



# Time Is Not On Our Side:

Triage Collections in Incident Response Investigations

Doug Metz, Professional Services Consultant  
Magnet Forensics

HTCIA Delaware Valley Chapter  
1<sup>st</sup> Quarter Meeting  
March 31, 2023





# WHO AM I

```
[PS /Users/dmetz> gc ./whoami.txt
```

Professional Services Consultant with Magnet Forensics.

Over 15 years in Incident Response supporting government, private sector, and academic institutions.

(former) Global Incident Response Manager for a Fortune 200 company.

HTCIA Delaware Valley-Philly Chapter

Volunteer for The Magnet Auxtera Project

PowerShell Enthusiast

ND Alumni #GoIrish

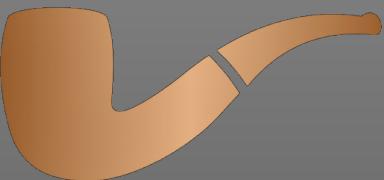
Twitter: @dwmetz

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

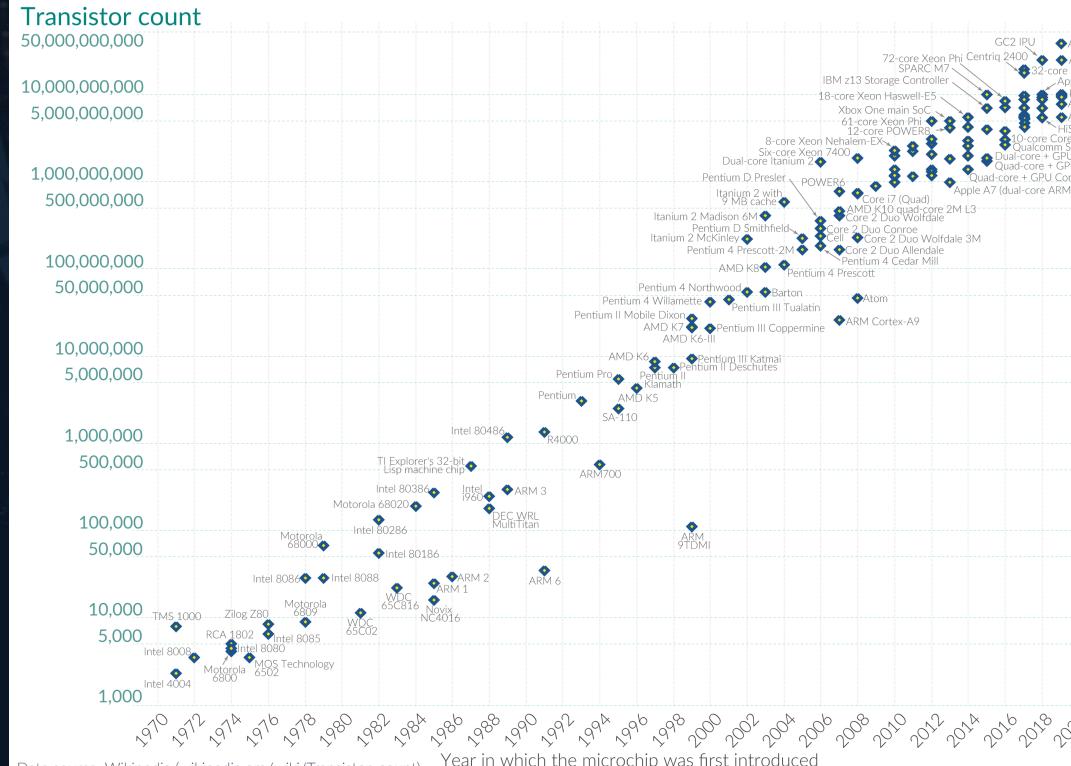


# MAGNITUDES OF DATA

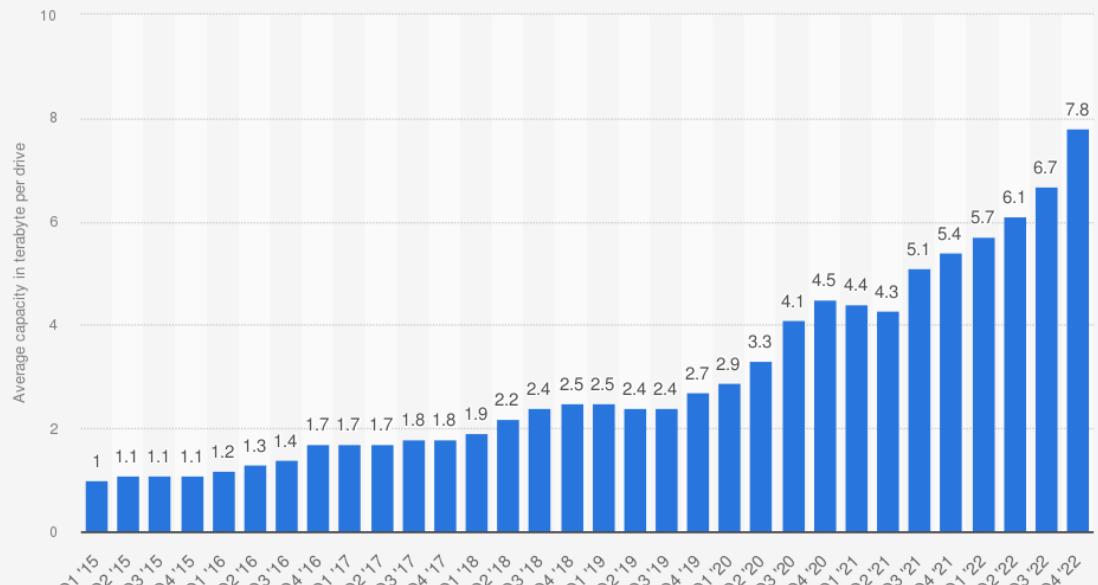
**Moore's Law:** The number of transistors on microchips doubles every two years

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.

Our World  
in Data



**Seagate's average capacity of hard disk drives (HDDs) worldwide from FY2015 to FY2022, by quarter (in terabyte per drive)**



Source  
Seagate  
© Statista 2022

Additional Information:  
Worldwide; Seagate; 2015 to 2022

Sources:

[https://en.wikipedia.org/wiki/Moore%27s\\_law#/](https://en.wikipedia.org/wiki/Moore%27s_law#/)  
<https://www.statista.com/statistics/795748/worldwide-seagate-average-hard-disk-drive-capacity/>



# What If I told You

Less than 5% of the data is critical to 99% of the investigation?





# triage noun

tri·age (*trē-'äzh* *'trē-äzh*)

- 1 **a** : the sorting of and allocation of treatment to patients and especially battle and disaster victims according to a system of priorities designed to maximize the number of survivors
- b** : the sorting of patients (as in an emergency room) according to the urgency of their need for care
- 2 : the assigning of priority order to projects on the basis of where funds and other resources can be best used, are most needed, or are most likely to achieve success

## triage transitive verb



# CyberPipe



An easy-to-use PowerShell script to collect memory and disk forensics for DFIR investigations.

Supports Windows: X64, x86, ARM

## Functions:

- Capture a memory image with DumpIt for Windows,
- Capture a triage image with KAPE,
- Check for encrypted disks,
- Recover the active BitLocker Recovery key,
- Save all artifacts, output, and audit logs to USB or source network drive.

```
.',;::cccccc:..          ....'....'.
.;ccclllloooddxo.      .';clooddooolcc:;:;.
.:ccclllloooddxo.      .,coxxxxndl:'..
'ccccclllloooddd'      .,'lxkxxxo:'.
'ccccclllloooddd'      .,:lxOkl;,oxo,.
':ccccclllloooddo.    .,dk0000kkd;'.
.:ccccclllloooddo.    .,;lk00000kkkd;
.;cccccllllooodddc:coxkkkk00000x:.
'cccccllllooooodddxxxxxkkkk0000x:.
,cccllllooooodddxxxxxkkkxlc,.
':llllooooodddxxxxxoc:.
.'';:cloodddolc:..
```

CyberPipe IR Collection Script  
<https://github.com/dwmetz/CyberPipe>  
@dwmetz | bakerstreetforensics.com

```
Collections directory exists.
Host directory created.
Determining OS build info...
Preparing _cape.cli...
Note: DumpIt & KAPE triage collection processes will launch in separate windows.
Triage aquisition will initiate after memory collection completes.
Checking for BitLocker Key...
Bitlocker key recovered.
** Collection Completed in 3 minutes and 7 seconds.**
```



# CyberPipe

## v4.0 Features: “One Script to Rule them All”

- Admin permissions check before execution.
- Memory acquisition will use Magnet Dumpli for Windows (previously used Magnet RAM Capture).
- Support for x64, ARM64 and x86 architectures.
- Both memory acquisition and triage collection now facilitated via KAPE batch mode with \_cape.cli dynamically built during execution.
- Capture directories now named to \$hostname-\$timestamp to support multiple collections from the same asset without overwriting.
- Alert if Bitlocker key not detected. Both display and (empty) text file updated if encryption key not detected.
- If key is detected it is written to the output file.
- More efficient use of variables for output files rather than relying on renaming functions during operations.
- Now just one script for Network or USB usage. Uncomment the “Network Collection” section for network use.
- Stopwatch function will calculate the total runtime of the collection.
- ASCII art “Ceci n'est pas une pipe.”

```
:111oooooodddxxxxoc;.
';::clooddddolc:...
.....  

"Write-Host -Fore Cyan "
Write-Host -Fore Gray "
Write-Host -Fore Gray "
Write-Host ""
Write-Host ""
$stopwatch = [System.Diagnostics.Stopwatch]::StartNew()
## Network Collection - uncomment the section below for Network use
<#
Write-Host -Fore Gray "Mapping network drive..."
$Networkpath = "X:\  

If (Test-Path -Path $Networkpath) {
    Write-Host -Fore Gray "Drive Exists already."
}
Else {
    # map network drive
    (New-Object -ComObject WScript.Network).MapNetworkDrive("X:","\\Server\Triage")
    # check mapping again
    If (Test-Path -Path $Networkpath) {
        Write-Host -Fore Gray "Drive has been mapped."
    }
    Else {
        Write-Host -Fore Red "Error mapping drive."
    }
}
Set-Location X:  

#>
## Below is for USB and Network:
$tstamp = (Get-Date -Format "yyyyMMddHHmm")
$collection = $env:COMPUTERNAME+$tstamp
$wd = Get-Location
If (Test-Path -Path Collections) {
    Write-Host -Fore Gray "Collections directory exists."
}
Else {  

    CyberPipe IR Collection Script"
https://github.com/dwmetz/CyberPipe
@dwmetz | bakerstreetforensics.com"
```



- Magnet DumpIt for Windows
- Encrypted Disk Detector (EDD)

# MAGNET FREE TOOLS

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

**MAGNET FORENSICS**

HOME KNOWLEDGE BASE TECH SUPPORT ARTIFACT EXCHANGE More ▾

## 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





# 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 application window. It has two main sections: 'Targets' on the left and 'Modules' on the right, both with tables for configuration. At the bottom, there is a 'Current command line' section with a command entered:

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

Below the command line are buttons for 'Copy command', 'Sync with Github', and 'Execute!'. On the far left edge of the slide, there is vertical text that reads 'SEEK JUSTICE. PROTECT THE INNOCENT.'



# TOOLS IN THE /bin - BYOE

The screenshot shows a file explorer window titled "KAPE > Modules > bin". The search bar contains "Search bin". The table lists the following files:

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
LEC.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

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
Dumpli_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



# CyberPipe Operations

## 1. Script launch

```
72.50% Files remaining to be copied: 369 (Copied: 794 Deferred queue count: 198 Deduced count: 45 Skipped count: 0 Errors: 0)
Deferring C:\Windows\System32\config\SECURITY.LOG1 due to IOException...
Deferring C:\Windows\System32\config\SECURITY.LOG2 due to IOException...
Deferring C:\Windows\System32\config\SOFTWARE.LOG1 due to IOException...
Deferring C:\Windows\System32\config\SOFTWARE.LOG2 due to IOException...
Deferring C:\Windows\System32\config\SYSTEM.LOG1 due to IOException...
Deferring C:\Windows\System32\config\SYSTEM.LOG2 due to IOException...
Deferring C:\Windows\System32\config\SAM due to IOException...
Deferring C:\Windows\System32\config\SECURITY due to IOException...
Deferring C:\Windows\System32\config\SOFTWARE due to IOException...
Deferring C:\Windows\System32\config\SYSTEM due to IOException...
Deferring C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT due to IOException...
Deferring C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG1 due to IOException...
Deferring C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT.LOG2 due to IOException...
Deferring C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT due to IOException...
Deferring C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG1 due to IOException...
Deferring C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT.LOG2 due to IOException...
Deferring C:\Users\jmoriarty\NTUSER.DAT due to IOException...
Deferring C:\Users\jmoriarty\ntuser.dat.LOG1 due to IOException...
Deferring C:\Users\jmoriarty\ntuser.dat.LOG2 due to IOException...
Deferring C:\Windows\System32\config\DEFAULT due to IOException...
Deferring C:\Windows\System32\config\DEFAULT.LOG1 due to IOException...
Deferring C:\Windows\System32\config\DEFAULT.LOG2 due to IOException...
Deferring C:\Users\jmoriarty\AppData\Local\Microsoft\Windows\UsrClass.dat due to IOException...
Deferring C:\Users\jmoriarty\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 due to IOException...
Deferring C:\Users\jmoriarty\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 due to IOException...
Deferring C:\Windows\System32\Tasks\{Microsoft\Windows\GroupPolicy\{A7719E0F-10DB-4640-AD8C-490CC6AD5202} due to UnauthorizedAccessException...
Deferring C:\Windows\System32\Tasks\{Microsoft\Windows\GroupPolicy\{A7719E0F-10DB-4640-AD8C-490CC6AD5202} due to UnauthorizedAccessException...
```

### 3. (2<sup>nd</sup> new window) Triage Collection

```
C:\Users\jmoriarty\Desktop\KAPE\cape.exe

KAPE version 1.3.0.2, Author: Eric Zimmerman, Contact: https://www.kroll.com/ape (ape@kroll.com)

KAPE directory: C:\Users\jmoriarty\Desktop\KAPE
Command line: --msource C:\ --mdest C:\Users\jmoriarty\Desktop\Collections\MORIARTY_202303141230 --module DumpIt_Memory,MagnetForensics_EDD --ul

System info: Machine name: MORIARTY, 64-bit: True, User: jmoriarty OS: Windows10 (10.0.22621)

Using Module operations
Module DumpIt_Memory: Found 1 processor
    Found processor Executable: DumpIt.exe, Cmd line: /O %destinationDirectory%\memdump.dmp /Q, Export: dmp, Append: False!
Module MagnetForensics_EDD: Found 1 processor
    Found processor Executable: EDD\EDDv310.exe, Cmd line: /batch >> %destinationDirectory%, Export: txt, Append: False!
Discovered 2 processors to run
Executing modules with file masks...
Executing remaining modules...
Running DumpIt.exe: /O C:\Users\jmoriarty\Desktop\Collections\MORIARTY_202303141230\Memory\memdump.dmp /Q
```

## 2. (new window) Memory Collection

#### 4. Clean-up and Complete



# CyberPipe Demo



SEEK JUSTICE. PROTECT THE INNOCENT.

[magnetforensics.com](http://magnetforensics.com)



# CyberPipe Output

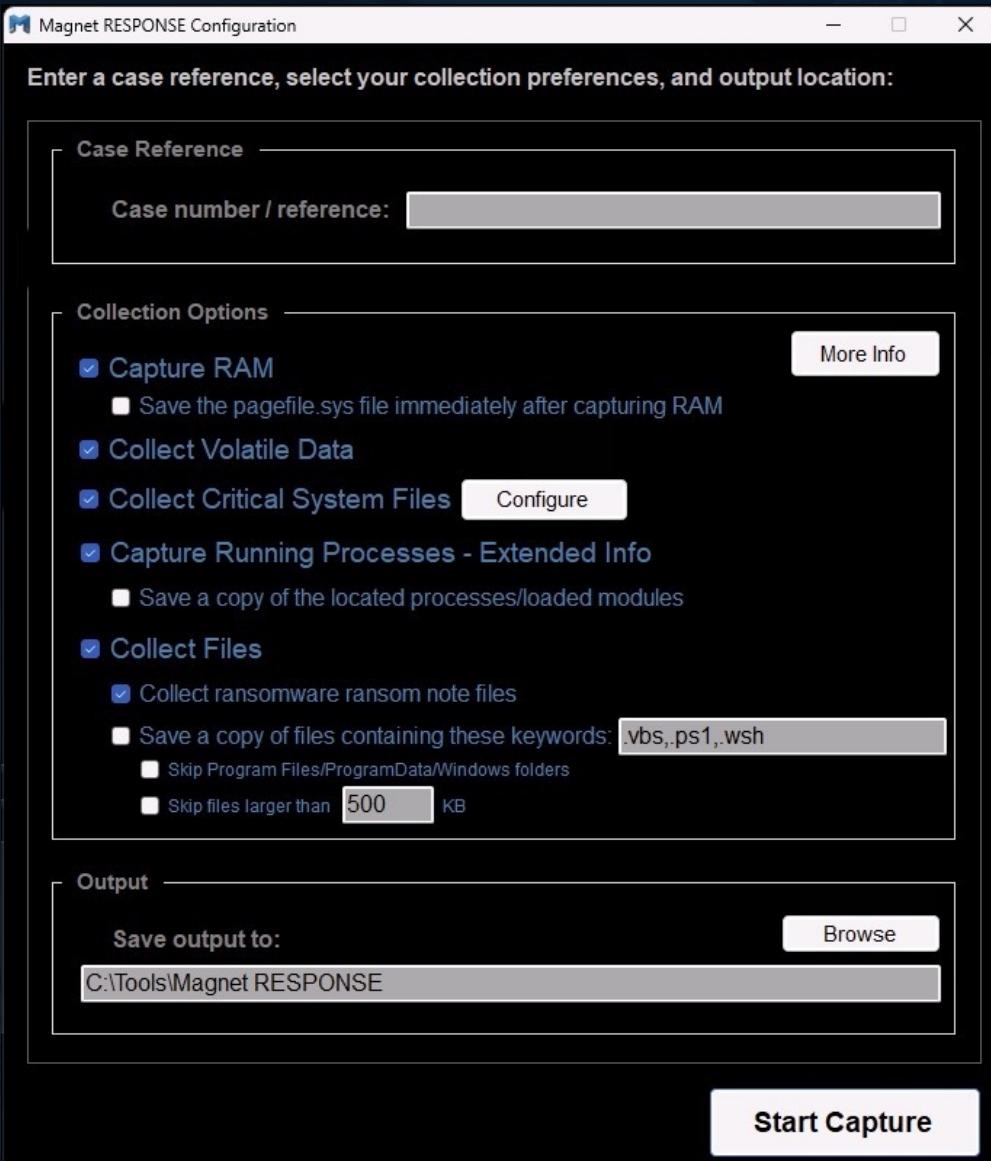
SEEK JUSTICE. PROTECT THE INNOCENT.

Name	Date modified	Type	Size
LiveResponse	3/14/2023 12:34 PM	File folder	
Memory	3/14/2023 12:34 PM	File folder	
2023-03-14T16_30_46_0089119_ConsoleL...	3/14/2023 12:32 PM	Text Document	2 KB
2023-03-14T16_32_09_1009544_ConsoleL...	3/14/2023 12:34 PM	Text Document	110 KB
2023-03-14T163209_MORIARTY.vhdx	3/14/2023 12:34 PM	Hard Disk Image F...	3,051,520 KB
collection-complete.txt	3/14/2023 12:34 PM	Text Document	1 KB

Name	Date modified	Type	Size
EDD.txt	3/14/2023 12:32 PM	Text Document	2 KB
MORIARTY_202303141230-key.txt	3/14/2023 12:34 PM	Text Document	1 KB
Collections > MORIARTY_202303141230 > Memory			
Name	Date modified	Type	Size
MORIARTY_202303141230.dmp	3/14/2023 12:32 PM	DMP File	16,382,988 ...
MORIARTY-profile.txt	3/14/2023 12:30 PM	Text Document	1 KB



# Magnet RESPONSE



Magnet RESPONSE lets investigators and non-technical users easily collect and preserve critical data relevant to incident response investigations from local endpoints.

Magnet RESPONSE is a free and easy-to-use solution to quickly collect and preserve data from local endpoints before it is potentially modified or lost. A pre-set collection profile lets you target a comprehensive set of files and data relevant to incident response investigations, including RAM.

Minimal to no training is required—it's as simple as running it on the endpoint, configuring the collection and clicking “start capture.” This makes Magnet RESPONSE useful in situations where non-technical users may need to collect and preserve data on behalf of law enforcement investigators as part of a cyber incident investigation.

<https://www.magnetforensics.com/resources/magnet-response/>

magnetforensics.com



# Magnet RESPONSE

## Key Benefits & Features:

- Easy-To-Use: A guided two-step process and progress bar is straightforward for even non-technical users to use
- Fast & Comprehensive: Collect and preserve data starting with the most volatile using the built-in Comae RAM capture (MAGNET DumplIt) functionality, and volatile data and files commonly associated to cybercrime, such as Windows Event Logs, Registry Hives, Jumplist files, and many other log files in minutes – no need for multiple tools to get the IR data you need
- Portable: It is comprised of a single executable file (less than 1MB), is easily downloaded, and can be stored and run from a USB key
- Collect by Keyword & Skip Large Files: configure free-form collections using your own set of keywords (or the defaults provided), with the option to limit the size of files collected to maintain speed
- Consolidated Output: Output is consolidated and saved as a .zip file for easy delivery or processing and analysis in Magnet AXIOM & Magnet AXIOM Cyber
- Data Integrity: An embedded hash value is provided to verify the integrity of the data



# Magnet RESPONSE

## Auto-collect Options

These options can be useful if you are providing the tool to a non-technical operator to simply capture the data and bring it back to you for processing/analysis.

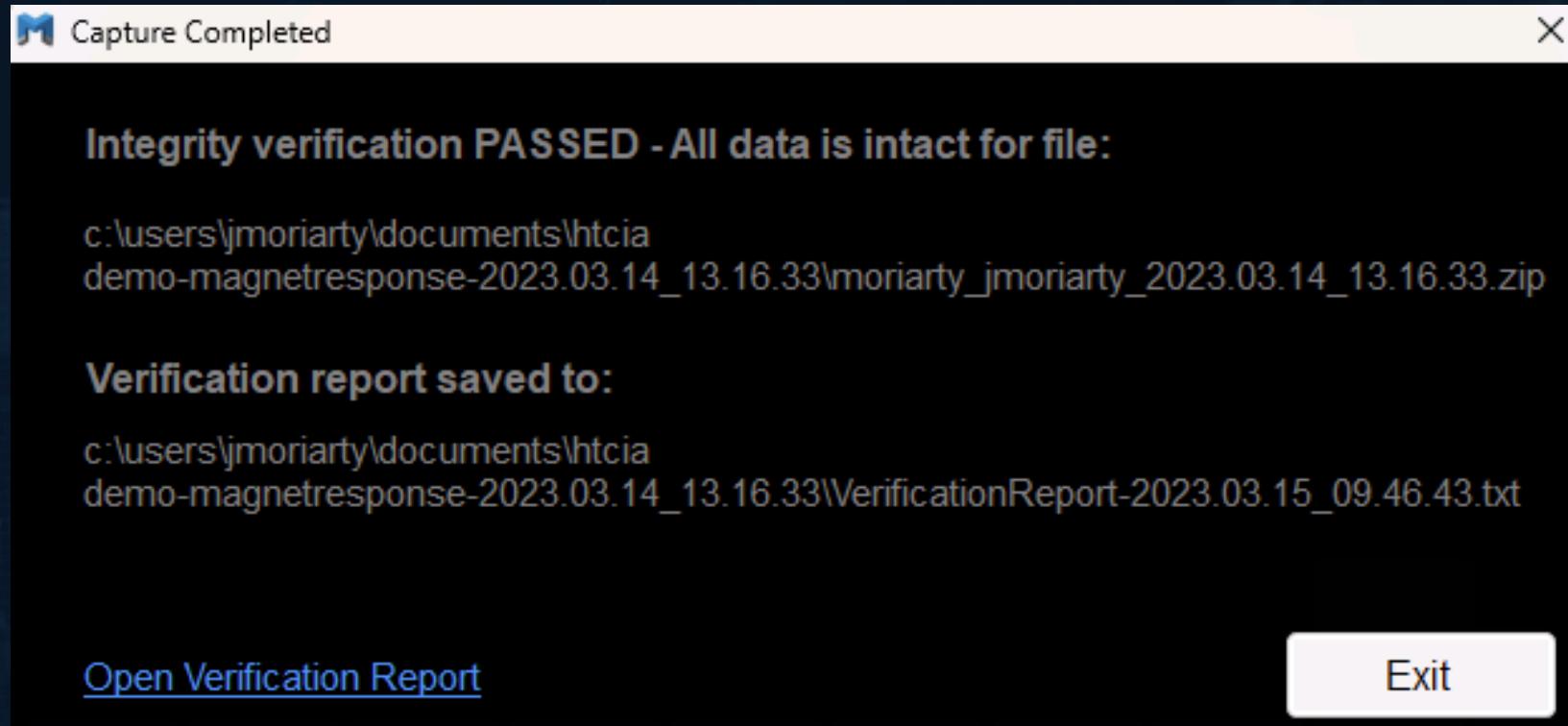
- Option 1 - Capture Everything Rename the executable to have the text "AutoCapture" (no quotes) anywhere in the filename. All options will be enabled, and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs from.
- Option 2 - Minimal Capture Rename the executable to have the text "AutoCaptureMinimal" (no quotes) anywhere in the filename. Only the "Volatile Data" and "Critical System Files" options will be enabled (no extended info saved for running processes), and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs from.



# Magnet RESPONSE

## Verifying a Capture Package

To verify the ZIP, simply drag and drop it on to the RESPONSE executable. RESPONSE will launch as normal and go directly into a verification process, providing a message at the end indicating if the verification was successful. A text file containing details of the verification is saved to the same folder.





# Magnet RESPONSE Demo



SEEK JUSTICE. PROTECT THE INNOCENT.

[magnetforensics.com](http://magnetforensics.com)



# Magnet RESPONSE Output

The screenshot displays two windows from the Magnet Forensics application. The top window shows the contents of a folder named 'HTCIA Demo-MagnetRESPONSE-2023.03.14\_13.16.33'. It contains two files: 'MORIARTY\_jmoriarty\_2023.03.14\_13.16.33...' (a ZIP File, 909,893 KB) and 'RAMDump-MORIARTY-20230314-131633...' (a DMP File, 16,382,988 bytes). The bottom window shows the contents of a folder named 'extracted' within the same directory. It contains four sub-folders: 'Logs', 'Processes', 'Saved\_Files', and 'Volatile\_Data', all created on 3/14/2023 at 1:37 PM.

Name	Date modified	Type
MORIARTY_jmoriarty_2023.03.14_13.16.33...	3/14/2023 1:21 PM	ZIP File
RAMDump-MORIARTY-20230314-131633...	3/14/2023 1:17 PM	DMP File

Name	Date modified	Type
Logs	3/14/2023 1:37 PM	File folder
Processes	3/14/2023 1:37 PM	File folder
Saved_Files	3/14/2023 1:37 PM	File folder
Volatile_Data	3/14/2023 1:37 PM	File folder



# Magnet RESPONSE Output

HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 > extracted > Saved_Files >				
Name	Date modified	HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 > extracted > Volatile_Data		
		Name	Date modified	Type
Amcache	3/14/2023 1:37 PM	Firewall_Info.txt	3/14/2023 1:19 PM	Text Document
Browser_History	3/14/2023 1:37 PM	IP_Info.txt	3/14/2023 1:19 PM	Text Document
Jumplists-AutomaticDestinations	3/14/2023 1:37 PM	Logged_On_Users.txt	3/14/2023 1:19 PM	Text Document
Jumplists-CustomDestinations	3/14/2023 1:37 PM	Network_Connections.txt	3/14/2023 1:17 PM	Text Document
MFT	3/14/2023 1:37 PM	Scheduled_Tasks.txt	3/14/2023 1:19 PM	Text Document
NTUSER.DAT	3/14/2023 1:37 PM	User_Accounts.txt	3/14/2023 1:19 PM	Text Document
PowerShell_History	3/14/2023 1:37 PM	Wifi_Info.txt	3/14/2023 1:19 PM	Text Document
Prefetch_Files	3/14/2023 1:37 PM	Windows_Services.txt	3/14/2023 1:19 PM	Text Document
Recent_Files	3/14/2023 1:37 PM	Windows_Version.txt	3/14/2023 1:19 PM	Text Document
Recycle_Bin	3/14/2023 1:37 PM			
Registry_Hives	3/14/2023 1:37 PM			
Scheduled_Tasks	3/14/2023 1:37 PM			
SRIIM	3/14/2023 1:37 PM			



# 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.



# EVIDENCE PROCESSING TIPS



SEEK JUSTICE. PROTECT THE INNOCENT.





# MEMORY PROCESSING

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet AXIOM Process 5.2.0.25407

File Tools Help

**EVIDENCE SOURCES**

**WINDOWS SELECT EVIDENCE SOURCE**

DRIVE IMAGE FILES & FOLDERS VOLUME SHADOW COPY MEMORY

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

The screenshot illustrates a digital forensic workflow for memory processing:

- PowerShell Window:** Shows the command `gc .\DMETZ-W10_build.txt` being run to read build information from a text file.
- Magnet AXIOM Process Window:** The "EVIDENCE SOURCES" tab is selected. It displays "CASE DETAILS" and "PROCESSING DETAILS" sections. Under "PROCESSING DETAILS", options like "Search archives and mobile backups" and "Add keywords to search" are listed. The "ARTIFACT DETAILS" section shows 0 artifacts found.
- Select Profile Window:** The "SELECT PROFILE" window is open, prompting the user to provide the correct image profile based on the operating system build number. It offers two options:
  - I want AXIOM Process to provide a list of recommended image profiles.
  - I want to select the image profile myself.A note explains that AXIOM Process can provide a list of recommended memory image profiles, which may take a while. It also notes that Volatility reports the KDBG address as "KdCopyDataBlock (V)" on Windows 8+ and "Offset (V)" on earlier versions.
- Notepad++ Window:** A file named `\synology\Collections\MORIARTY\MORIARTY.txt` is open, showing the build information: Major 10, Minor 0, Build 19043, Revision 0.
- File Explorer Window:** The "MORIARTY" folder is selected, showing its contents. The folder structure includes subfolders like Books, Desktop, GoodNotes, Locker, Pictures, Tools, VSCode, and files like transfer-complete.txt, 2021-07-15T204305\_ConsoleLog.txt, 2021-07-15T204305\_MORIARTY.zip, MORIARTY.txt, MORIARTY.7z, 2021-07-15T204305\_MORIARTY, and memdump.raw.



# MEMORY ARTIFACTS FROM VOLATILITY

SEEK JUSTICE. PROTECT THE INNOCENT.

**MATCHING RESULTS (56 of 56)**

**Column view**

	Prot...	Local IP Ad...	Remote IP...	State	Proc...	Owner	Created Date/T...	Artifact type
<b>MEDIA</b>	<b>1,908</b>							
<b>DOCUMENTS</b>	<b>4</b>							
<b>PEER TO PEER</b>	<b>2</b>							
<b>OPERATING SYSTEM</b>	<b>1,559</b>							
<b>MEMORY</b>	<b>118,719</b>							
API Hooks (apihooks)	27,685							
Dynamically Loaded Libraries (dlllist)	9,447							
Files (filescan)	10,578							
Hidden/Residual Modules (modscan)	218							
Hidden/Terminated Processes (psscan)	95							
Image Info (imageinfo)	1							
LDR Modules (ldrmodules)	9,941							
Loaded Kernel Modules (modules)	214							
Malware Finder (malfind)	22							
Network Info (netscan)	56							
Open Handles (handles)	57,996							
Process Security Identifiers (getsids)	2,284							
Processes (pslist)	181							
Timeline (timeliner)	1							
<b>LOCATION &amp; TRAVEL</b>	<b>1</b>							
<b>CUSTOM</b>	<b>47</b>							





# VMDK IMAGE PROCESSING

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet AXIOM Process 5.9.0.30292

File Tools Help

EVIDENCE SOURCES

SELECT EVIDENCE SOURCE

DRIVE IMAGE FILES & FOLDERS VOLUME SHADOW COPY MEMORY

Select the image

This PC > This PC > T5-X (D:) > Collections > DMETZ-W10

Name	Date modified	Type	Size
Decrypt	2/15/2022 8:27 AM	File folder	
2022-02-15T132640_DMETZ-W10.vhdx	2/15/2022 8:28 AM	Hard Disk Image File	4,329,472 K
DMETZ-W10_20220215_082500.raw	2/15/2022 8:26 AM	RAW File	18,341,888 K

File name: 2022-02-15T132640\_DMETZ-W10.vhdx

All Supported Images (\*.E01, ...)

Open Cancel

BACK NEXT

The screenshot shows the Magnet AXIOM Process software interface. On the left, there's a sidebar with sections for Case Details, Evidence Sources (selected), Processing Details, Artifact Details (0), and Analyze Evidence. The main area is titled 'EVIDENCE SOURCES' and 'SELECT EVIDENCE SOURCE'. It features five icons: DRIVE, IMAGE (which is selected), FILES & FOLDERS, VOLUME SHADOW COPY, and MEMORY. A modal window titled 'Select the image' is open, showing a file browser view of 'This PC > This PC > T5-X (D:) > Collections > DMETZ-W10'. It lists three items: 'Decrypt' (a folder), '2022-02-15T132640\_DMETZ-W10.vhdx' (a VHDX image file), and 'DMETZ-W10\_20220215\_082500.raw' (a RAW file). The '2022-02-15T132640\_DMETZ-W10.vhdx' file is highlighted. At the bottom of the modal are 'File name:' dropdown, 'All Supported Images (\*.E01, ...)' dropdown, 'Open' button, and 'Cancel' button. At the very bottom of the main window are 'BACK' and 'NEXT' buttons.

Computer > Windows > Load Evidence > IMAGE

magnetforensics.com



# ARTIFACTS FROM TRIAGE IMAGE (VMDK)

Magnet AXIOM Examine v5.2.0.25407 - HTCIA\_CSIRT-Collect

File Tools Process Help



## 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.v...

VIEW EVIDENCE FOR THIS SOURCE ONLY

Evidence number 2021-07-15T204305\_MORIARTY.vhdx

Description

Location 2021-07-15T204305\_MORIARTY.vhdx

Platform Computer

Magnet AXIOM Examine v5.2.0.25407 - HTCIA\_CSIRT-Collect

File Tools Process Help

### FILTERS

Keyword lists Skin tone



Artifacts

### MATCHING RESULTS

306,038

### REFINED RESULTS

292

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

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

## 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 &



# 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={...}})	b' \$LogicalDisk += @(\$_   Select @{n="Name";e={...}})	PowerShell H
1801	@{n="Volume Label";e={\$_.VolumeName}},`	b' @{n="Volume Label";e={\$_.VolumeName}},`	PowerShell H
1802	@{n="Size (Gb)";e={"(0:N2)" -f (\$_.Size/1GB))}},`	b' @{n="Size (Gb)";e={"(0:N2)" -f (\$_.Size/1GB))}},`	PowerShell H
1803	@{n="Used (Gb)";e={"(0:N2)" -f (\$_.Size/1GB)) - ...}}	b' @{n="Used (Gb)";e={"(0:N2)" -f (\$_.Size/1GB)) - ...}}	PowerShell H
1804	@{n="Free (Gb)";e={"(0:N2)" -f (\$_.FreeSpace/1G...)}}	b' @{n="Free (Gb)";e={"(0:N2)" -f (\$_.FreeSpace/1G...)}}	PowerShell H
1805	@{n="Free (%)" ;e=(if(\$_.Size) {"(0:N2)" -f (\$_.Free...})}}	b' @{n="Free (%)" ;e=(if(\$_.Size) {"(0:N2)" -f (\$_.Free...}))}	PowerShell H
1806	}	b' )'	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			

**1**

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

**DETAILS**

Order 1

Command List (UTF8) python --version

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

Artifact type PowerShell History

Item ID 586032

**EVIDENCE INFORMATION**

Source 2022-02-15T132640\_DMETZ-W10.vhd

- 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.vhd

TAGS, COMMENTS & PROFILES

Time zone UTC+0:00



# 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)**

	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-E881-4B31-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-B824}
	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-E881-4B31-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-98F/}
	2006	2/14/2022 8:49:31 PM	14	A rule has been deleted in the Windows Firewall exc...	{FC8AEA85-1A02-459A-98F/}
	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 0-1879813800-110756685-8232 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

**EVIDENCE (69,398)**

Entr...	Application Name
28271	SMB
71080	SMB
80279	teams.exe
73746	
37402	
73739	teams.exe
60863	SMB
61649	
73557	
55880	SMB
73550	teams.exe
37535	SMB
62551	
55904	SMB
61640	teams.exe
56705	
62543	teams.exe
56695	teams.exe
81459	
87369	
87388	powerpnt.exe
55927	SMB
51669	
70966	onedrive.exe
51666	teams.exe

**MEMORY** 1

MAGNET FORENSICS EXPLORE P

INDUSTRY NEWS OCTOBER 5, 2022

**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.

1/14/2022 6: Bytes Sent 9413  
 \device\harddiskvolume3\users\dmetz\appdata\loc... 1/20/2022 7:  
 \device\harddiskvolume3\users\dmetz\appdata\loc... 1/14/2022 6:  
 2/8/2022 7:3  
 2/14/2022 8:  
 \device\harddiskvolume3\program files\microsoft of... 2/14/2022 8:  
 System\SMB 1/14/2022 1:  
 1/13/2022 8:  
 \device\harddiskvolume3\program files\microsoft o... 1/28/2022 2:  
 \device\harddiskvolume3\users\dmetz\appdata\loc... 1/13/2022 8:

Bytes Received 103982  
 Artifact type **SRUM Network Usage**  
 Item ID 758619

**EVIDENCE INFORMATION**

Source 2022-02-15T132640\_DMETZ-W10.vhdx - Partition 1 (Microsoft NTFS, 11.85 GB)  
 KAPE (2022-02-15T13:26:40) C:\Windows\System32\SRU\SRUDB.dat  
 Recovery method Parsing

Time zone UTC+0:00



# 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

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**

Operating System	746,938
Web Related	54,323
Refined Results	7,887
Media	3,339
Custom	2,082
Application Usage	375
Cloud Services	10

### 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

The screenshot displays four windows of the Magnet AXIOM Process software:

- EVIDENCE SOURCES:** Shows icons for COMPUTER, MOBILE, CLOUD, VEHICLE, and REMOTE COMPUTER.
- EVIDENCE SOURCES ADDED TO CASE:** A grid of evidence items.
- EVIDENCE SOURCES:** A configuration window for a remote computer named MORIARTY, with fields for IP address (moriarty), User name (dwmetz), and Password (\*\*\*\*\*). A "DEPLOY AGENT" button is present.
- EVIDENCE SOURCES:** A window titled "SELECT ITEMS TO DOWNLOAD" for the remote computer MORIARTY. It shows the computer is connected and downloading file system structure and metadata. It includes sections for "REVIEW AND SELECT THE DATA FROM THE TARGET COMPUTER" (with options for TARGETED LOCATIONS, FILES AND DRIVES, and MEMORY) and "ITEMS TO DOWNLOAD".





# RESOURCES

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

Magnet DumpIt for Windows: <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>

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

Magnet RESPONSE:

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

Blog: <https://bakerstreetforensics.com>



# THANK YOU



<https://github.com/dwmetz>



<https://bakerstreetforensics.com>



doug.metz@magnetforensics.com



<https://www.linkedin.com/in/dwmetz/>



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



@dwmetz

