



MAGNET
FORENSICS®

TECHNO SECURITY 2022

Free Tools for DFIR Triage Collections

Doug Metz, Professional Services Consultant
Magnet Forensics



Doug Metz

Professional Services Consultant with Magnet Forensics.

Over a decade of experience in Incident Response and Forensics in corporate environments.

Most recently served as Global Incident Response Manager for a Fortune 200, managing a globally dispersed team of analysts and the 24x7 Security Operations Center.

Blog: BakerStreetForensics.com, focused on DFIR tips and tricks, PowerShell, and Windows Subsystem for Linux (WSL).



@dwmetz

BAKER STREET FORENSICS

D . F . I . R .

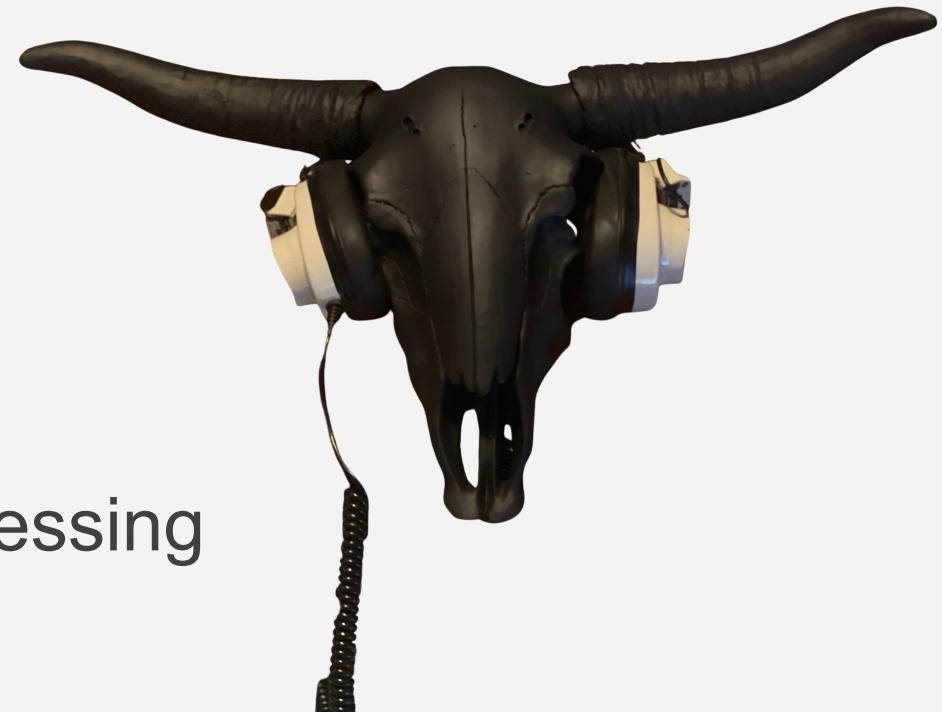
WHERE IRREGULARS ARE PART OF
THE GAME



magnetforensics.com

Agenda

- 5 Elements of the collection kit
- CSIRT-Collect Use Cases
- MRC, EDD & KAPE
- Hardware Choices
- Script Output
- Tips for Effective Evidence Processing





5 Collection Kit Elements

- POWERSHELL (CSIRT script)
- MAGNET RAM CAPTURE
- ENCRYPTED DISK DETECTOR (EDD)
- KAPE
- HIGH SPEED USB DEVICE

CSIRT-Collect PowerShell

CSIRT-Collect is a PowerShell script for Incident Response investigations that captures RAM and disk artifacts to a network share.

CSIRT-Collect_USB is a variant of the script intended to be run direct from a USB device.



CSIRT-Collect

RAM (MRC)

Triage (KAPE)

Compression

Network share

-

-



CSIRT-Collect_USB

RAM (MRC)

Triage (KAPE)

[omitted in USB edition]

USB device

Encrypted Disk Detection (EDD)

Bitlocker Key Recovery



Collect from Network Isolated Assets

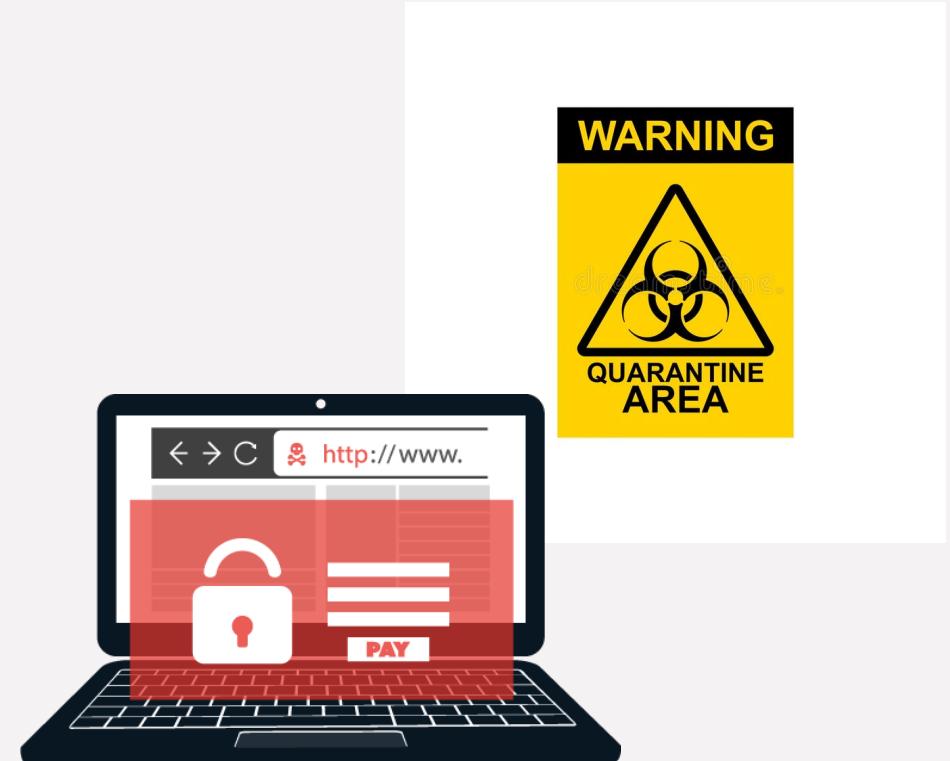
USB Use Cases:

Ransomware response

Airgap; Manufacturing / Medical / ICS

Enterprise resources not available

BOGHOK (Boots on Ground, Hands on Keyboard)





MAGNET Free Tools

MAGNET RAM
CAPTURE

ENCRYPTED DISK
DETECTOR (EDD)



<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

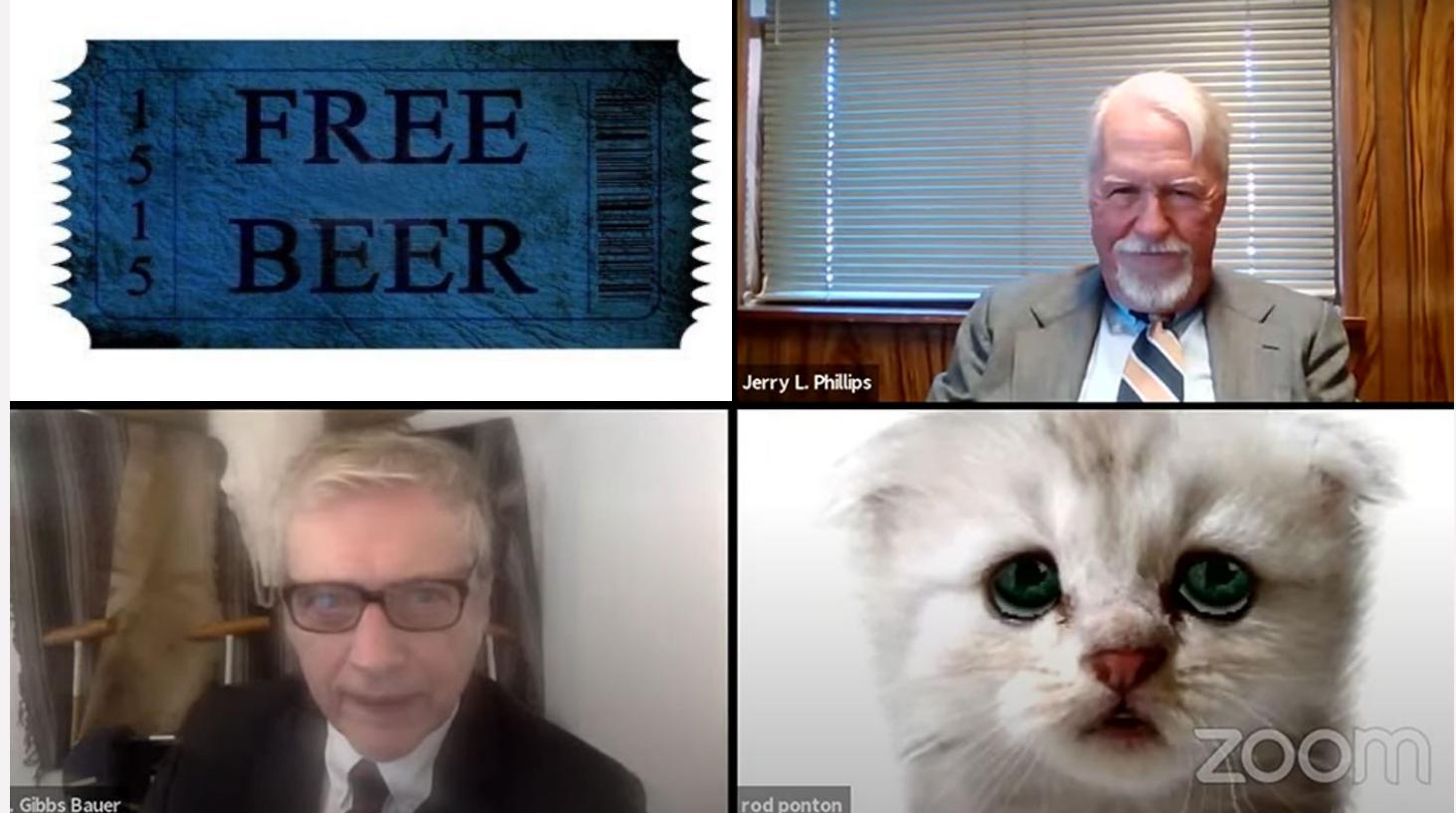
FREE TOOLS

- [Generate wordlists with the AXIOM Wordlist Generator](#)
- [Acquire Memory with MAGNET RAM Capture](#)
- [System requirements: Magnet ACQUIRE](#)
- [Prepare iOS devices for acquisition](#)
- [Magnet ACQUIRE supported Android devices](#)

[View All \(20+\)](#)

Not a Lawyer (or a Cat)

*Free to _ Use?
Modify? Distribute?
Profit?*



Gratis versus Libre - Wikipedia

KAPE licensing

“The solo edition of the Kroll Artifact Parser and Extractor (KAPE) allows the tool to be used at no cost by any local, state or international government agency, and by educational or research organization, or for internal company purposes. An enterprise license is required when KAPE is used on a third-party network and/or as part of a paid engagement.“

More:

<https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape/enterprise-license>





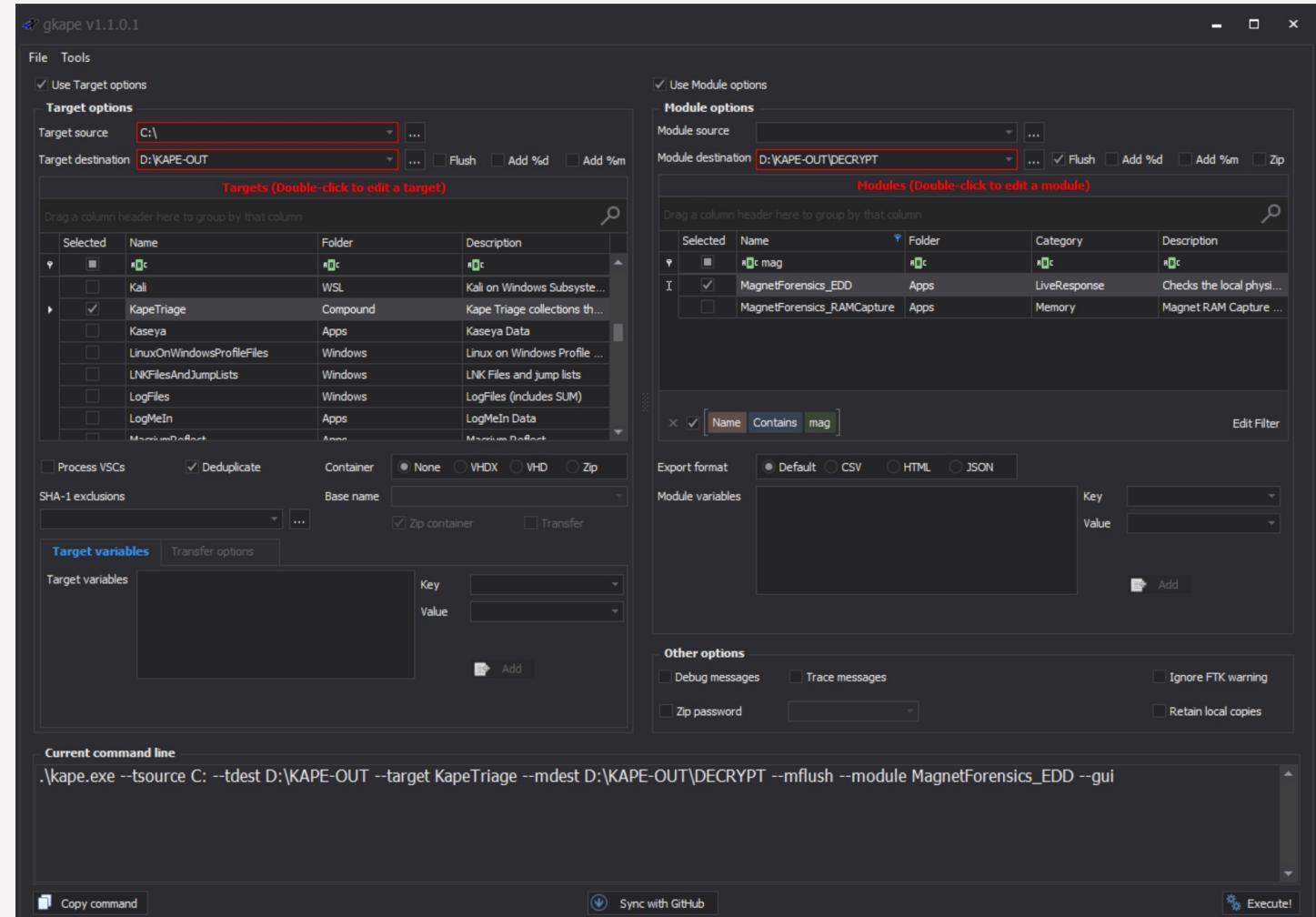
KAPE

GUI and Command Line

KAPE has two primary components, Targets & Modules.

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

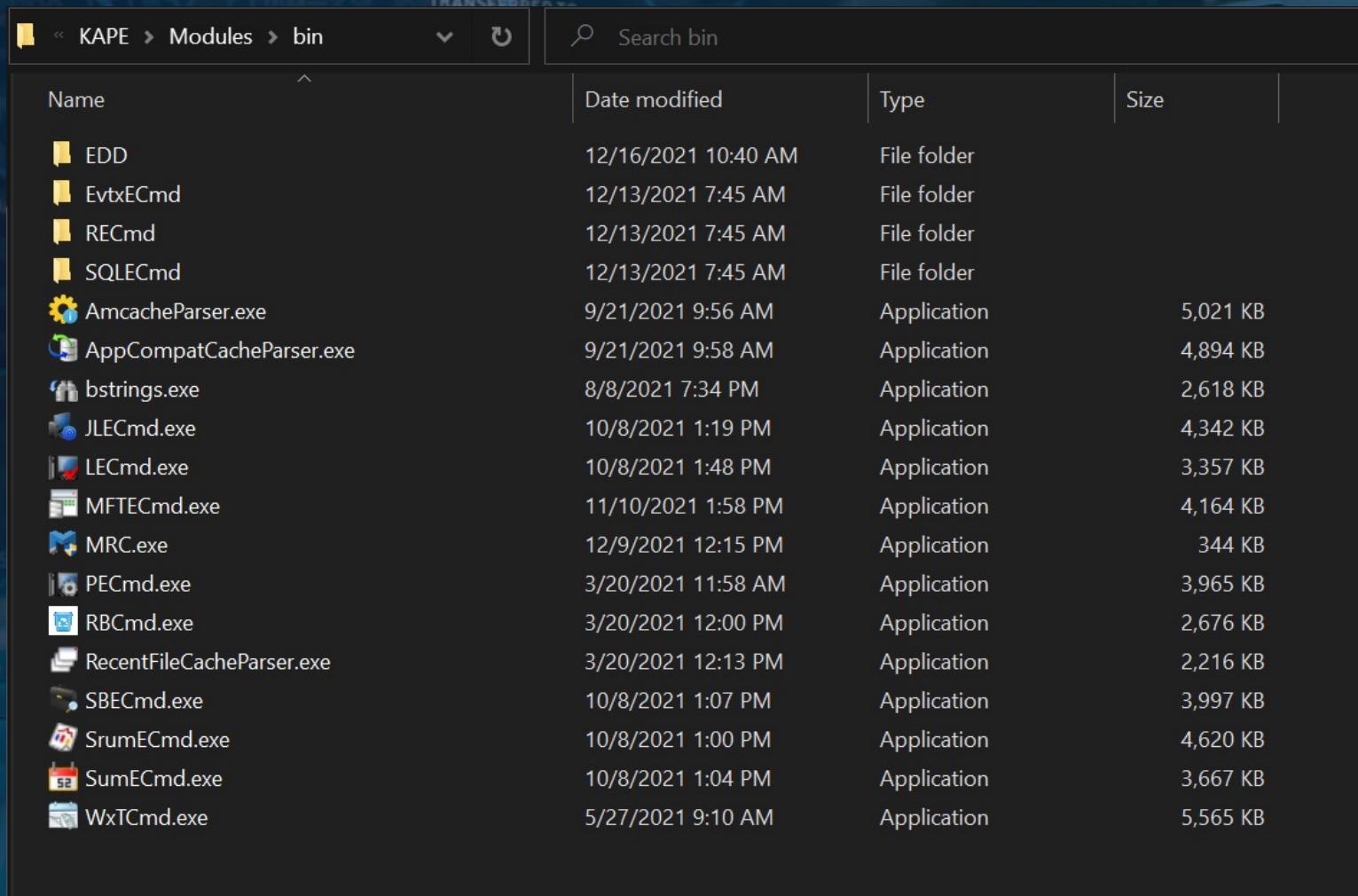
Modules: processing routines that can be run on what is collected (parse, convert to CSV, more) and run executables.



<https://www.sans.org/tools/kape/>



Tools in the /bin - BYOE



The screenshot shows a file explorer window titled "KAPE > Modules > bin". The search bar at the top right contains the text "Search bin". The table below lists the contents of the /bin directory:

Name	Date modified	Type	Size
EDD	12/16/2021 10:40 AM	File folder	
EvtxECmd	12/13/2021 7:45 AM	File folder	
RECcmd	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
LECcmd.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

The screenshot shows a Visual Studio Code interface with a dark theme. On the left is a sidebar with various icons. The main editor window displays a configuration file named `MagnetForensics_EDD.mkape`. The content of the file is as follows:

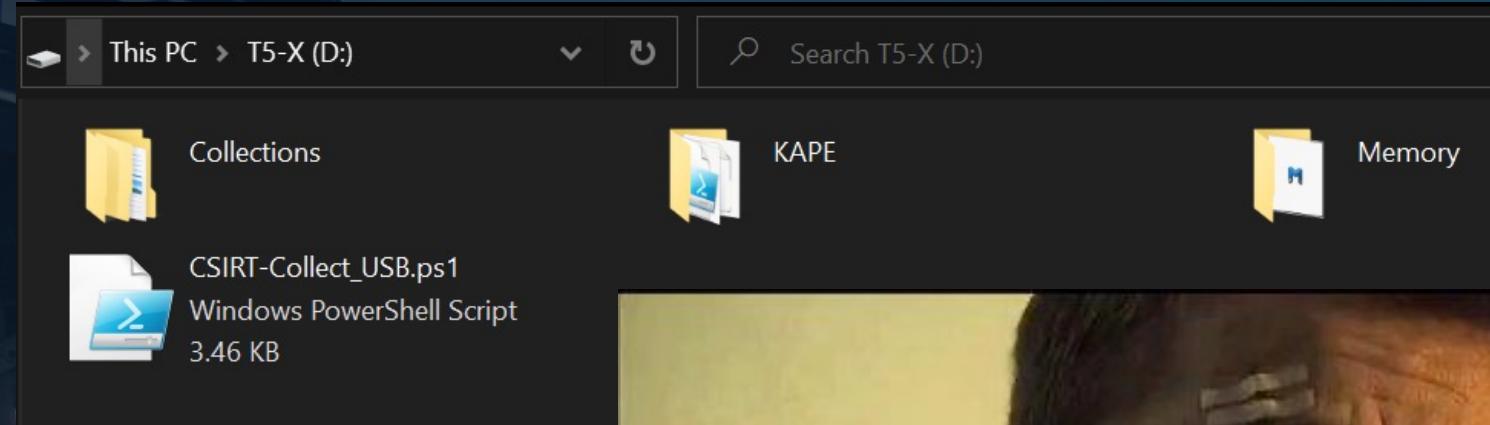
```
D: > KAPE > Modules > Apps > MagnetForensics_EDD.mkape
5  Id: c7212da1-ed41-4560-95f7-1a2d99acc1f8
6  BinaryUrl: http://magnetfiles.com/free_tools/EDD/EDDv300.zip
7  ExportFormat: txt
8  Processors:
9
10 |   Executable: EDD\EDDv302.exe
11 |   CommandLine: /batch >> %destinationDir%
12 |   ExportFormat: txt
13 |   ExportFile: EDD.txt
14
15 # Documentation
16 # https://www.magnetforensics.com/resources/encr
17 # Create a folder "EDD" within the "Modules\bin"
18 # Place "EDDv300.exe", "EDDv300.exe.config" file
19
```

To the right of the editor is a file explorer sidebar titled "KAPE > Modules > Apps". It lists several items, all of which are MKAPE files, indicating they are ready to be used with the KAPE framework. The items listed are:

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
DumpIt_Memory.mkape	12/17/2021 9:41 AM	MKAPE File	1 KB
Everything_ParseEPU.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



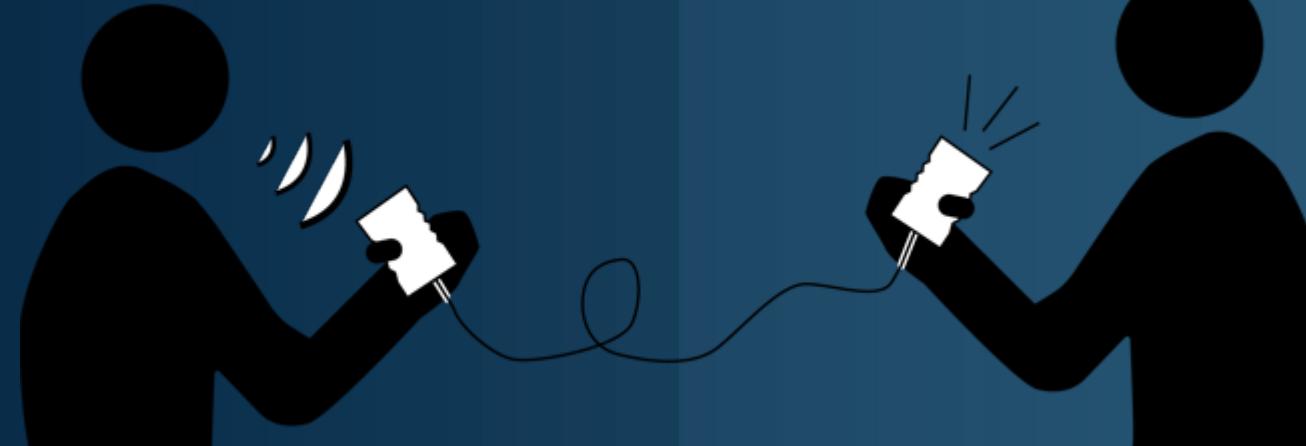
USB Contents





The Handoff

"I need you to do a forensic capture of the RAM and active processes and then proceed with a triage collection of host artifacts. Then check if encrypted disks are present. If so, validate recovery key can be retrieved before powering off. And keep a detailed log of all your actions."



- 1. Plug in USB device
- 2. Open PowerShell as Admin
- 3. Execute CSIRT-Collect_USB.ps1"



Script Walk Through



Memory Collection

Administrator: PowerShell

```
PS D:\> & '.\CSIRT-Collect USB.ps1'

-----  
CSIRT IR Collection Script - USB, v2.2  
https://github.com/dwmetz/CSIRT-Collect  
@dwmetz | bakerstreetforensics.com  
-----  
Directory: D:\Collections  
Mode           LastWriteTime  
----           -----  
d--- 2/11/2022 2:34 PM  
Initiating Magnet Ram Capture.  
Capturing memory...  
This process may take several minutes...
```



magnetforensics.com



Build Info >>> KAPE Triage Execution

```
0.56%: Files remaining to be cop X + ▾ - □ ×  
-----  
Directory: D:\Collections  
  
Mode           LastWriteTime  
----           -----  
d--- 2/11/2022 2:34 PM  
Initiating Magnet Ram Capture.  
Capturing memory...  
This process may take several minutes...  
Determining OS build info...  
Cleaning up memory collection...  
Collecting OS artifacts...  
KAPE version 1.1.0.1 Author: Eric Zimmerman (kape@kroll.com)  
  
KAPE directory: D:\Kape  
Command line: --tsource C: --tdest Collections\DMETZ-W10 --target KapeTriage --vhdx DMETZ-W10 --zv false --module Magnet  
Forensics_EDD --mdest Collections\DMETZ-W10\Decrypt  
  
System info: Machine name: DMETZ-W10, 64-bit: True, User: dmetz OS: Windows10 (10.0.19044)  
  
Using Target operations  
Found 14 targets. Expanding targets to file list...  
Target 'ApplicationEvents' with Id '2da16dbf-ea47-448e-a00f-fc442c3109ba' already processed. Skipping!  
Found 1,261 files in 7.074 seconds. Beginning copy...
```



KAPE Modules (EDD) >>> .vhdx

```
Preparing VHDX container... + - X

df84\ActivitiesCache.db-shm' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\AAD.9b34a
814-50a1-4e9e-a5e6-f03b6c21df84\ActivitiesCache.db-shm'. Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\AAD.9b34a814-50a1-4e9e-a5e6-f03b6c21
df84\ActivitiesCache.db-wal' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\AAD.9b34a
814-50a1-4e9e-a5e6-f03b6c21df84\ActivitiesCache.db-wal'. Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db'
to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db'.
Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db-
shm' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.
db-shm'. Hashing source file...
Copied deferred file 'C:\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.db-
wal' to 'D:\Collections\DMETZ-W10\C\Users\dmetz\AppData\Local\ConnectedDevicesPlatform\b0be2ec34b6d5075\ActivitiesCache.
db-wal'. Hashing source file...

Copied 1,160 (Deduplicated: 101) out of 1,261 files in 76.7647 seconds. See '*_CopyLog.csv' in the VHD(X)/Zip located in
'D:\Collections\DMETZ-W10' for copy details

Using Module operations
Setting --msource to 'D:\Collections\DMETZ-W10' since --source was not provided
Creating module destination directory 'D:\Collections\DMETZ-W10\Decrypt'
Found processor 'Executable: EDD\EDDv302.exe, Cmd line: /batch >> %destinationDirectory%, Export: txt, A
ppend: False!
Discovered 1 processor to run.
Executing modules with file masks...
Executing remaining modules...
Running 'EDD\EDDv302.exe': /batch >> D:\Collections\DMETZ-W10\Decrypt\LiveResponse
Executed 1 processor in 2.6672 seconds
Initializing VHDX creation. This may take a while...
```



Encrypted Disk Detector (EDD)

```
Administrator: PowerShell + - X
VHDX file 'D:\Collections\DMETZ-W10\2022-02-11T193611_DMETZ-W10.vhdx' created.
Cleaning up files in 'D:\Collections\DMETZ-W10'...
Total execution time: 122.9963 seconds
Encrypted Disk Detector v3.0.2
Copyright (c) 2009-2021 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is governed by the End User License Agreement available at www.magnetforensics.com/legal. //
* Checking physical drives on system... *
Checking PhysicalDrive1 - Samsung Portable SSD T5 SCSI Disk Device (1,000 GB) - Status: OK
Checking PhysicalDrive2 - USB Flash Disk USB Device (2 GB) - Status: OK
Checking PhysicalDrive0 - SKHynix_HFS512GDE9X081N (512 GB) - Status: OK
* Completed checking physical drives on system. *
* Now checking logical volumes on system... *
Drive C: [Label: Windows] (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 511 GB, Free Space: 78 GB
Drive D: [Label: T5-X] (PhysicalDrive1), Drive Type: Fixed, Filesystem: exFAT, Size: 1,000 GB, Free Space: 828 GB
Drive F: [Label: AXIOM - C20200122001664] (PhysicalDrive2), Drive Type: Removable, Filesystem: NTFS, Size: 2 GB, Free Space: 2 GB
* Completed checking logical volumes on system. *
* Running Secondary Bitlocker Check... *
Volume C: [Windows] is encrypted using Bitlocker.
* Completed Secondary Bitlocker Check... *
* Checking for running processes... *
* Completed checking running processes. *
*** Encrypted volumes and/or processes were detected by EDD. ***
Retrieving BitLocker Keys
```



Bitlocker Recovery Key Extraction

```
Administrator: PowerShell
ace: 2 GB
* Completed checking logical volumes on system. *
* Running Secondary Bitlocker Check... *
Volume C: [Windows] is encrypted using Bitlocker.
* Completed Secondary Bitlocker Check... *
* Checking for running processes... *
* Completed checking running processes. *
*** Encrypted volumes and/or processes were detected by EDD. ***
Retrieving BitLocker Keys

KeyProtectorId      : {185E68FA-7B39-4908-8419-126E20CFF54E}
AutoUnlockProtector :
KeyProtectorType    : Tpm
KeyFileName         :
RecoveryPassword   :
KeyCertificateType :
Thumbprint          :

KeyProtectorId      : {6F0700E7-557A-464C-948F-0DE868F51700}
AutoUnlockProtector :
KeyProtectorType    : RecoveryPassword
KeyFileName         :
RecoveryPassword   : 6484[REDACTED]549967
KeyCertificateType :
Thumbprint          :

** Process Complete **

PS D:\> |
```



Collection Output

The screenshot displays two separate file explorers side-by-side, both titled "Search DMETZ-W10".

Top File Explorer (DMETZ-W10 Collection):

Name	Date modified	Type	Size
Decrypt	2/15/2022 8:27 AM	File folder	
2022-02-15T132640_ConsoleLog.txt	2/15/2022 8:28 AM	Text Document	106 KB
2022-02-15T132640_DMETZ-W10.vhdx	2/15/2022 8:28 AM	Hard Disk Image File	4,329,472 KB
collection-complete.txt	2/15/2022 8:28 AM	Text Document	1 KB
DMETZ-W10_20220215_082500.raw	2/15/2022 8:26 AM	RAW File	18,341,888 KB
DMETZ-W10_build.txt	2/15/2022 8:26 AM	Text Document	1 KB

Bottom File Explorer (LiveResponse):

Name	Date modified	Type
DMETZ-W10_recovery.txt	2/15/2022 8:28 AM	Text Document
EDD.txt	2/15/2022 8:27 AM	Text Document

Hardware Choices



15:30 mem done

20:00 vhdx

25:48 done

1:45 mem done

3:15 vhdx

3:55 done



Evidence Processing Tips





Memory Processing

PS D:\Collections\DMETZ-W10> gc .\DMETZ-W10_build.txt

Major	Minor	Build	Revision
10	0	19043	0

PS D:\Collections\DMETZ-W10>

Magnet AXIOM Process 5.9.0.30292

EVIDENCE SOURCES

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
- Vehicle 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_10240_17770

KDBG address: Win10x64_19041

Memory artifacts powered by Volatility

BACK NEXT



VMDK Image Processing

Magnet AXIOM Process 5.9.0.30292

File Tools Help

CASE DETAILS

EVIDENCE SOURCES

PROCESSING DETAILS

- Search archives and mobile backups On
- 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
- Vehicle artifacts

ANALYZE EVIDENCE

EVIDENCE SOURCES

WINDOWS SELECT EVIDENCE SOURCE

DRIVE IMAGE FILES & FOLDERS VOLUME SHADOW COPY MEMORY

Select the image

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 interface. On the left, there's a sidebar with sections for Case Details, Evidence Sources (which is selected), Processing Details, Artifact Details (0), and Analyze Evidence. The Processing Details section contains several options like searching archives and calculating hash values. Below that is a section for Artifact Details with categories for Computer, Mobile, Cloud, and Vehicle artifacts. The main area is titled 'EVIDENCE SOURCES' and 'WINDOWS SELECT EVIDENCE SOURCE'. It features five icons: DRIVE, IMAGE (which is selected and highlighted in blue), FILES & FOLDERS, VOLUME SHADOW COPY, and MEMORY. Below this is a 'Select the image' dialog box. The dialog shows a file tree starting from 'This PC' and navigating to 'T5-X (D:) > Collections > DMETZ-W10'. Inside this folder, it lists three items: 'Decrypt' (a folder), '2022-02-15T132640_DMETZ-W10.vhdx' (a Hard Disk Image File), and 'DMETZ-W10_20220215_082500.raw' (a RAW File). At the bottom of the dialog, there's a file name field set to '2022-02-15T132640_DMETZ-W10.vhdx', a dropdown for 'All Supported Images (*.E01, ...)', and 'Open' and 'Cancel' buttons.



Memory Artifacts from Volatility

MATCHING RESULTS (56 of 56)

	Prot...	Local IP Ad...	Remote IP...	State	Proc...	Owner	Created Date/T...	Artifact type
	TCPv4	0.0.0.0:49666	0.0.0.0:	LISTENING	1568	svchost.exe	7/13/2021 6:32:56 PM	Network Info (ne
	TCPv4	192.168.4.64:49788	23.41.169.130:80	ESTABLISHED	-1			Network Info (ne
	UDPV4	0.0.0.0:	*.*		3284	dasHost.exe	7/13/2021 6:33:00 PM	Network Info (ne
	UDPV6	::0	*.*		3284	dasHost.exe	7/13/2021 6:33:00 PM	Network Info (ne
	UDPV4	0.0.0.0:	*.*		3284	dasHost.exe	7/13/2021 6:33:00 PM	Network Info (ne
	TCPv4	0.0.0.0:5040	0.0.0.0:	LISTENING	6632	svchost.exe	7/13/2021 6:33:13 PM	Network Info (ne
	TCPv4	192.168.4.64:139	0.0.0.0:	LISTENING	4	System	7/13/2021 6:33:02 PM	Network Info (ne
	TCPv4	192.168.4.64:49787	23.41.169.130:80	CLOSE_WAIT	-1			Network Info (ne
	UDPV4	0.0.0.0:	*.*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
	UDPV4	0.0.0.0:	*.*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
	UDPV6	::0	*.*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
	UDPV6	::0	*.*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
	UDPV4	0.0.0.0:	*.*		3976	svchost.exe	7/14/2021 10:41:13 AM	Network Info (ne
	UDPV4	0.0.0.0:	*.*		6632	svchost.exe	7/13/2021 6:33:11 PM	Network Info (ne
	TCPv4	0.0.0.0:47001	0.0.0.0:	LISTENING	4	System	7/13/2021 6:35:01 PM	Network Info (ne
	TCPv6	::47001	::0	LISTENING	4	System	7/13/2021 6:35:01 PM	Network Info (ne
	TCPv4	0.0.0.0:7680	0.0.0.0:	LISTENING	4188	svchost.exe	7/13/2021 6:34:59 PM	Network Info (ne
	TCPv6	::7680	::0	LISTENING	4188	svchost.exe	7/13/2021 6:34:59 PM	Network Info (ne
	TCPv4	0.0.0.0:5357	0.0.0.0:	LISTENING	4	System	7/13/2021 6:33:04 PM	Network Info (ne
	TCPv6	::5357	::0	LISTENING	4	System	7/13/2021 6:33:04 PM	Network Info (ne
	TCPv4	192.168.4.64:49782	104.117.182.56:443	CLOSE_WAIT	-1			Network Info (ne
	TCPv4	192.168.4.64:49786	23.41.169.130:80	CLOSE_WAIT	-1			Network Info (ne
	UDPV6	::0	*.*		3064	svchost.exe	7/15/2021 8:28:59 PM	Network Info (ne
	UDPV4	0.0.0.0:	*.*		3064	svchost.exe	7/15/2021 8:28:59 PM	Network Info (ne
	UDPV4	0.0.0.0:	*.*		3064	svchost.exe	7/15/2021 7:04:52 PM	Network Info (ne
	UDPV6	::0	*.*		3064	svchost.exe	7/15/2021 7:04:52 PM	Network Info (ne



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)

Order Command List (UTF8) Command List (Raw) Artifact type

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 (\$_.Fre...)	b' @({n="Free (%)"e=(if(\$_.Size) ("0:N2" -f (\$_.Fre...)	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

Column view

1

2022-02-15T132640_DMETZ-W10.vhdx

DETAILS

ARTIFACT INFORMATION

- 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.vhdx - 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.vhdx

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/Time	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 exception list.	{8B724E29-6C65-4399-B1C8}
2004	2/14/2022 8:53:04 PM	308	A rule has been added to the Windows Firewall exception list.	{A8E695EF-27BD-4830-B3AF}
2004	2/14/2022 8:53:04 PM	309	A rule has been added to the Windows Firewall exception list.	{3B65252B-E881-4B31-B91C}
2004	2/14/2022 8:53:04 PM	310	A rule has been added to the Windows Firewall exception list.	{E344DFB1-72BC-43AF-B0A1}
2004	2/14/2022 8:53:04 PM	311	A rule has been added to the Windows Firewall exception list.	{57D99815-6AF3-41B1-B824}
2004	2/14/2022 8:53:17 PM	312	A rule has been added to the Windows Firewall exception list.	{80F1EA52-4FED-40F1-98E7}
2004	2/14/2022 8:53:17 PM	313	A rule has been added to the Windows Firewall exception list.	{FC968866-F413-4D1B-A0C2}
2006	2/14/2022 8:54:33 PM	314	A rule has been deleted in the Windows Firewall exception list.	{3B65252B-E881-4B31-B91C}
2006	2/14/2022 8:54:33 PM	315	A rule has been deleted in the Windows Firewall exception list.	{A8E695EF-27BD-4830-B3AF}
2004	2/14/2022 8:49:31 PM	10	A rule has been added to the Windows Firewall exception list.	{884168A9-58A1-4719-A111}
2004	2/14/2022 8:49:31 PM	13	A rule has been added to the Windows Firewall exception list.	{47E0E03C-07D3-417E-933A}
2004	2/14/2022 8:49:31 PM	12	A rule has been added to the Windows Firewall exception list.	{FC8AEA85-1A02-459A-98F/}
2006	2/14/2022 8:49:31 PM	14	A rule has been deleted in the Windows Firewall exception list.	{FC8AEA85-1A02-459A-98F/}
2004	2/14/2022 8:49:31 PM	11	A rule has been added to the Windows Firewall exception list.	{167FD499-2C58-437E-B2FF}
2006	2/14/2022 8:49:31 PM	15	A rule has been deleted in the Windows Firewall exception list.	{167FD499-2C58-437E-B2FF}
2006	2/14/2022 8:49:31 PM	16	A rule has been deleted in the Windows Firewall exception list.	{884168A9-58A1-4719-A111}
2006	2/14/2022 8:49:31 PM	17	A rule has been deleted in the Windows Firewall exception list.	{47E0E03C-07D3-417E-933A}
2004	2/14/2022 8:49:31 PM	18	A rule has been added to the Windows Firewall exception list.	{2337CE28-2973-4EA5-96EB}
2004	2/14/2022 8:49:31 PM	19	A rule has been added to the Windows Firewall exception list.	{9864DEDA-F8CA-4990-98C}
2004	2/14/2022 8:49:31 PM	20	A rule has been added to the Windows Firewall exception list.	{6E024BF2-B25F-46E7-9203-}
2004	2/14/2022 8:49:31 PM	21	A rule has been added to the Windows Firewall exception list.	{8A6E7D10-A9D4-44AE-B2B}
2006	2/14/2022 8:51:10 PM	29	A rule has been deleted in the Windows Firewall exception list.	{3daa47ad-4db9-45b8-8f97-}
2006	2/14/2022 8:51:10 PM	30	A rule has been deleted in the Windows Firewall exception list.	{88d76b46-70a0-47be-ad62-}
2004	2/14/2022 8:51:10 PM	31	A rule has been added to the Windows Firewall exception list.	{8044754e-571c-414a-b91b-}
2004	2/14/2022 8:51:10 PM	32	A rule has been added to the Windows Firewall exception list.	{7f42b00-bd25-41f9-ba12-}
2006	2/14/2022 8:51:10 PM	33	A rule has been deleted in the Windows Firewall exception list.	{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-A0C2-90F0F00EFA02}**
 Rule Name **OneDrive**
 Modifying User **S-1-5-80-3088073201-1464728630-1879813800-1107566885-823218052**
 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</Keywords>

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 Partial results Keyword lists Skin tone

Type a search term... GO ADVANCED

EVIDENCE (69,398)

Entr...	Application Name	Full Path	Recorded
70970	SMB	System\SMB	12/23/2021
28271	SMB	System\SMB	1/28/2022 4:
71080	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...	2/7/2022 5:1
80279			1/31/2022 8:
73746			1/31/2022 8:
37402			1/4/2022 2:3
73739	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...	1/31/2022 8:
60863	SMB	System\SMB	1/18/2022 11:
61649			1/19/2022 7:
73557			1/31/2022 4:
55880	SMB	System\SMB	1/14/2022 1:
73550	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...	1/31/2022 4:
37535	SMB	System\SMB	1/4/2022 5:3
62551			1/20/2022 7:
55904	SMB	System\SMB	1/14/2022 1:
61640	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...	1/19/2022 7:
56705			1/14/2022 6:
62543	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...	1/20/2022 7:
56695	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...	1/14/2022 6:
81459			2/8/2022 7:3
87369			2/14/2022 8:
87388	powerppt.exe	\device\harddiskvolume3\program files\microsoft\of...	2/14/2022 8:
55927	SMB	System\SMB	1/14/2022 1:
51669			1/13/2022 8:
70966	onedrive.exe	\device\harddiskvolume3\program files\microsoft\o...	1/28/2022 2:
51666	teams.exe	\device\harddiskvolume3\users\dmetz\appdata\loc...	1/13/2022 8:

18630

2022-02-15T132640_DMETZ-W10.vhdx

DETAILS

ARTIFACT INFORMATION

Entry ID	18630
Application Name	Microsoft.Windows.Search_1.14.2.19041_neutral_neutral_cw5n1h2txyewy
Full Path	Microsoft.Windows.Search_1.14.2.19041_neutral_neutral_cw5n1h2txyewy
Recorded Timestamp Date/Time	12/17/2021 1:21:00 PM
Security Identifier	S-1-12-1-2603919380-1318998177-1005643429-2229215596
Interface Type	IEEE80211
Network Name (SSID)	BakerStreet
Bytes Sent	9413
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 Imported

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: Doug Metz

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

[ADD NEW EVIDENCE](#)

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

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 IMEs.

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

EVIDENCE SOURCES

SELECT EVIDENCE SOURCE

- COMPUTER
- MOBILE
- CLOUD
- VEHICLE
- REMOTE COMPUTER

EVIDENCE SOURCES ADDED TO CASE

Type	Image - location name	Evidence number	Search type	Status
Computer artifacts	Windows 10 Pro	1	File search	Completed

EVIDENCE SOURCES

REMOTE COMPUTER DEPLOY AGENT

Provide information about the remote computer that you want to deploy the agent to.

Remote computer IP address: **MORIARTY**

User name: **dwmertz**

Password: *********

Agent location on remote computer: **C:**

DEPLOY AGENT

EVIDENCE SOURCES

REMOTE COMPUTER TO DOWNLOAD

Computer name: **MORIARTY**
User name: **dwmertz**
Local end point: **192.168.4.181**
Computer status: **Connected** Downloading the file system structure and metadata

STOP AND DELETE AGENT

REVIEW AND SELECT THE DATA FROM THE TARGET COMPUTER

Review the files and folders on the remote computer and select the drives, files, folders, and memory that you want to download. To save time searching the complete list of files and folders, select Targeted locations to view a list of typical files and folders that you might want to download.

ITEMS TO DOWNLOAD

The selected items will be saved to an ADF4-1 container **EDIT**

Item	Download start date/time	Items downloaded

BACK **NEXT**





Thank You



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



@dwmetz



doug.metz@magnetforensics.com



<https://bakerstreetforensics.com>