Practice, Files staged;
Evaluate Deployment Options

Consider your KAPE(s):

What collection elements best suit your requirements?

Contribute:

CSIRT-Collect is Open Sourced

Fork - Contribute



Resources

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

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

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>

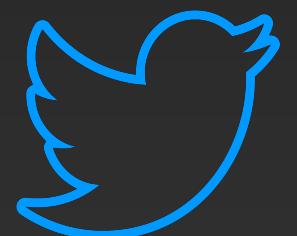
FOR498 – Battlefield Forensics & Acquisition: <https://www.sans.org/cyber-security-courses/battlefield-forensics-and-data-acquisition/>

Blog: <https://bakerstreetforensics.com>

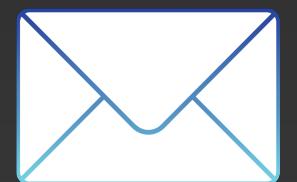
Thank You



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



@dwmetz



dwmetz@gmail.com

