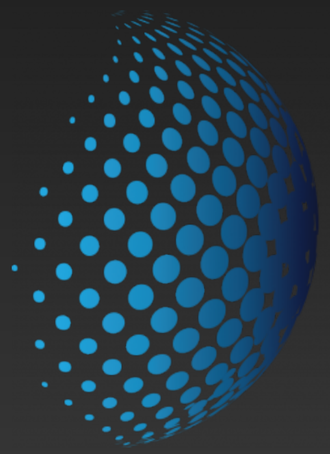
PowerShell Tools for IR Forensics Collection

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  ange 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

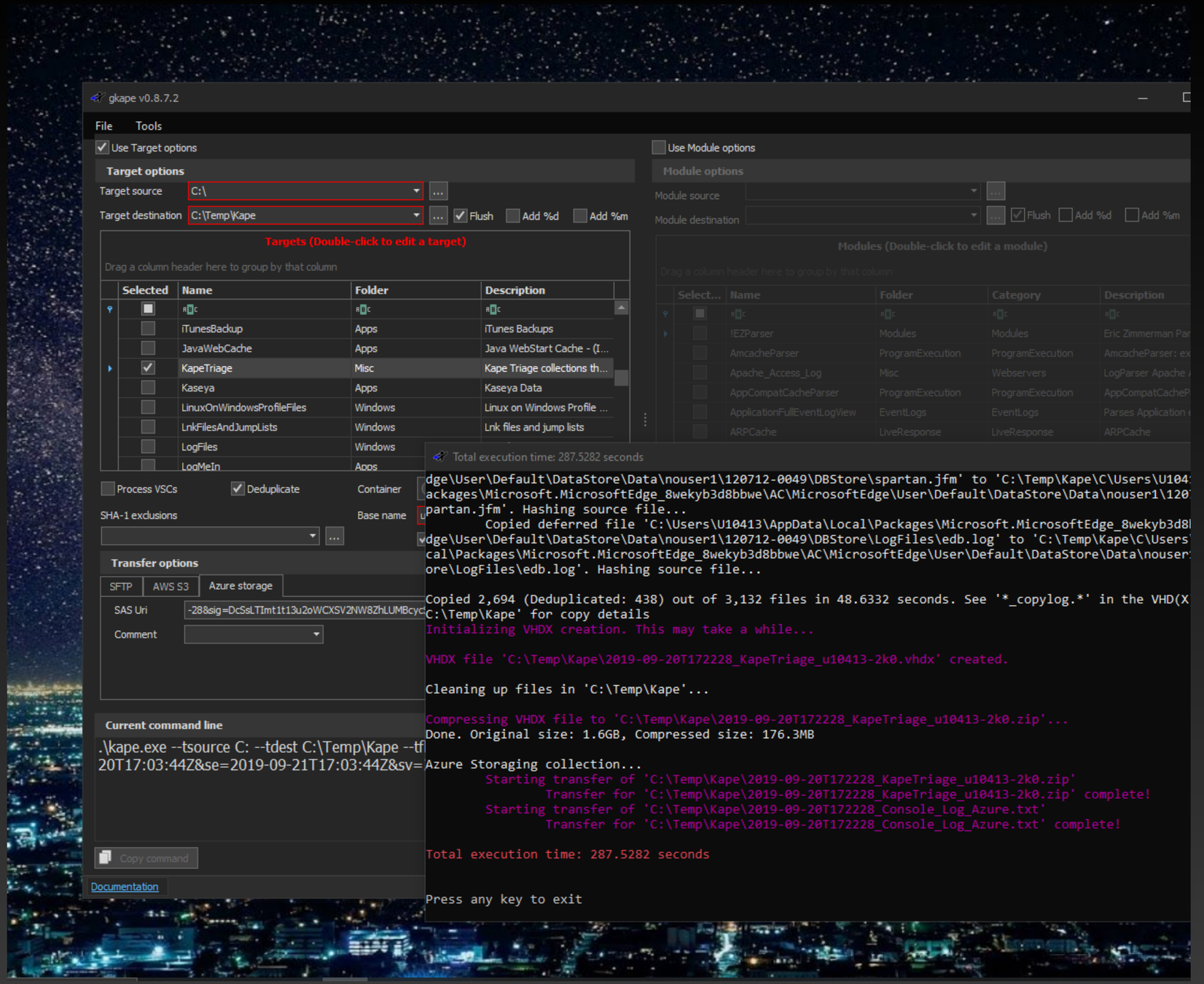
KAPE has two primary components, Targets & Modules.

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.

KAPE



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

```
[System.Environment]::OSVersion.Version > C:\Temp\IR\windowsbuild.txt
Write-Host -Fore Green "Renaming file..."
Get-ChildItem -Filter "*windowsbuild*" -Recurse | Rename-Item -NewName {$_.name -replace

## create output directory on "Collections" share
mkdir X:\$env:COMPUTERNAME

Write-Host -Fore Green "Copying memory image to network..."

## copy memory image to network
robocopy . "\\Synology\Collections\$env:COMPUTERNAME" *.7z *.txt

## delete the directory and contents
Write-Host -Fore Green "Removing temporary files"
Set-Location C:\TEMP
Remove-Item -LiteralPath "C:\temp\IR" -Force -Recurse

## create the KAPE directory on the client
Write-Host -Fore Green "Creating KAPE directory on host..."
mkdir C:\Temp\KAPE -Force

## execute the KAPE "OS" collection
Write-Host -Fore Green "Collecting OS artifacts..."
Set-Location X:\KAPE
.\kape.exe --tsource C: --tdest C:\Temp\KAPE --target !SANS_Triage --vhdx $env:COMPUTERN


## transfer evidence to share
Set-Location C:\Temp\Kape
robocopy . "\\Synology\Collections\$env:COMPUTERNAME"

## delete the local directory and contents
Write-Host -Fore Green "Removing temporary files"
Set-Location C:\TEMP
Remove-Item -LiteralPath "C:\temp\KAPE" -Force -Recurse
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

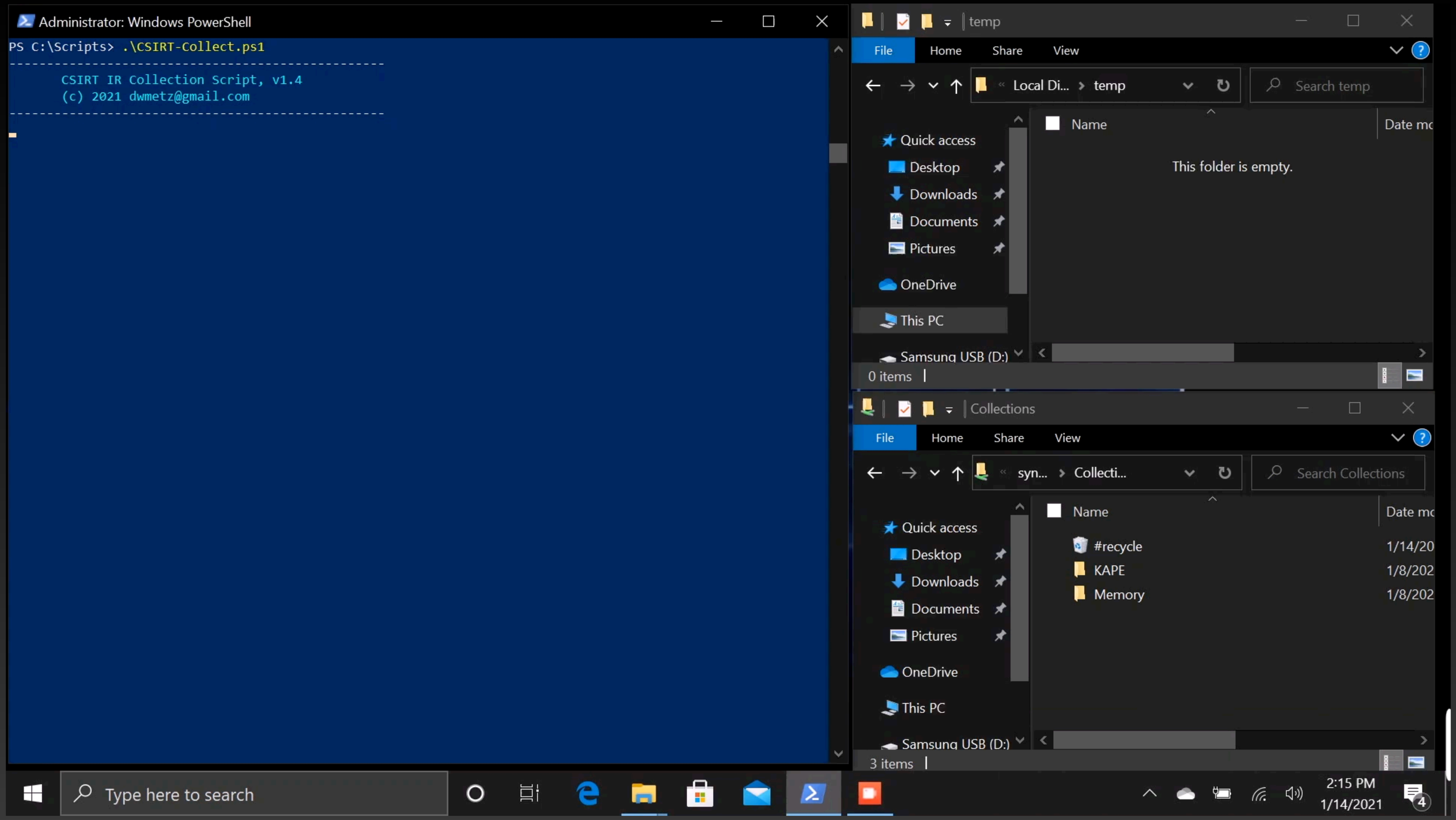
Easily portable (network share, USB, Azure/AWS)

Deployment Options

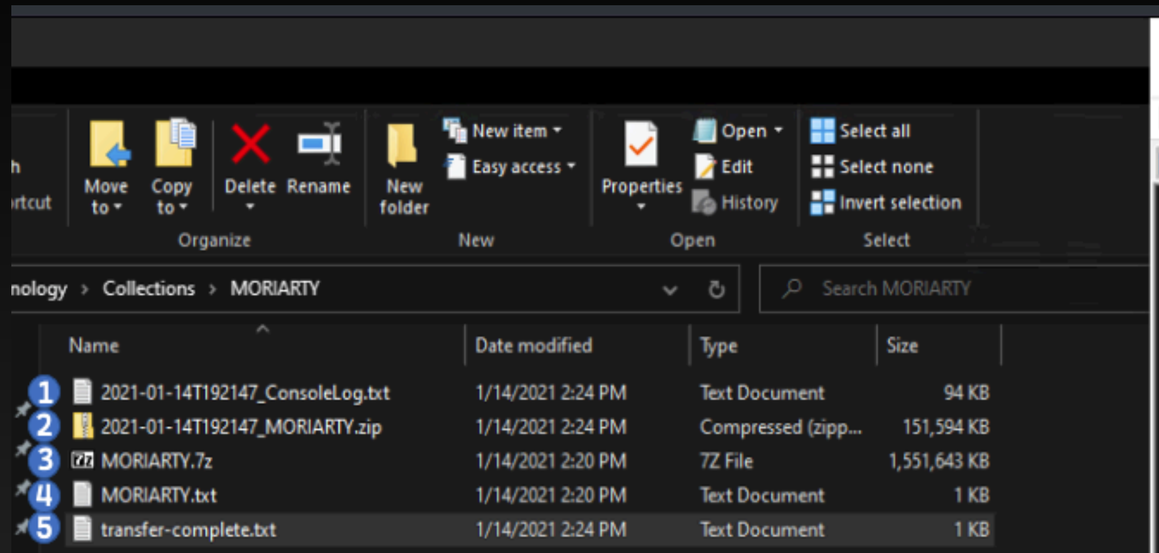
- SOC (Security Operations Center)
- Help Desk
- Field Support / Local IT
- Group Policy
- SOAR (Automation)
- EDR (Endpoint Detection and Response)
- USB Media *

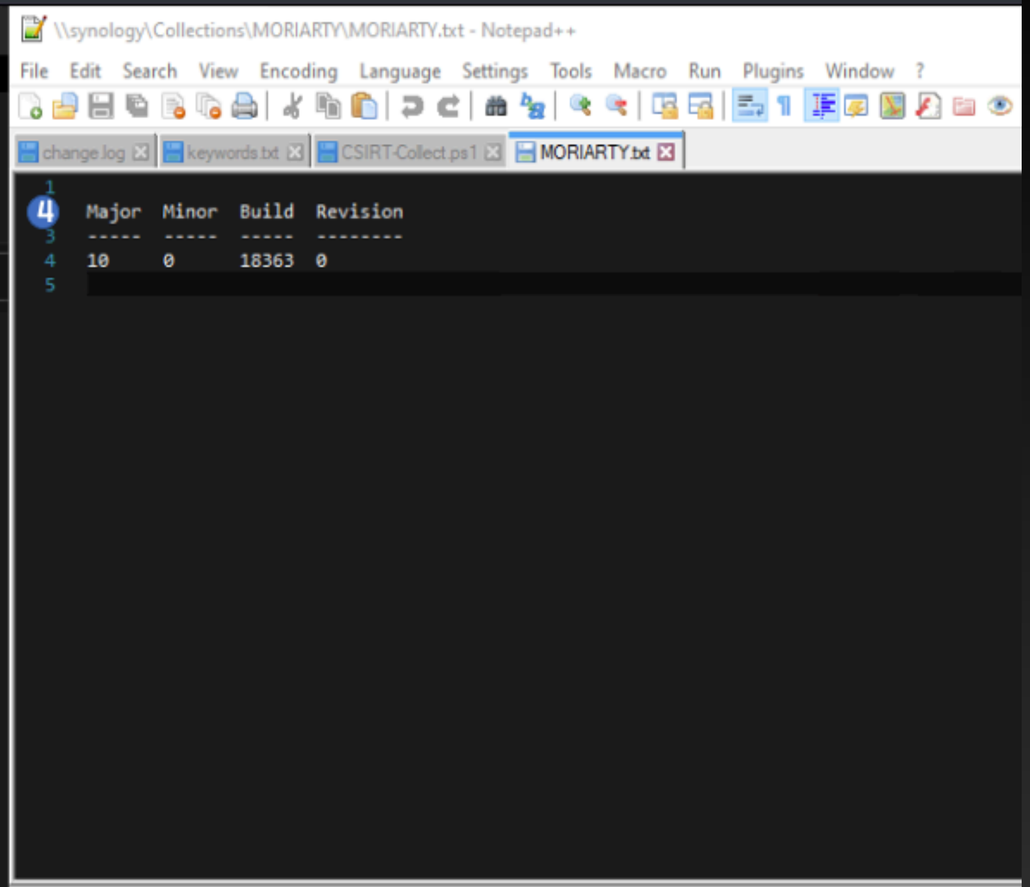
CSIRT-Collect.ps1 Demo

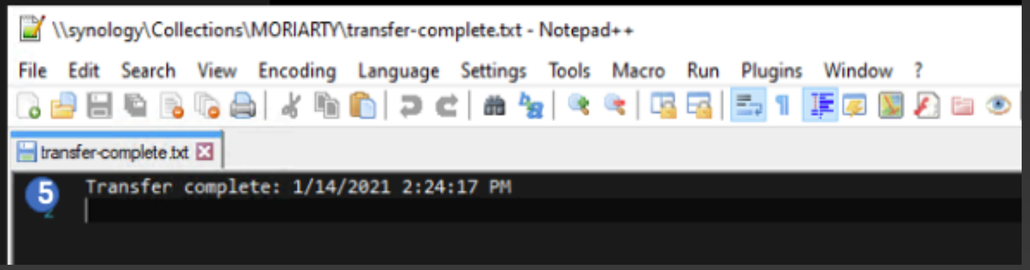
May the Demo gods smile on us


Administrator: Windows PowerShell
PS C:\Scripts> .\CSIRT-Collect.ps1
CSIRT IR Collection Script, v1.4
(c) 2021 dwmetz@gmail.com
temp
File
Home
Share
View
Local Di... › temp
Search temp
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Samsung USB (D:)
Name
Date mo
This folder is empty.
0 items
Collections
File
Home
Share
View
syn... › Collecti...
Search Collections
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Samsung USB (D:)
Name
Date mo
#recycle
1/14/20
KAPE
1/8/202
Memory
1/8/202
3 items
Type here to search
2:15 PM
1/14/2021
4

Reviewing the Collection Output





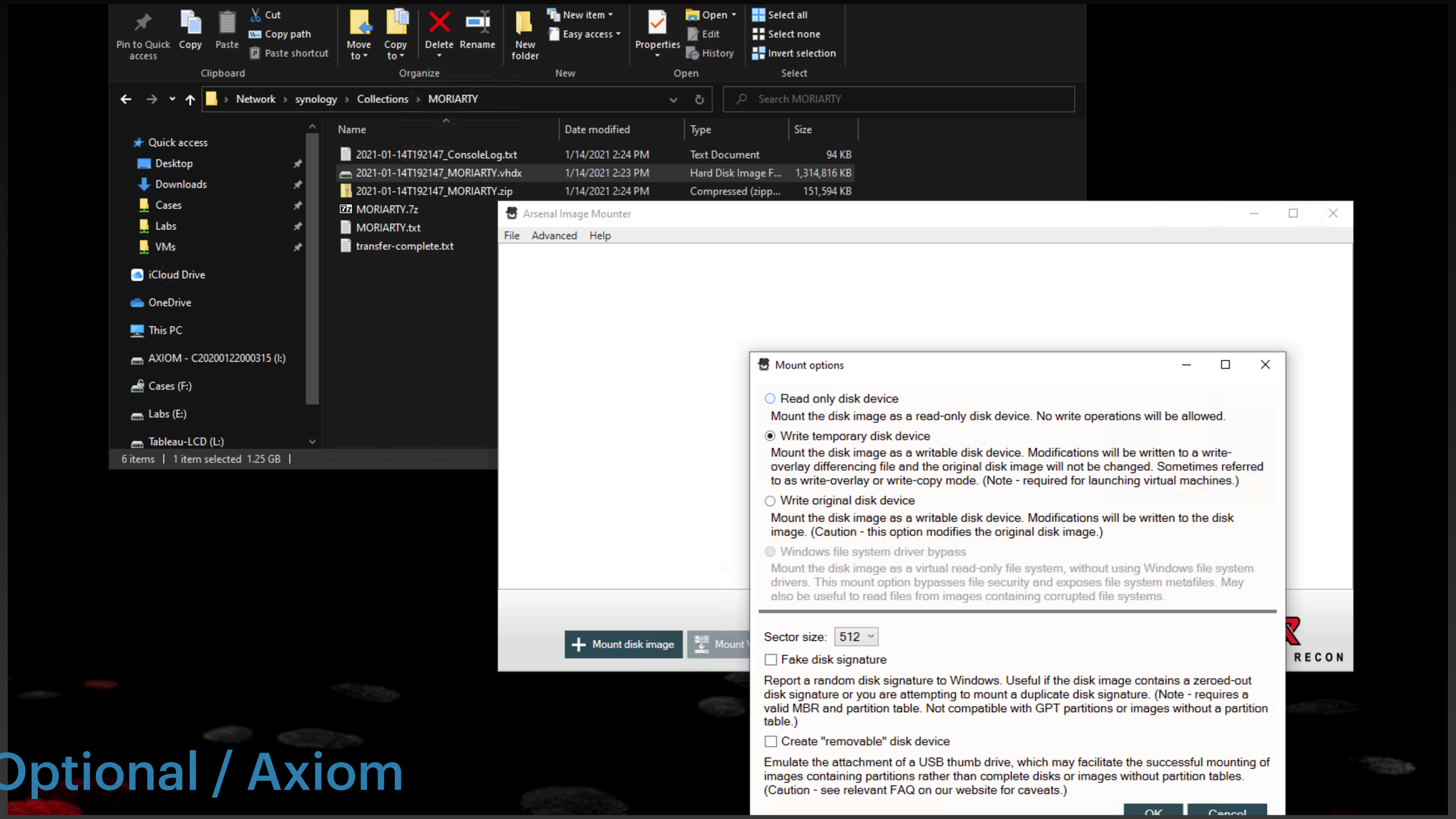


Files Generated:

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

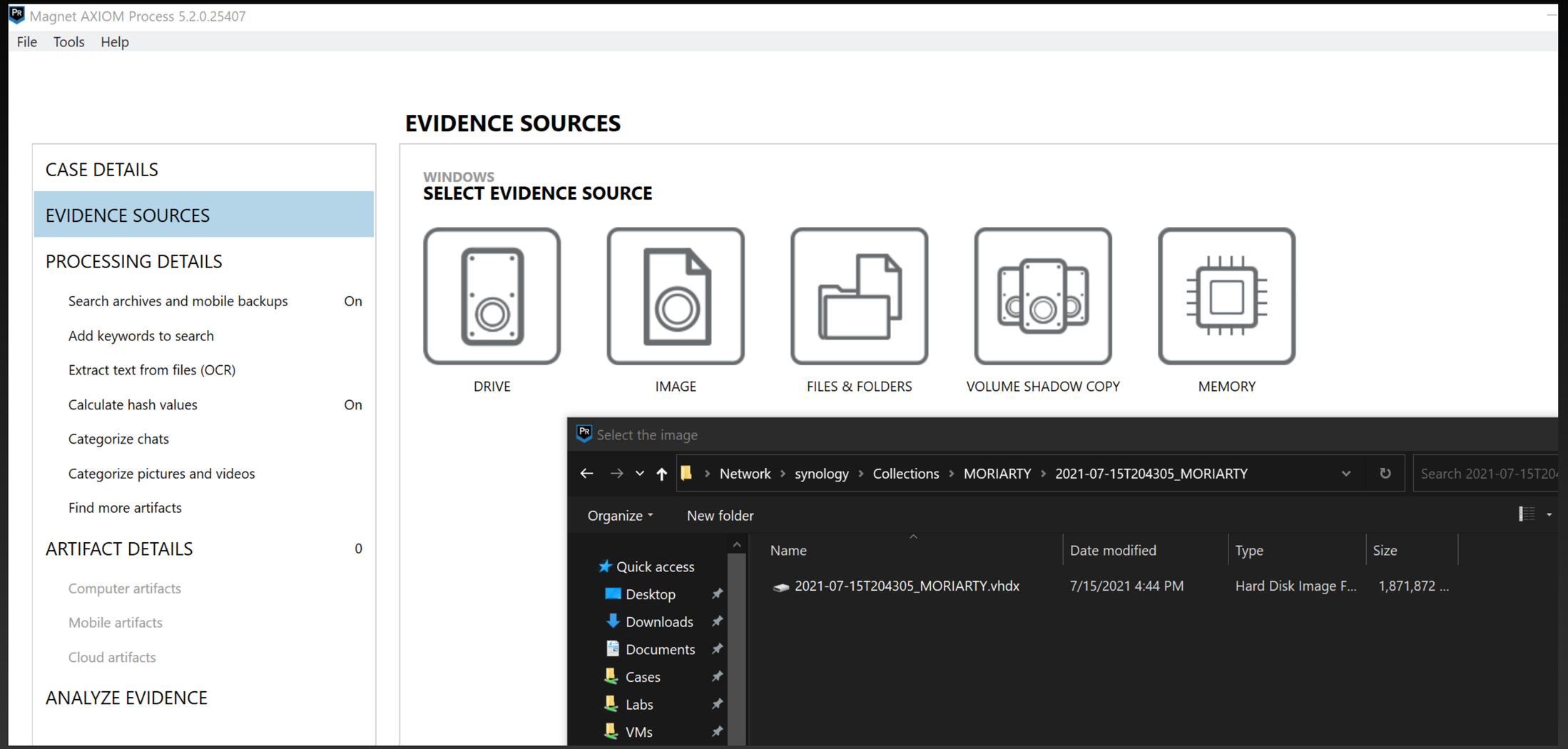
Evidence Processing Tips

Mount the VMDK with Arsenal Image Mounter



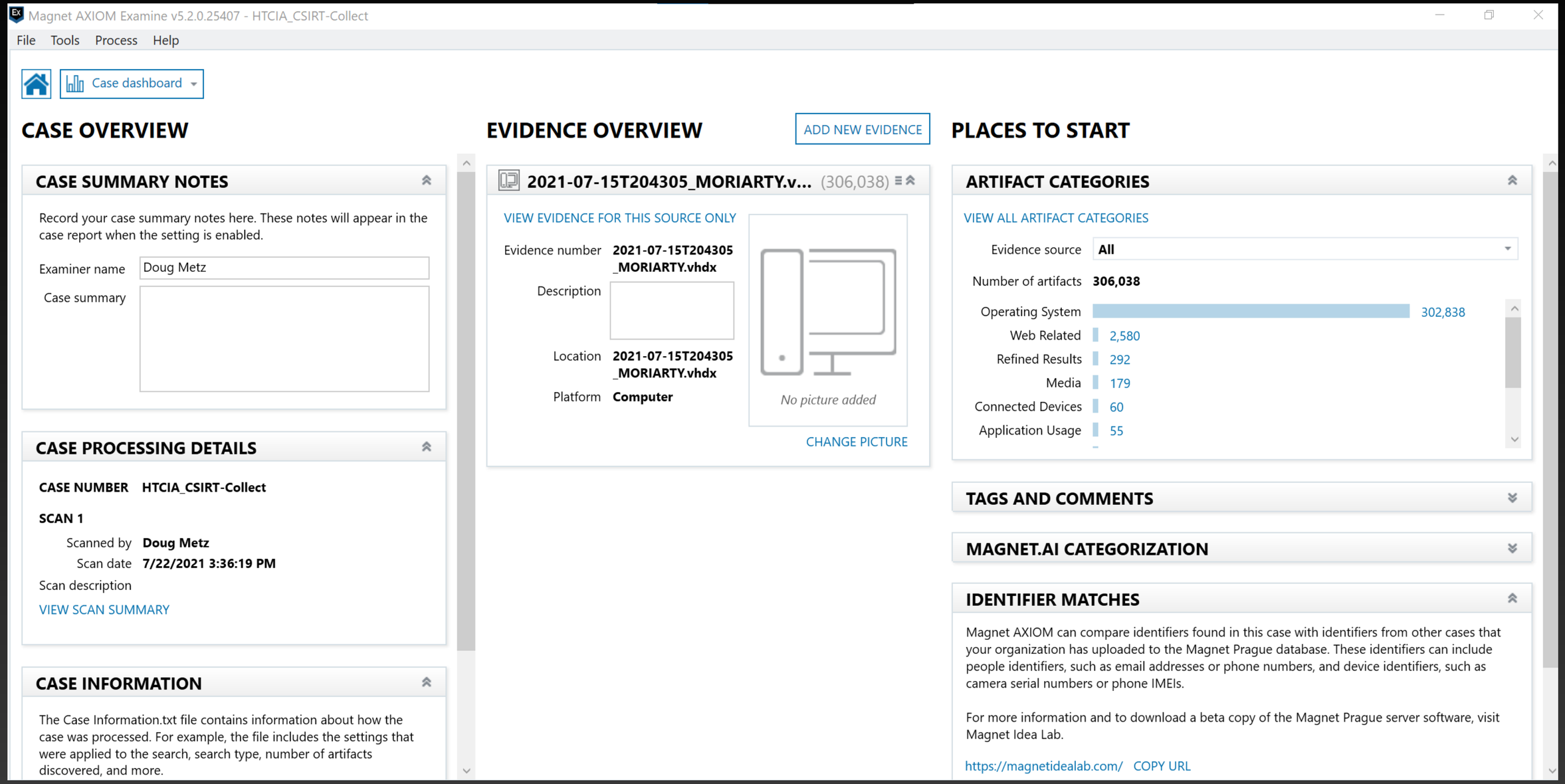
* Optional / Axiom

Process the VMDK



Computer > Windows > Load Evidence > IMAGE

Artifacts from VMDK

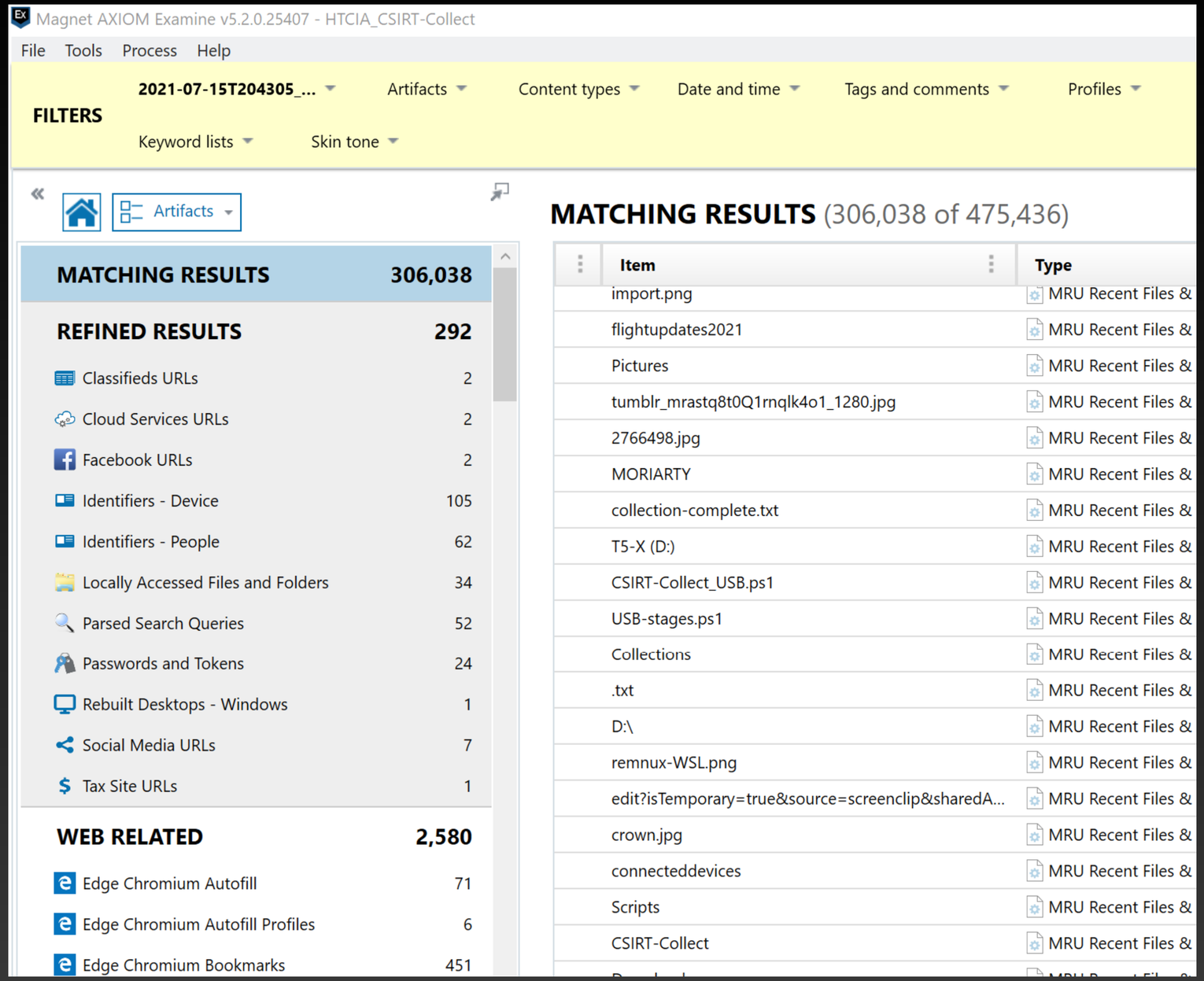


Under the KAPE

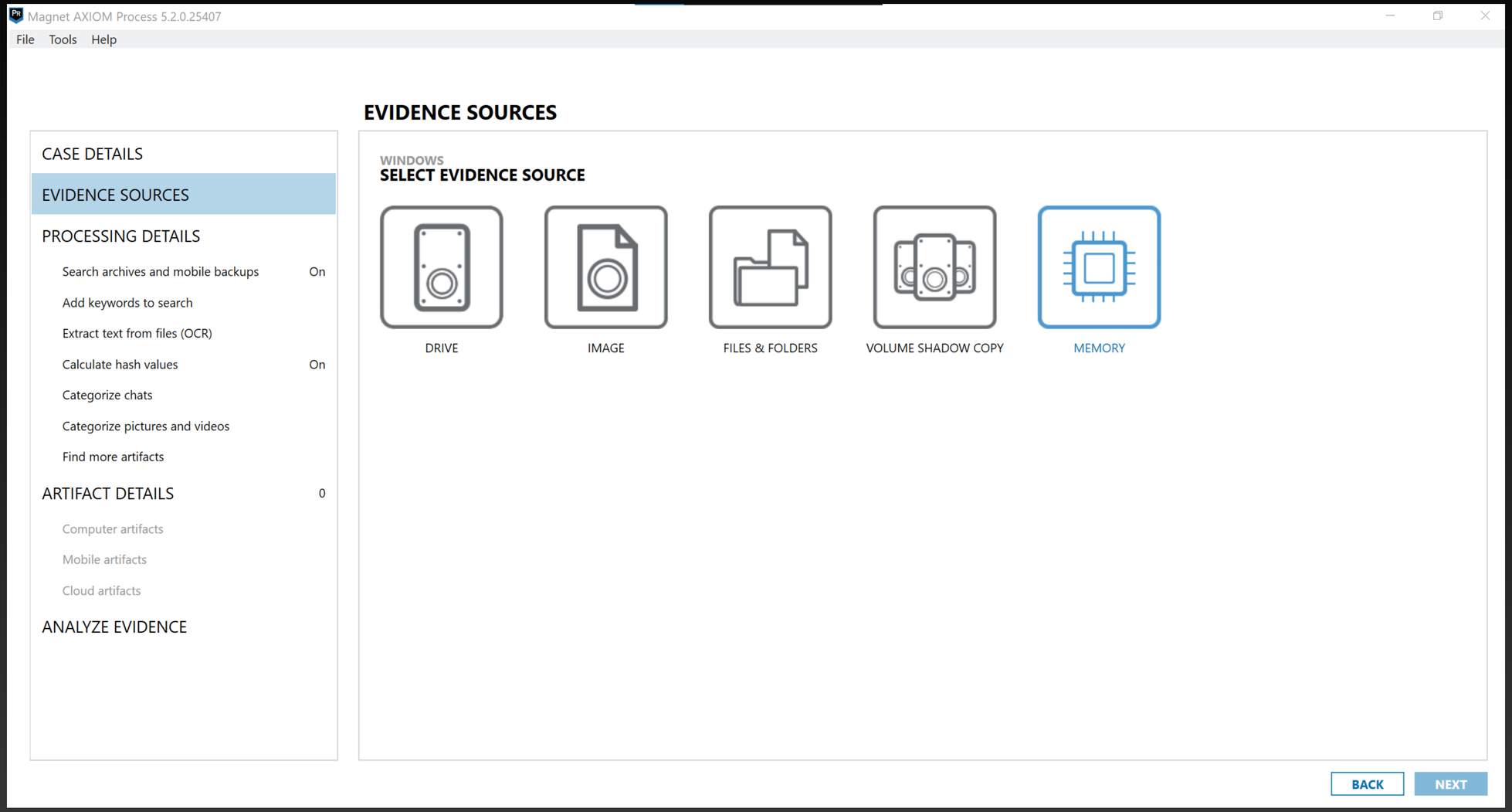
KAPE: 1.8GB Collection > 300,000+ Artifacts

Customize KAPE to collect what only what you need for investigation

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

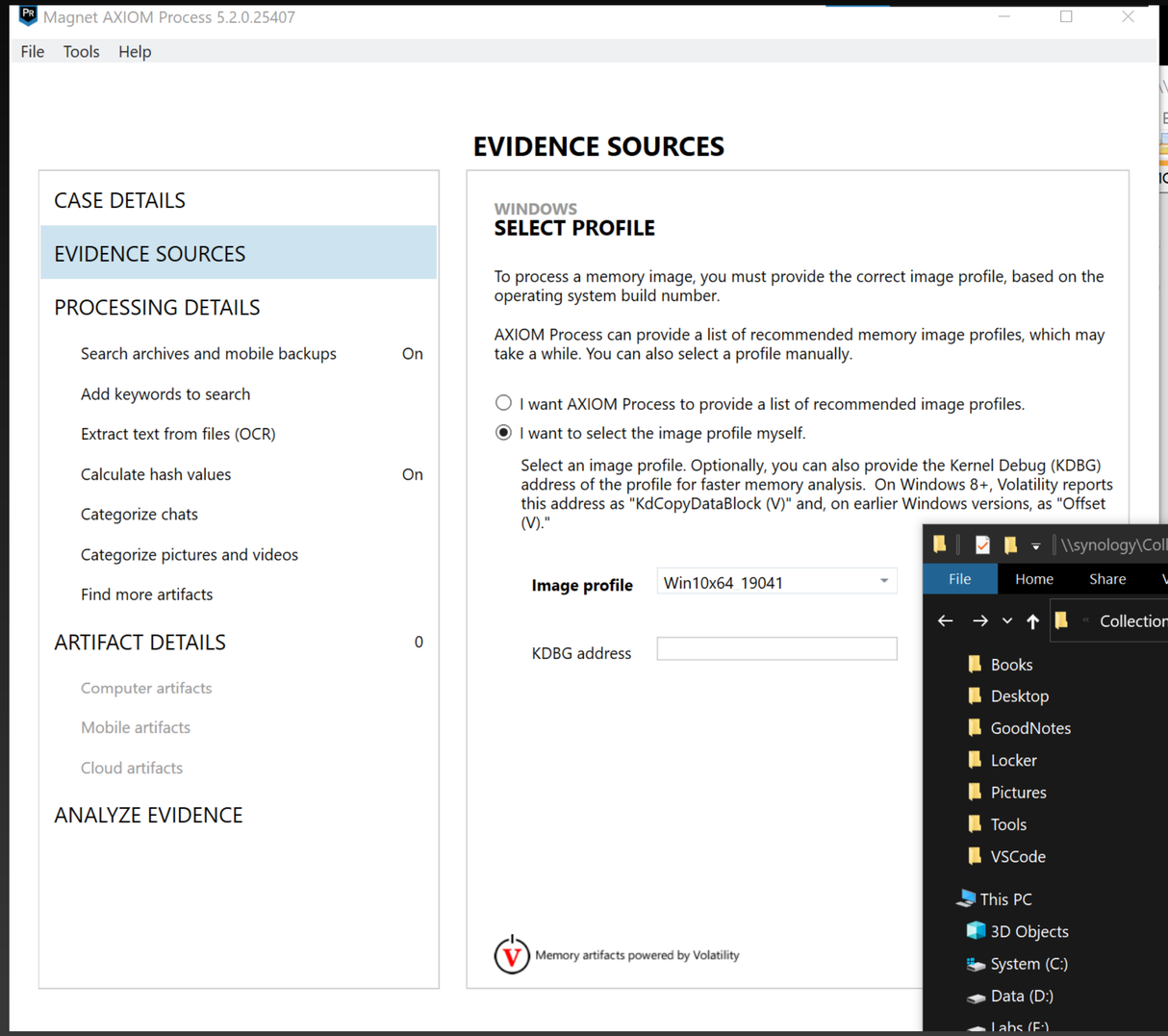


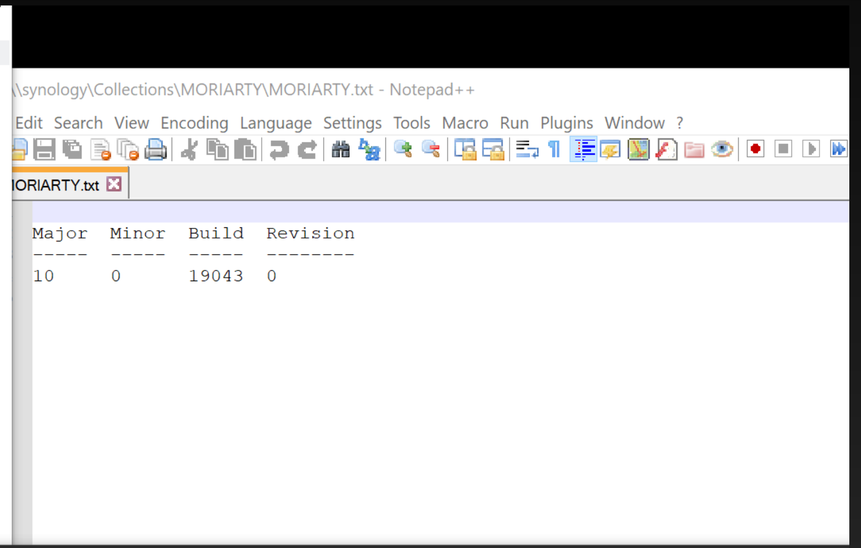
Memory Processing

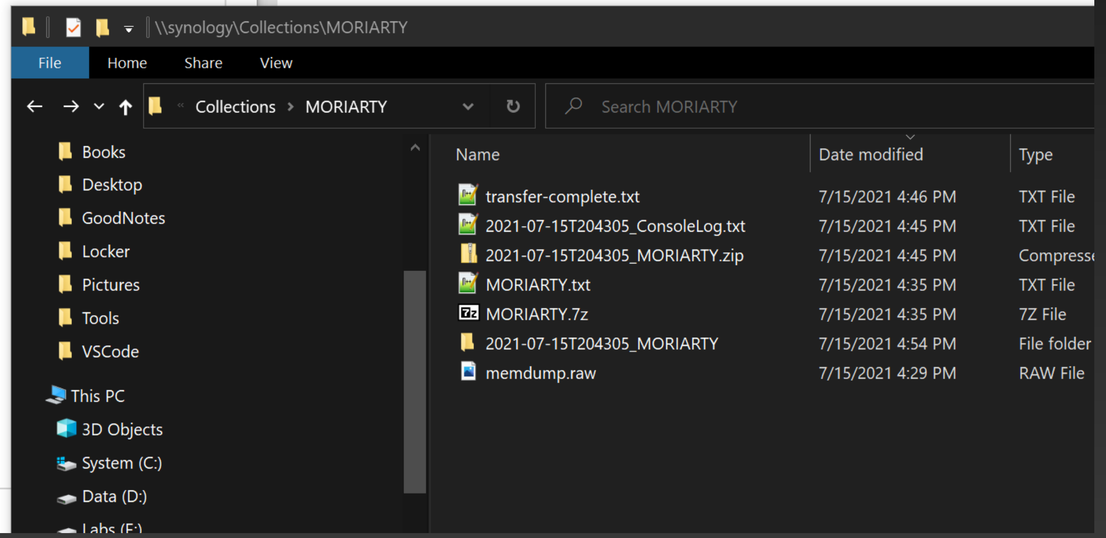


Memory Processing

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





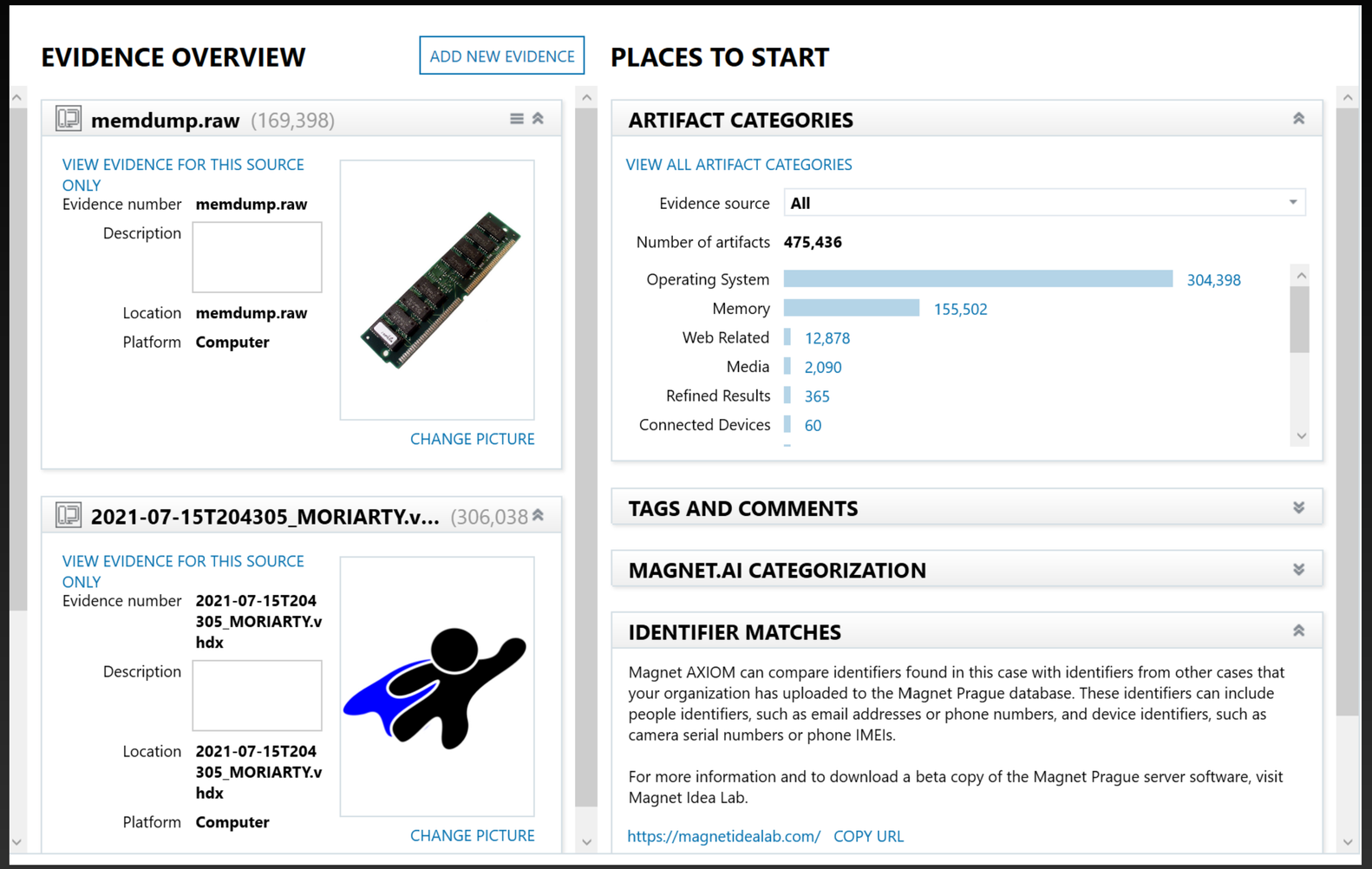


Bring it all together with Axiom

Combine Memory and Triage Collections in Axiom

Combine collections from multiple assets (Connections)

Timeline of activity for multiple assets



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-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

Thank You

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

@dwmetz

dwmetz@gmail.com