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

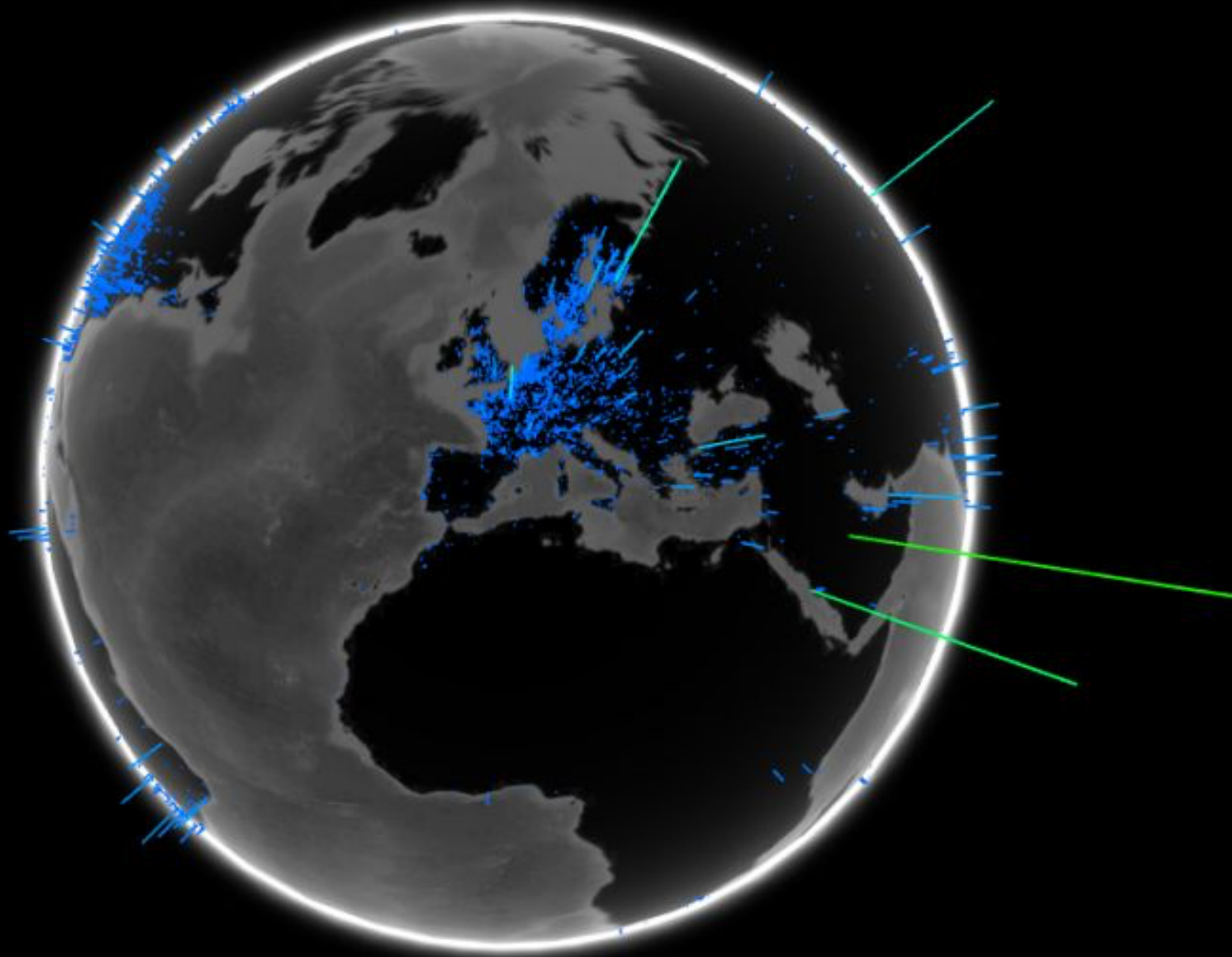
Affiliations:
SANS Advisory Board
DFIR Review
FIRST
HTCIA

ND Alumni #GoIrish

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



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

```
## map the network drive and change to that directory
Write-Host -Fore Green "Mapping network drive..."

$Networkpath = "X:\"


If (Test-Path -Path $Networkpath) {
    Write-Host -Fore Green "Drive Exists already"
}
Else {
    #map network drive
    (New-Object -ComObject WScript.Network).MapNetworkDrive("X:","\\Synology\Collections")

    #check mapping again
    If (Test-Path -Path $Networkpath) {
        Write-Host -Fore Green "Drive has been mapped"
    }
    Else {
        Write-Host -For Red "Error mapping drive"
    }
}
#Remove-PSDrive -Name X
#New-PSDrive -Name X -PSProvider FileSystem -Root "\\Synology\Collections"

# create local memory directory
Write-Host -Fore Green "Setting up local directory..."
mkdir C:\temp\IR -Force
Set-Location C:\temp\IR
Write-Host -Fore Green "Copying tools..."
robocopy "\\Synology\Collections\Memory" . *.exe
## capture memory image
Write-Host -Fore Green "Capturing memory..."
.\winpmem.exe memdump.raw
```

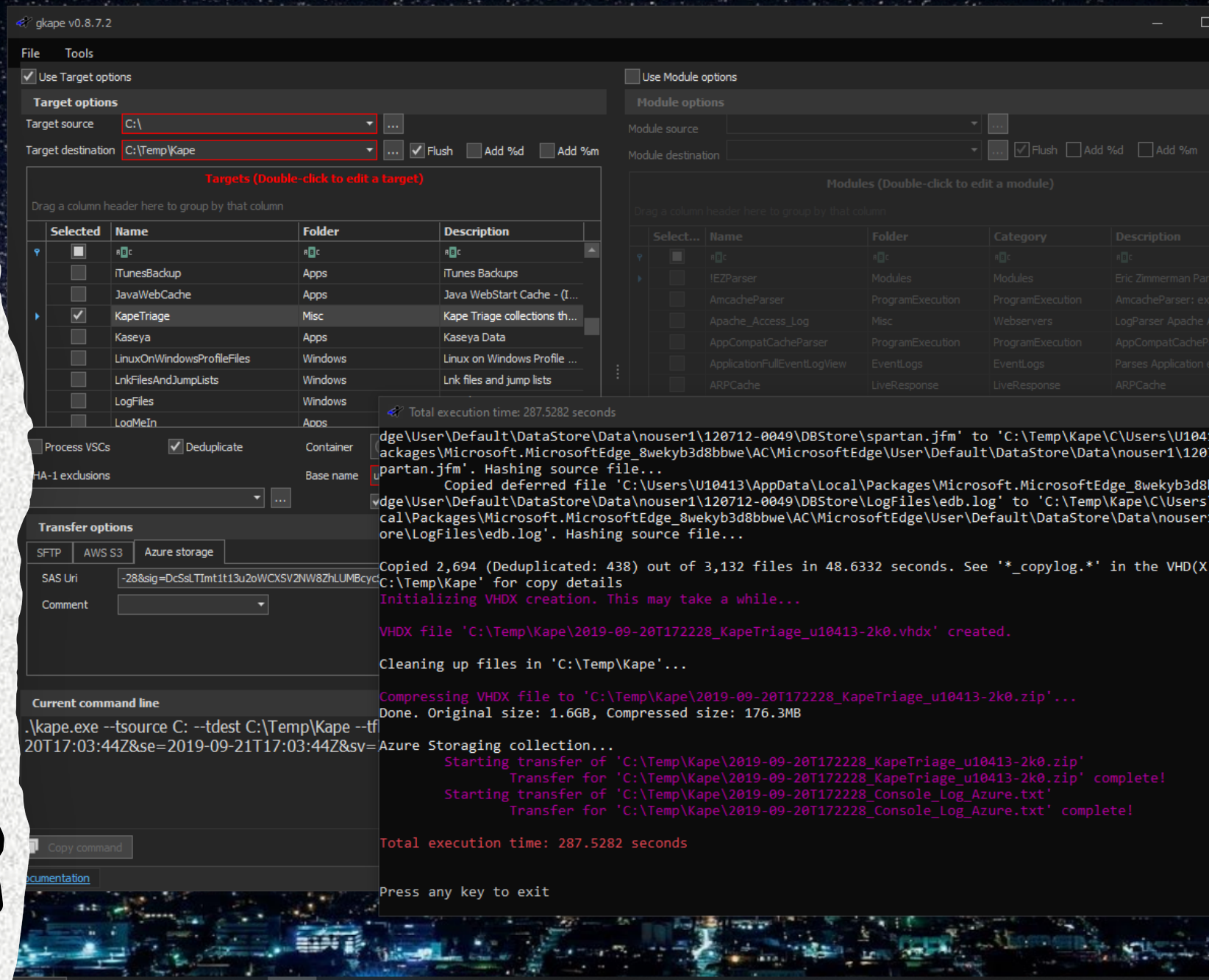
KAPE:

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

```
[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 ‘win

## create output directory on "IR" 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:COMPUTERNAME


## 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
```

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

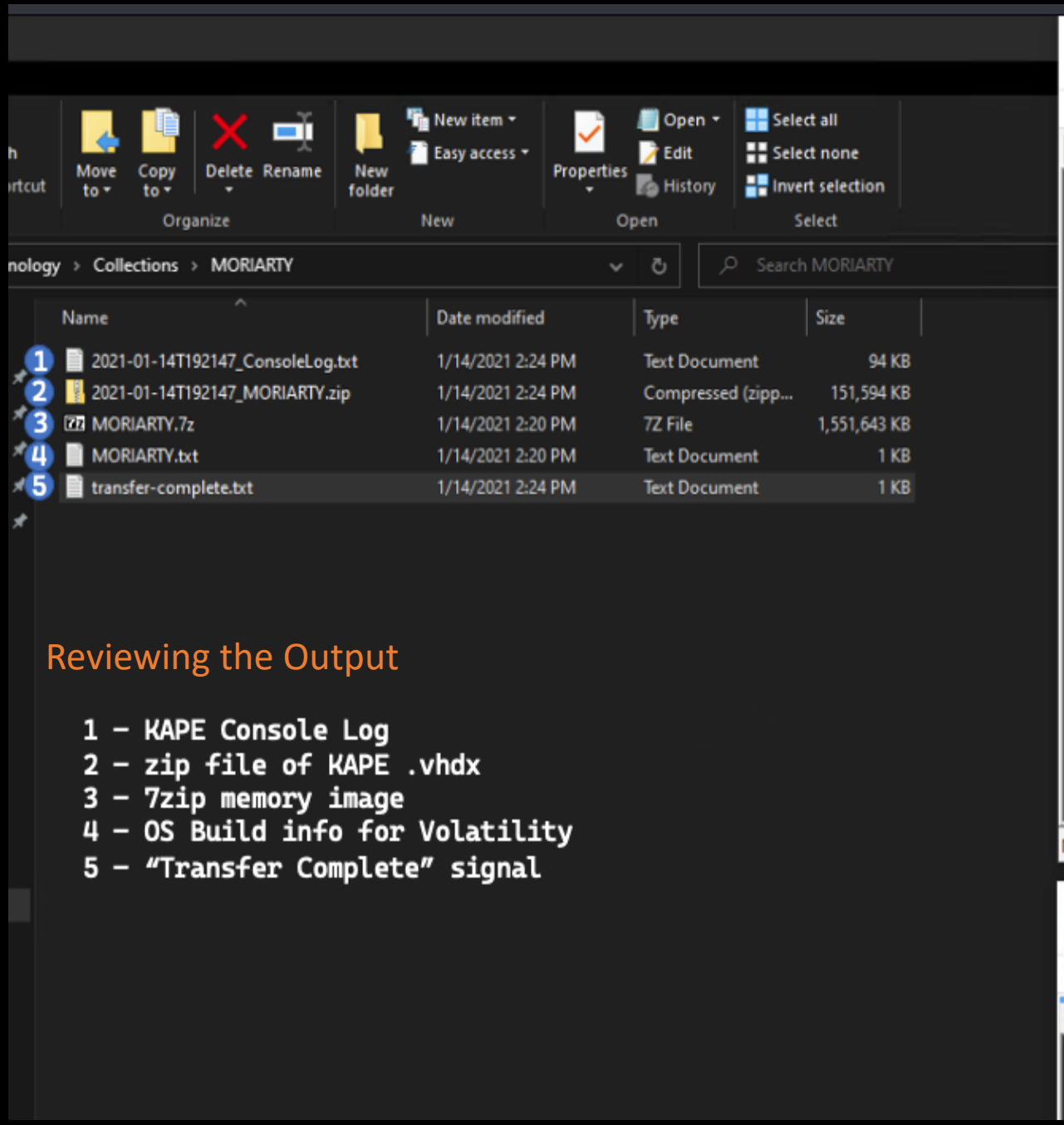
Data management on endpoints helps to preserve disk space

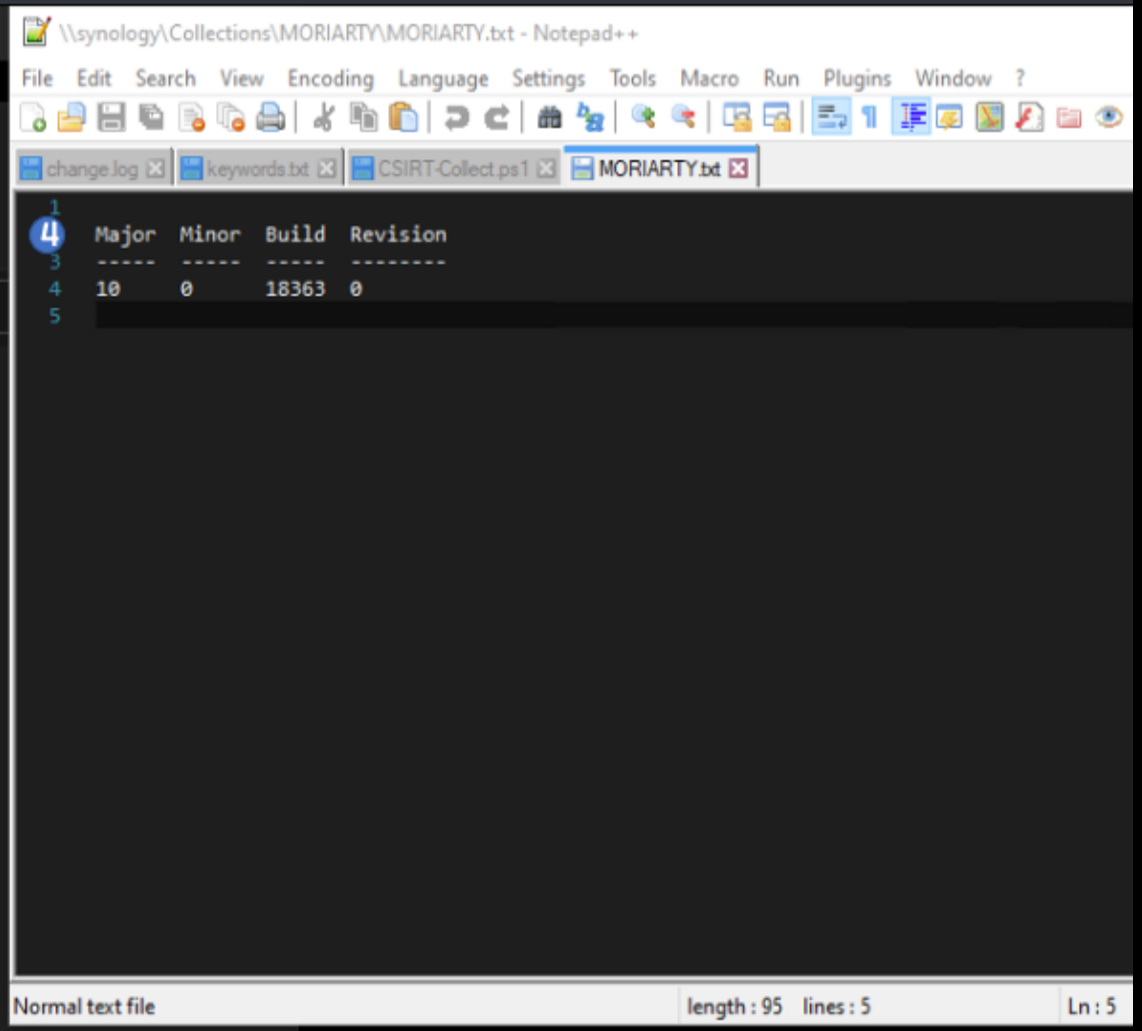
Easily portable (network share, USB, Azure/AWS)

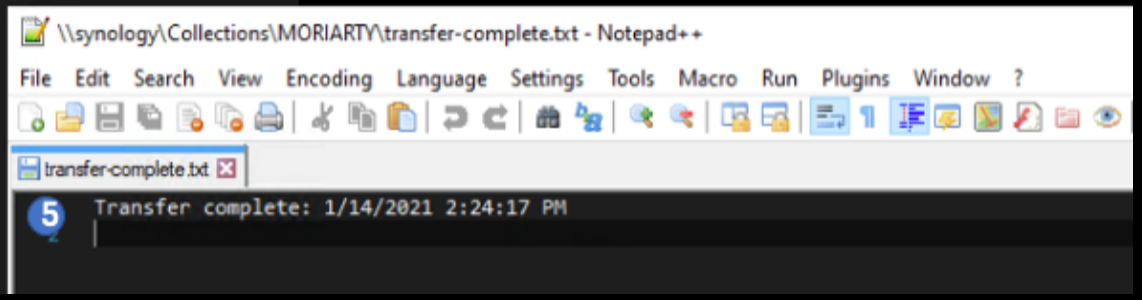
Deployment Options:

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


CSIRT-Collect.ps1
Demo



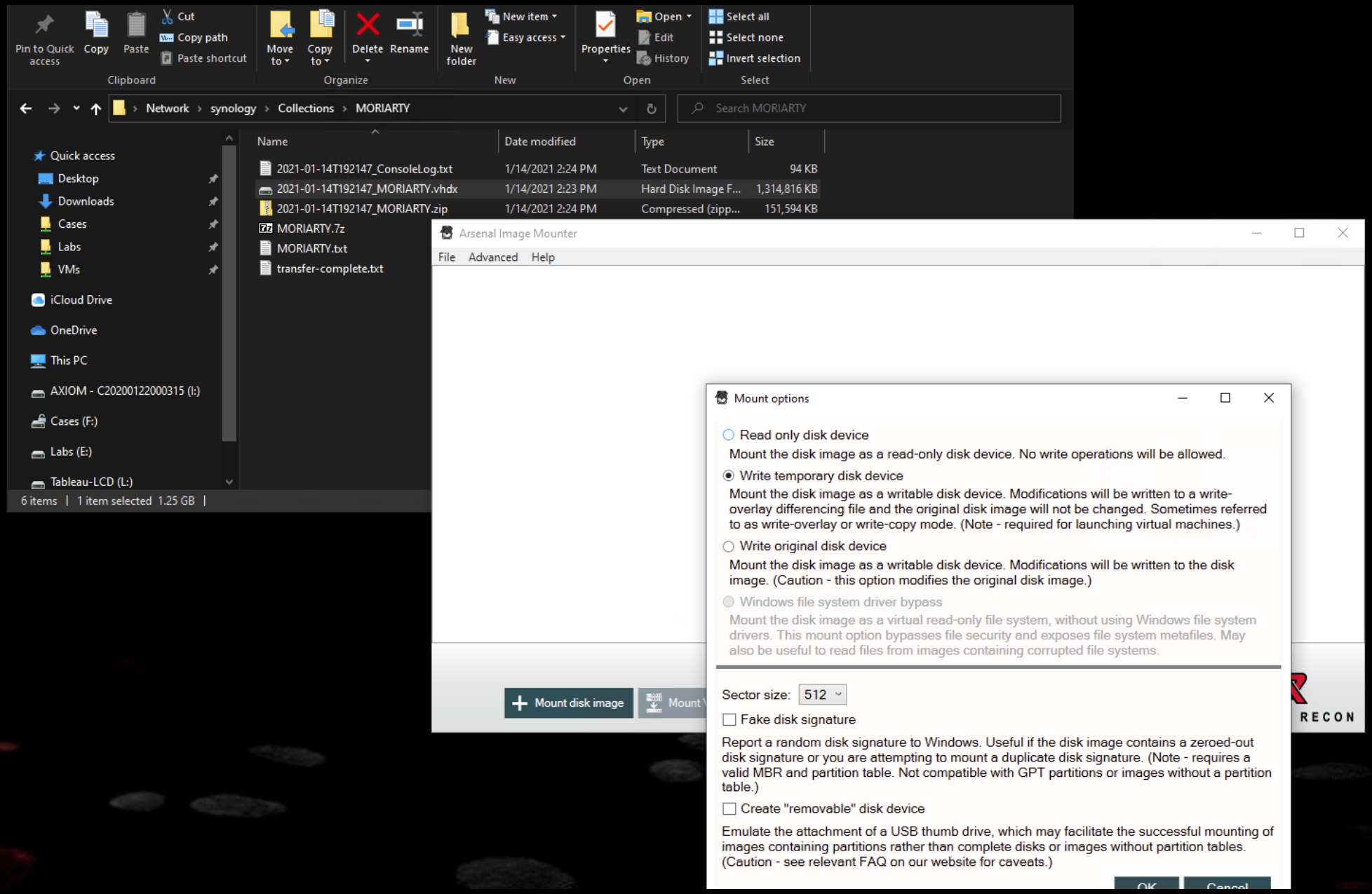




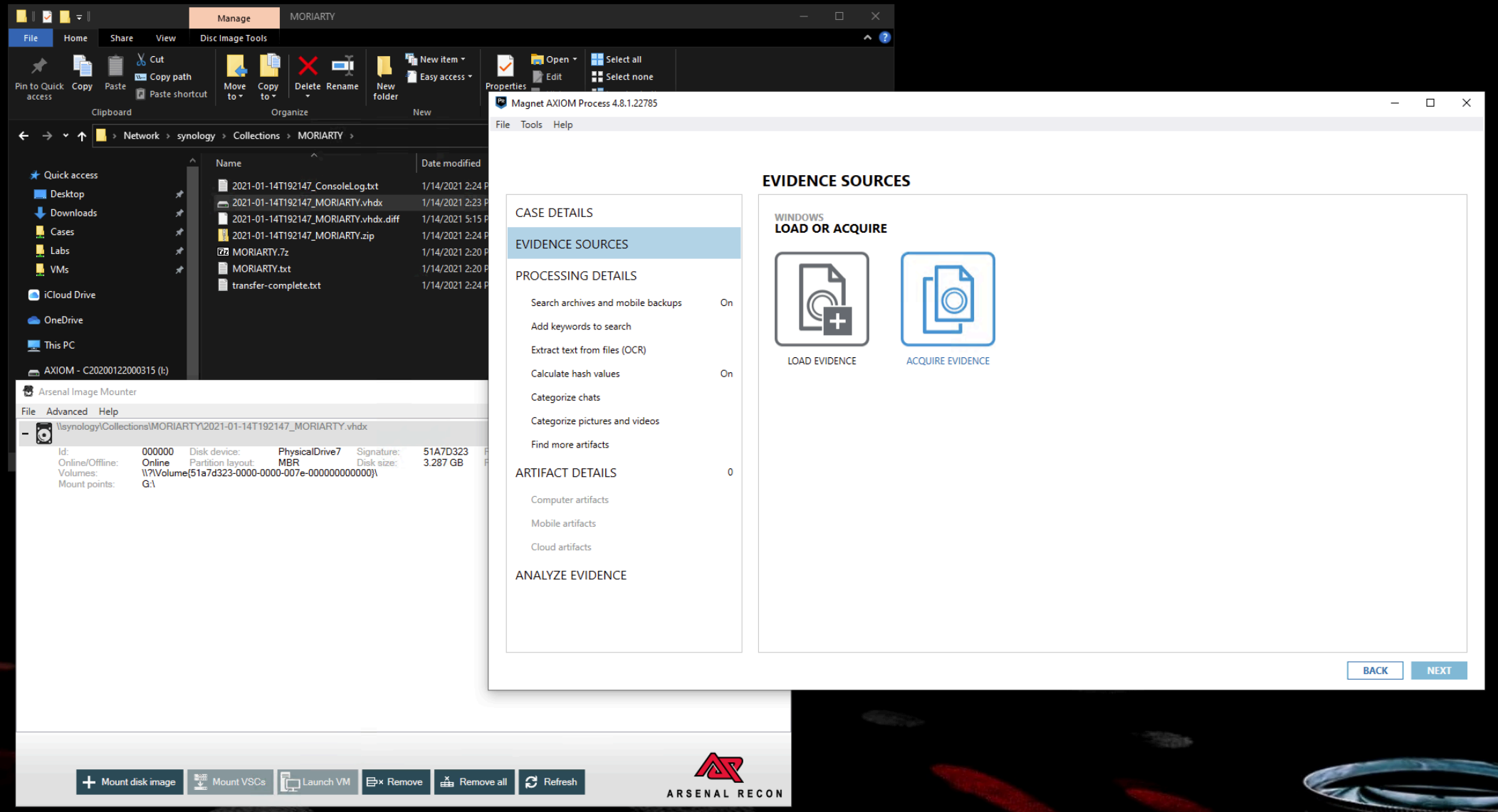
Reviewing the Output

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

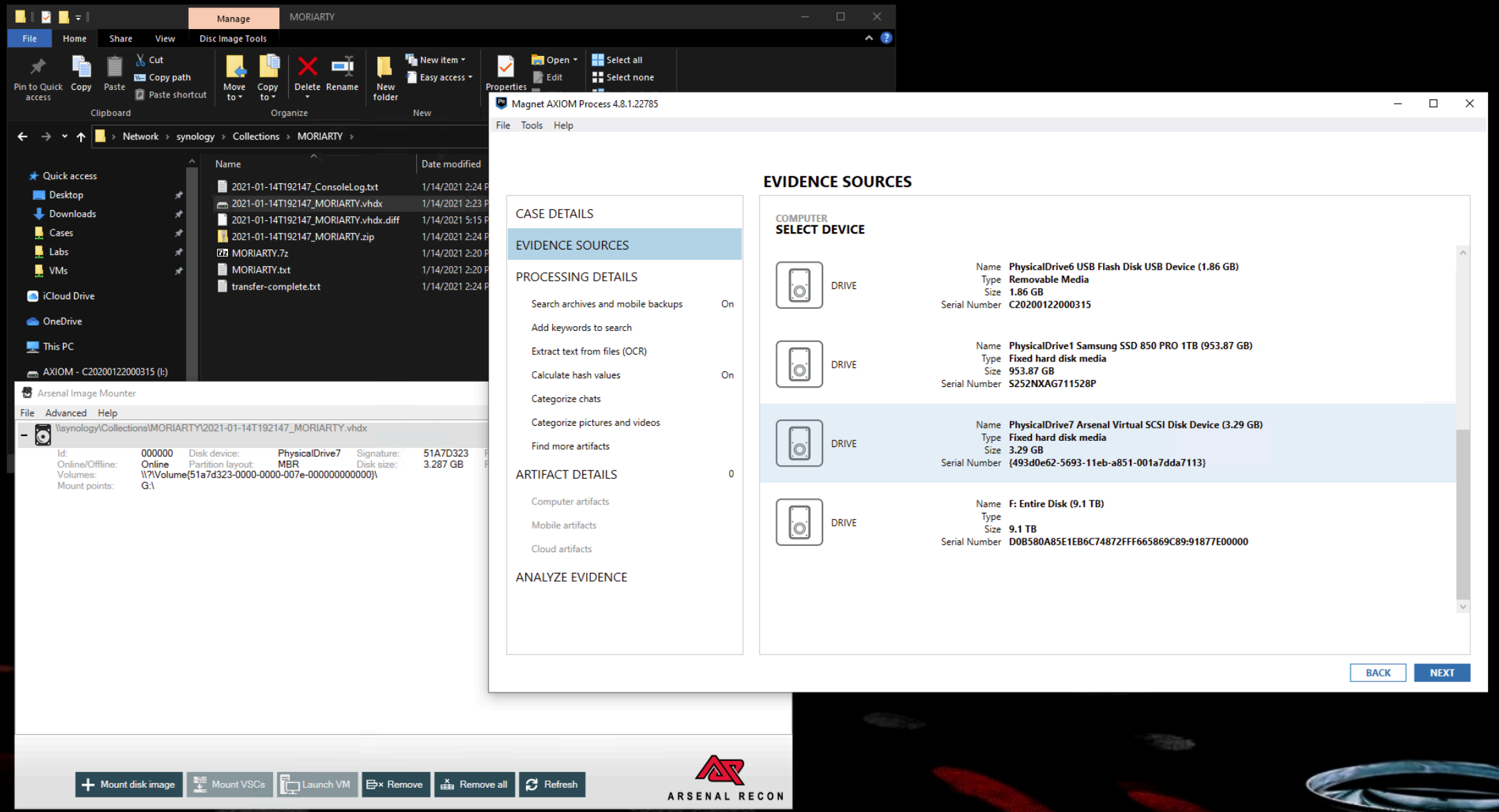
Mount the VMDK with Arsenal Image Mounter



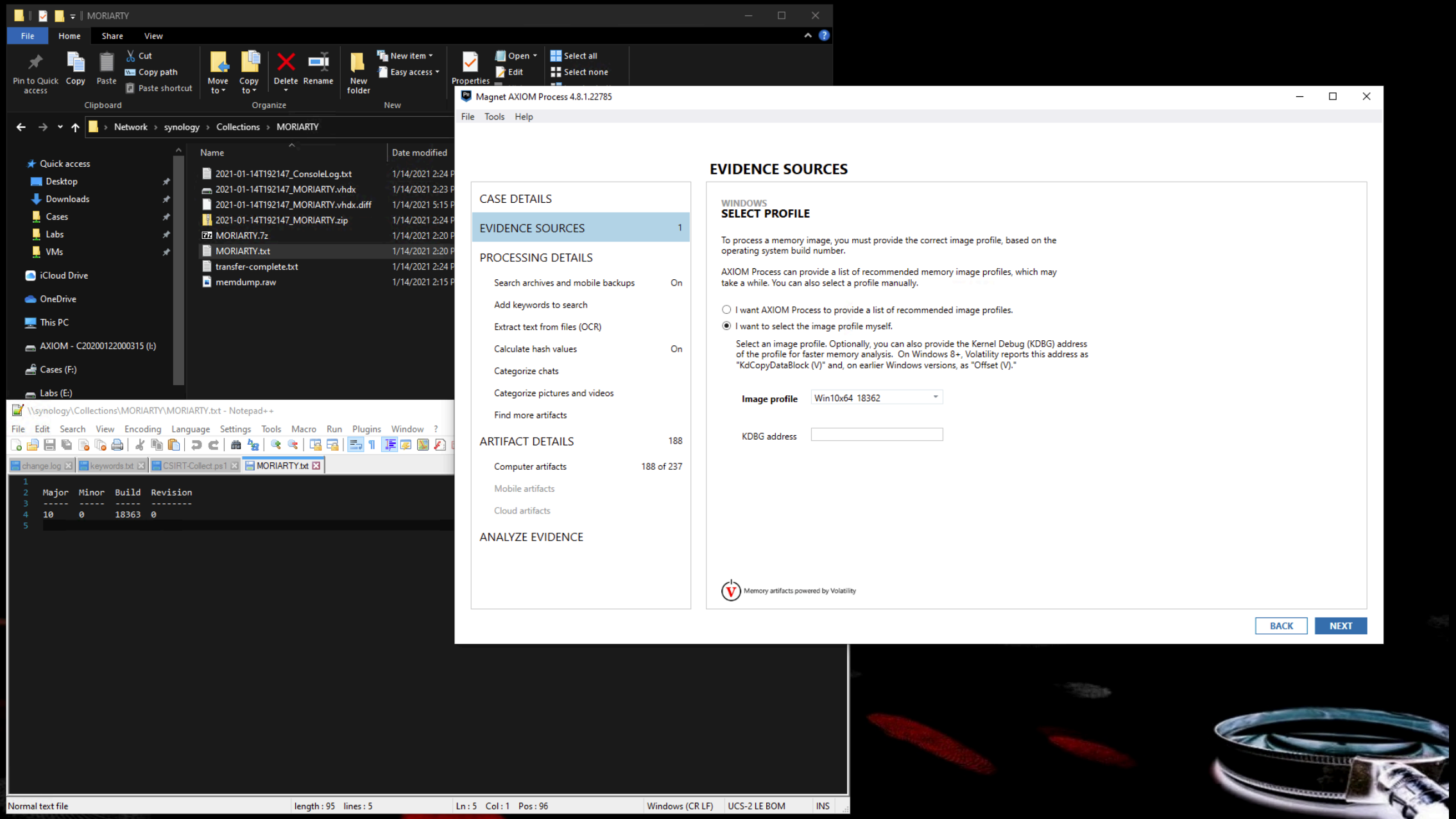
AQUIRE the mounted image with Axiom Process



AQUIRE the mounted image with Axiom Process (2)



Use the Build Info .txt for Memory Profile

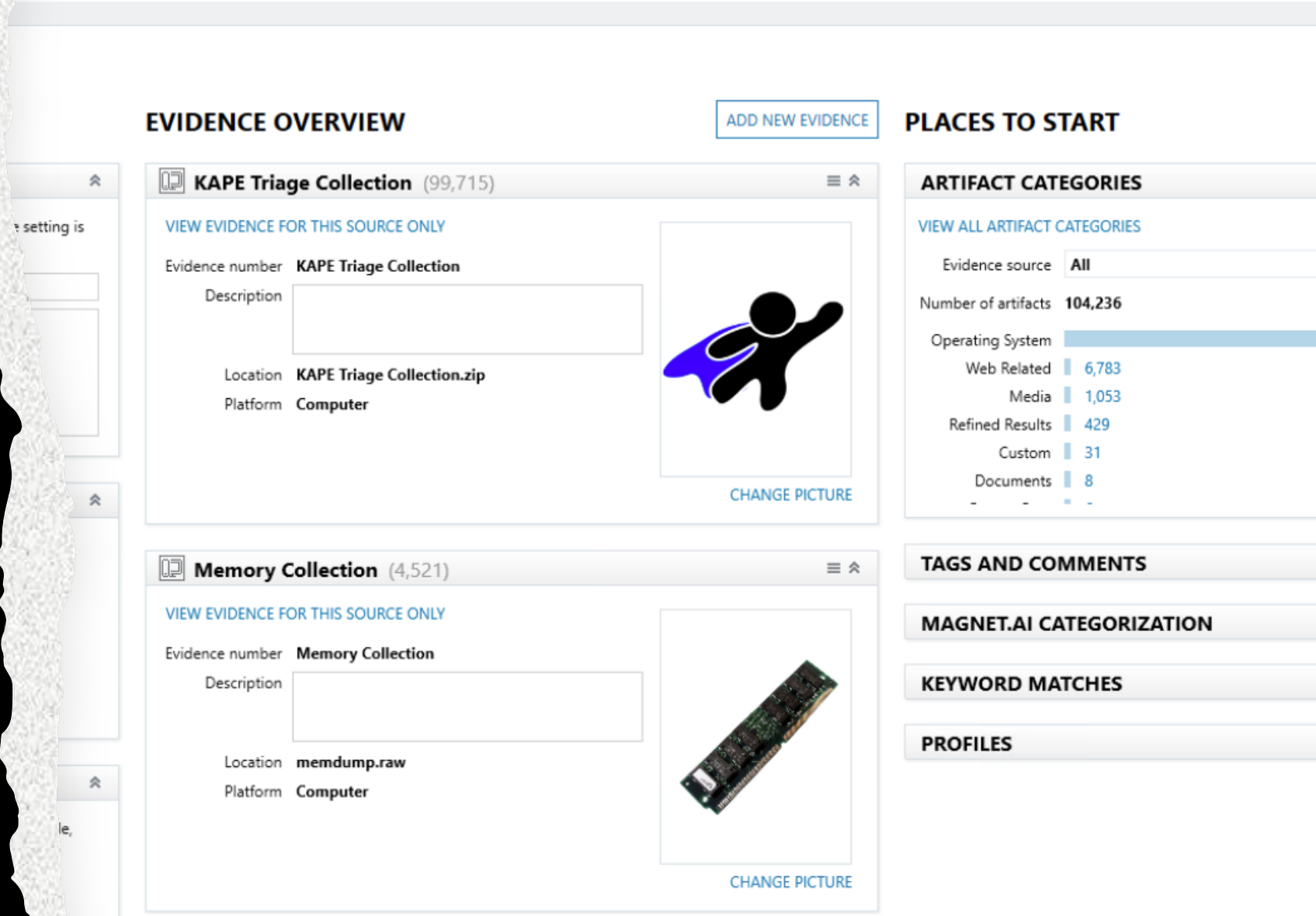


Bring it all into Axiom

Combine Memory and Triage Collections in Axiom

Combine collections from multiple assets (Connections)

Timeline of activity for multiple assets

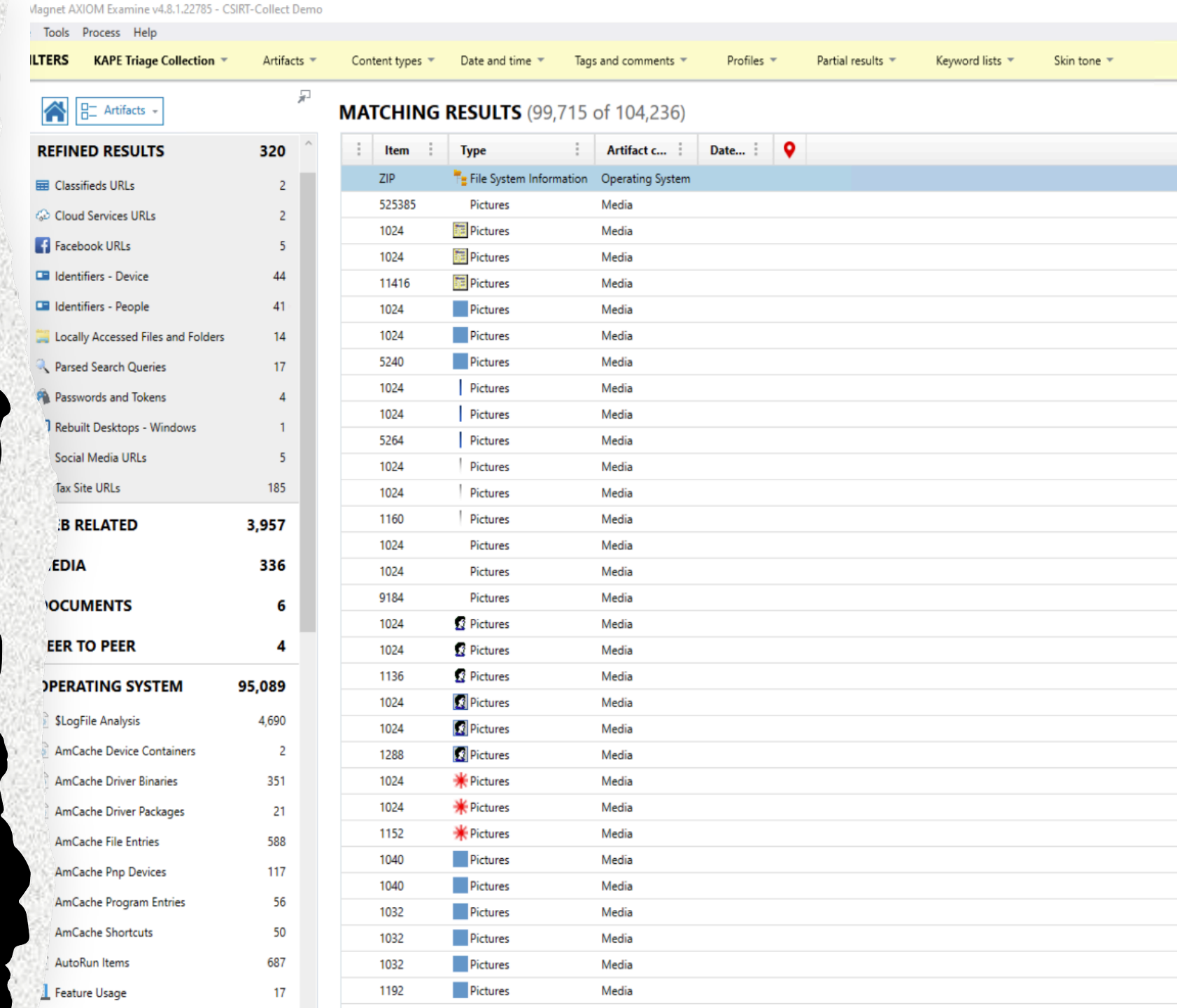


Under the KAPE

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



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

http://bakerstreetforensics.com