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

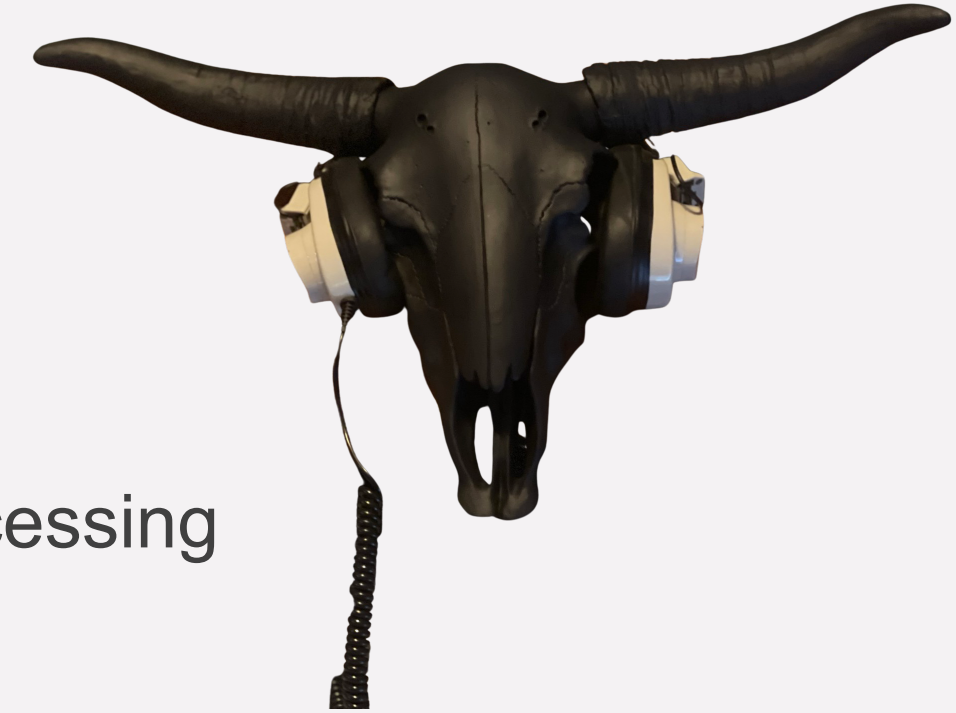
BAKER STREET FORENSICS

D . F . I . R .

WHERE IRREGULARS ARE PART OF THE GAME

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	CSIRT-Collect_USB
RAM (MRC)	RAM (MRC)
Triage (KAPE)	Triage (KAPE)
Compression	[omitted in USB edition]
Network share	USB device
-	Encrypted Disk Detection (EDD)
-	Bitlocker Key Recovery

Collect from Network Isolated Assets

USB Use Cases:

Ransomware response

Airgap; Manufacturing / Medical / ICS

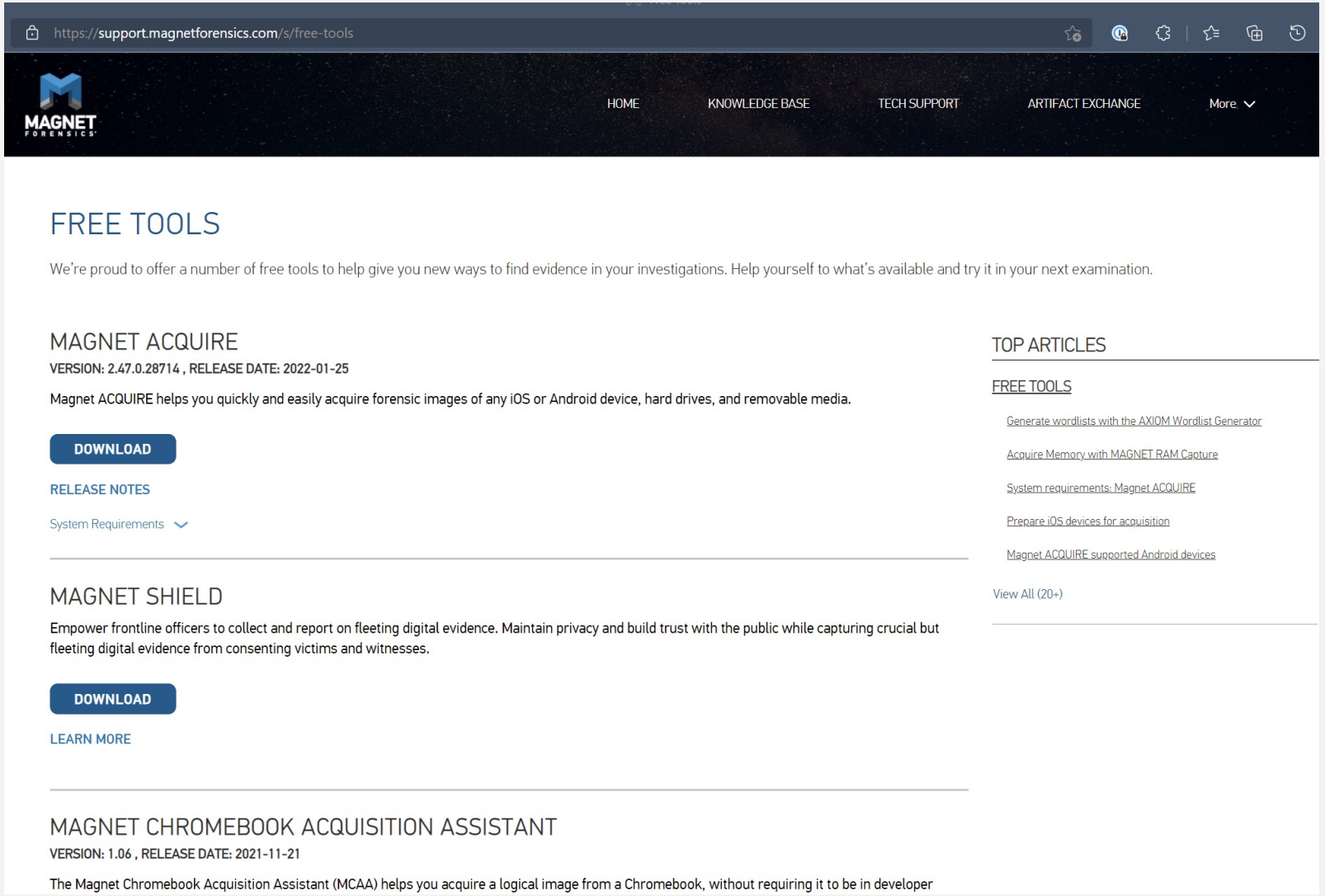
Enterprise resources not available

BOGHOK (Boots on Ground, Hands on Keyboard)

MAGNET Free Tools

MAGNET RAM CAPTURE

ENCRYPTED DISK DETECTOR (EDD)

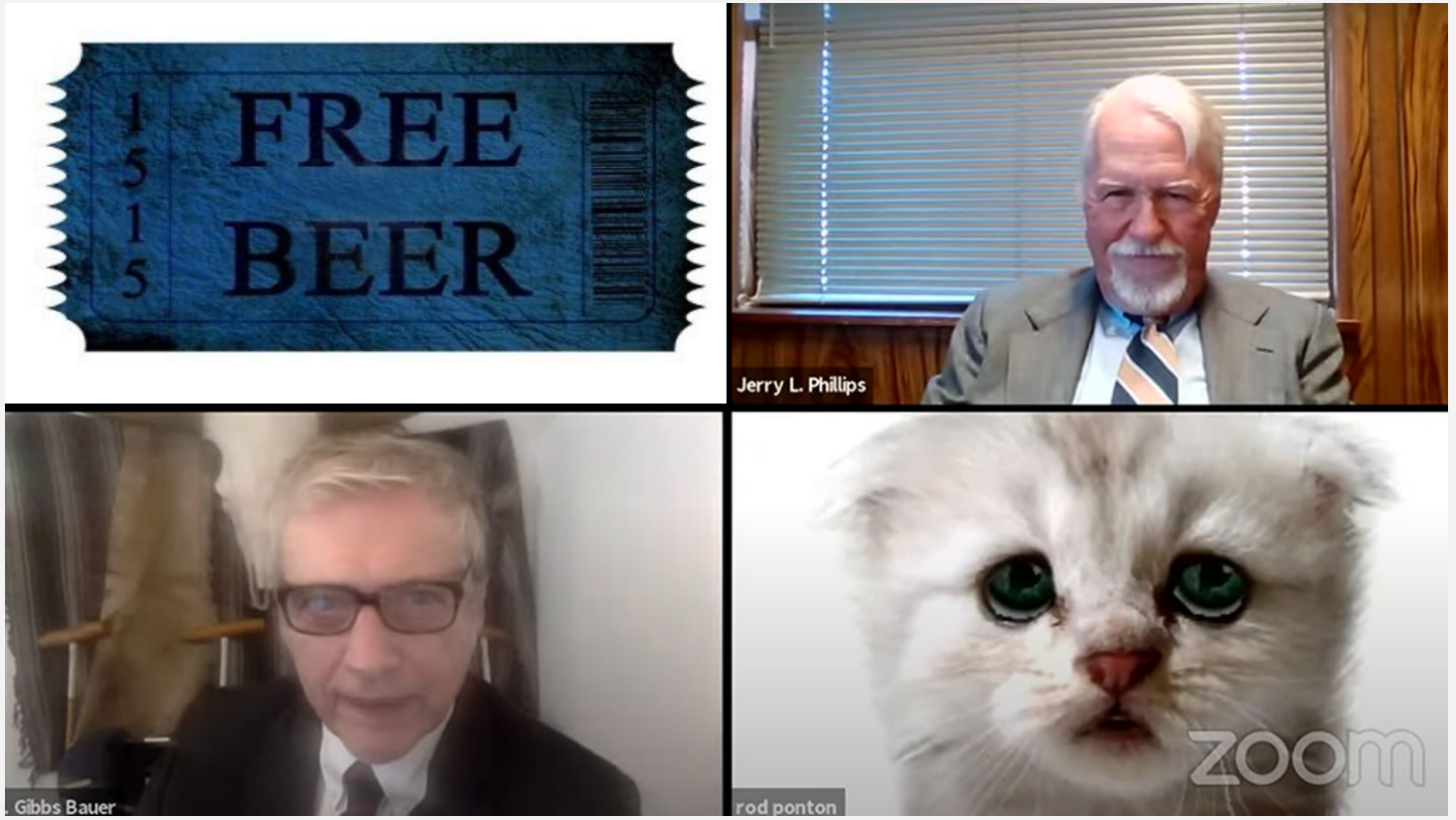


MAGNET FORENSICS — TECHNO SECURITY 2022

magnetforensics.com

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

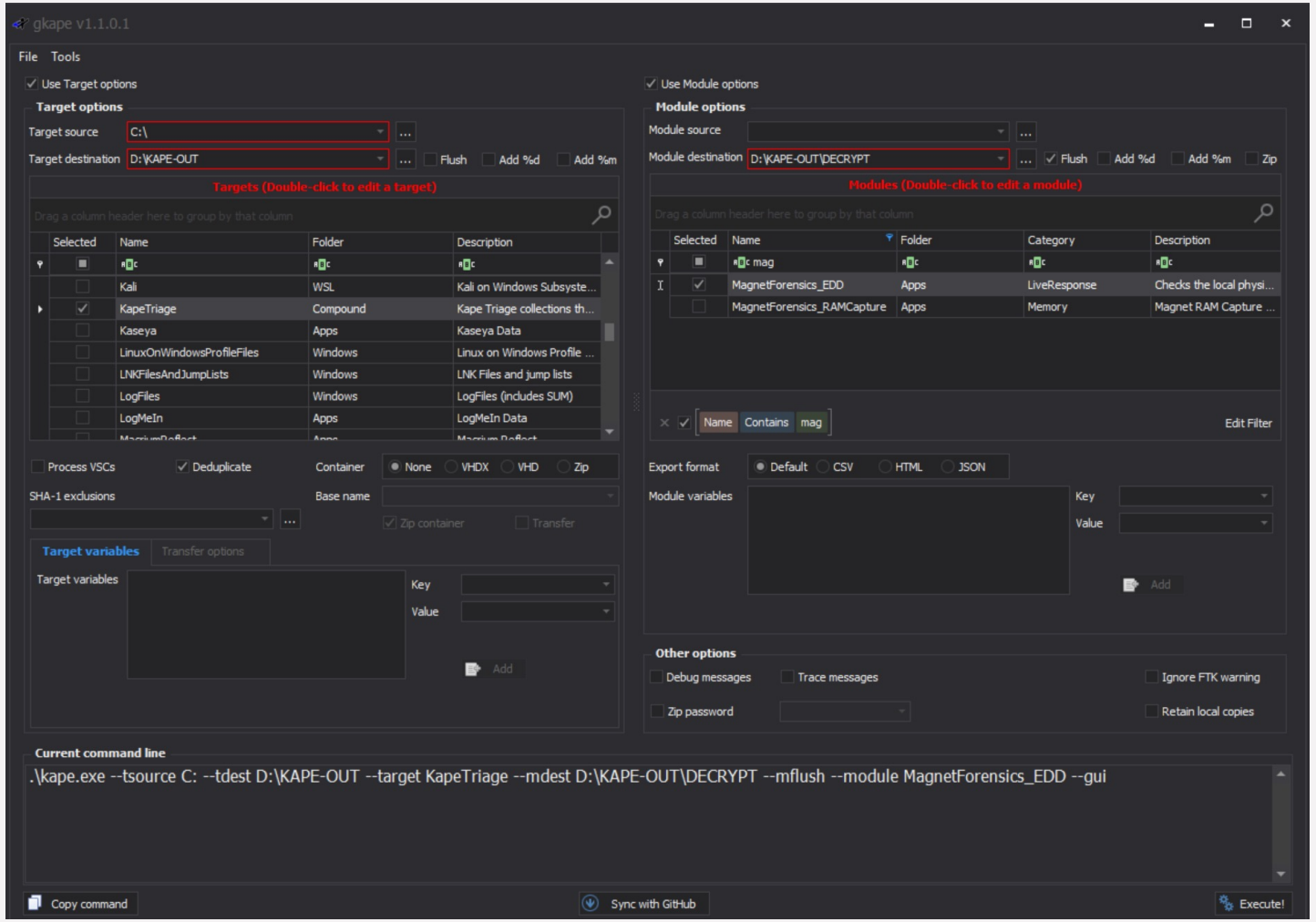
KAPE

GUI and Command Line

KAPE has two primary components, Targets & Modules.

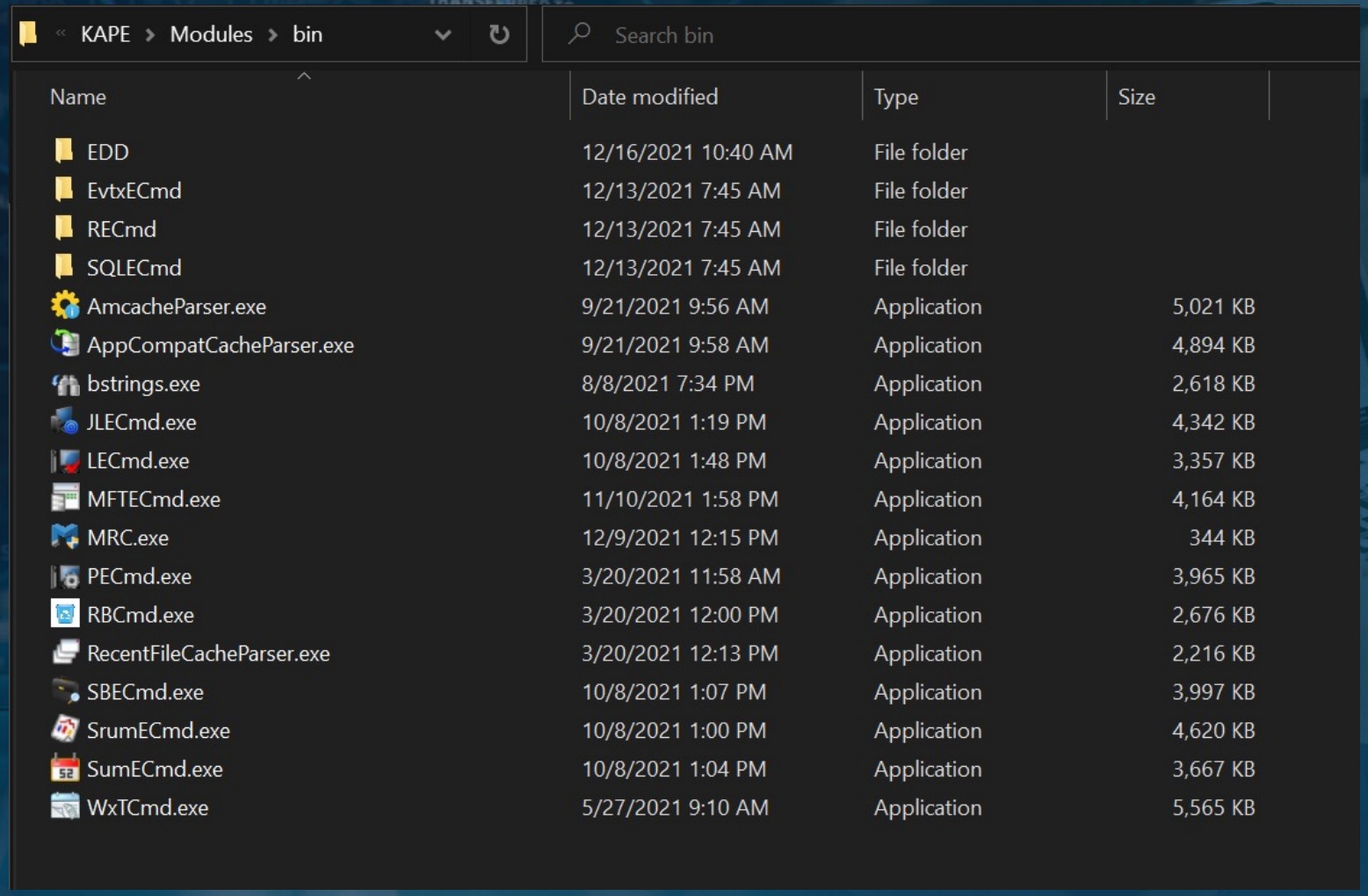
Targets: categories of artifacts that can be collected (registry, event logs, browser activity…)

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



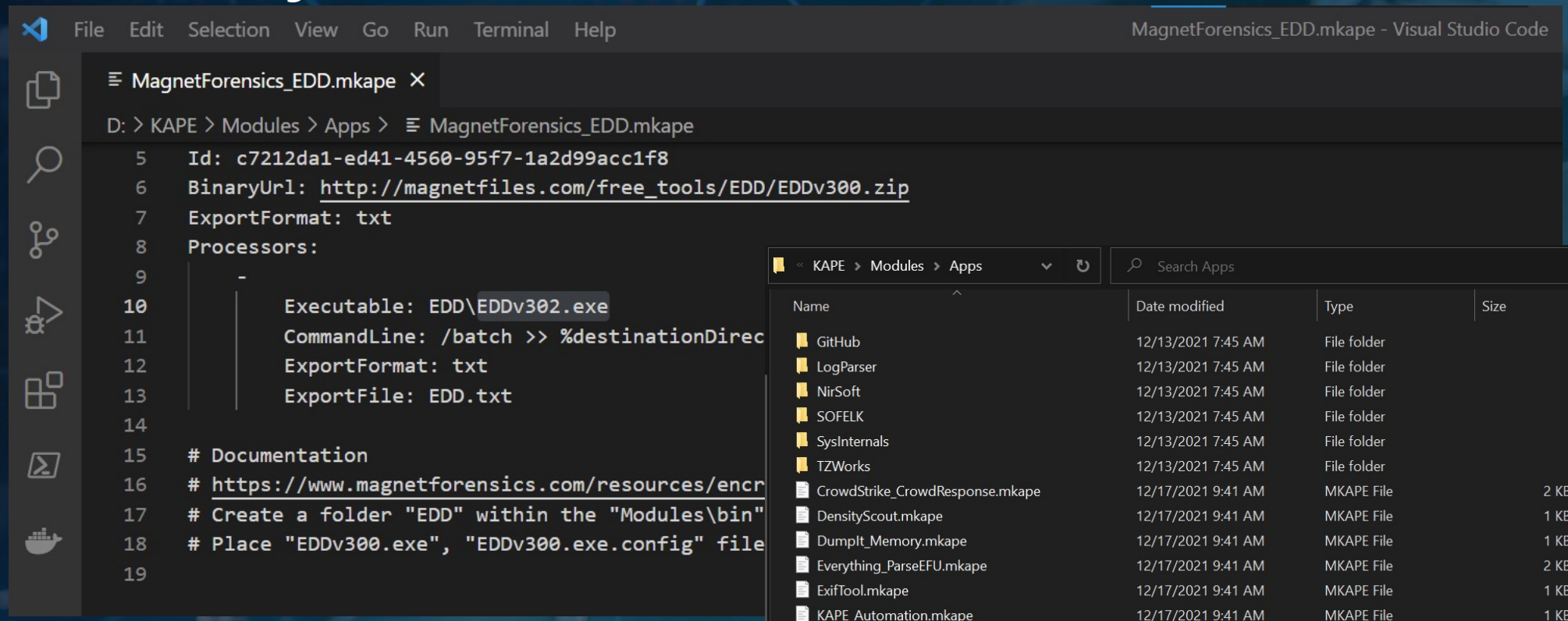
https://www.sans.org/tools/kape/

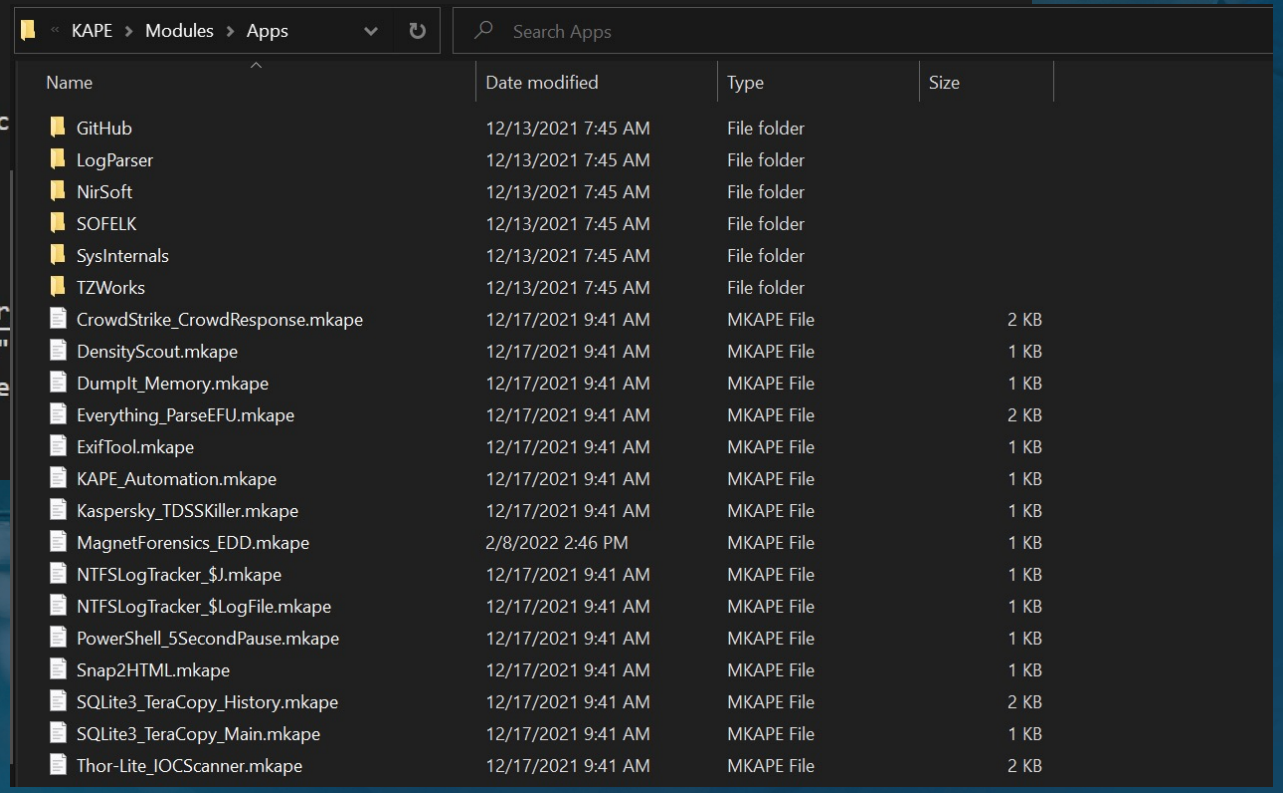
Tools in the /bin - BYOE



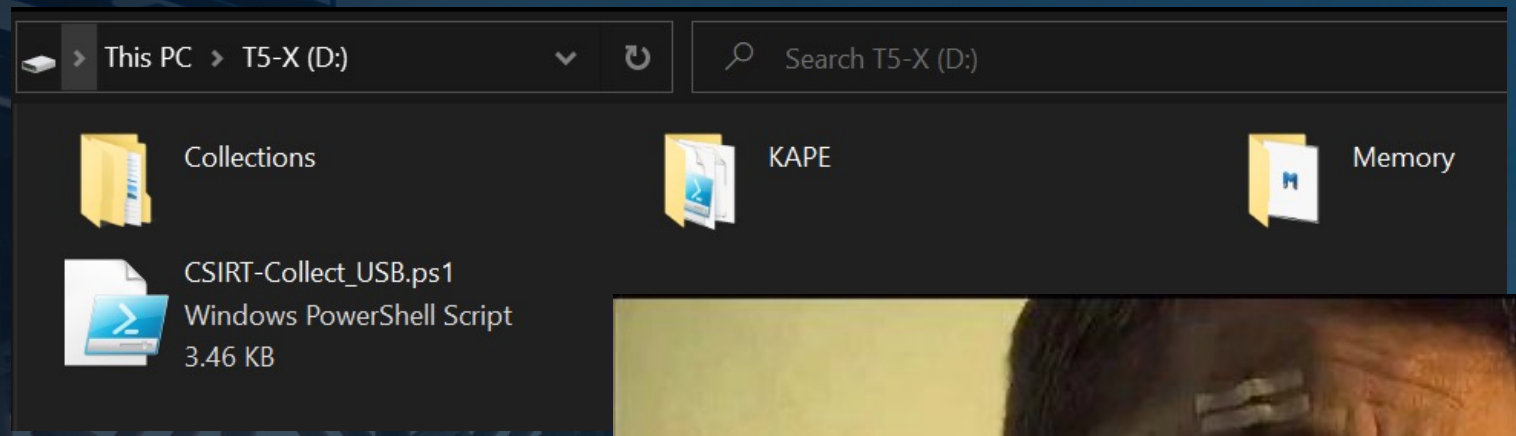
Name	Date modified	Type	Size
EDD	12/16/2021 10:40 AM	File folder	
EvtxECmd	12/13/2021 7:45 AM	File folder	
RECmd	12/13/2021 7:45 AM	File folder	
SQLECmd	12/13/2021 7:45 AM	File folder	
AmcacheParser.exe	9/21/2021 9:56 AM	Application	5,021 KB
AppCompatCacheParser.exe	9/21/2021 9:58 AM	Application	4,894 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
LECmd.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

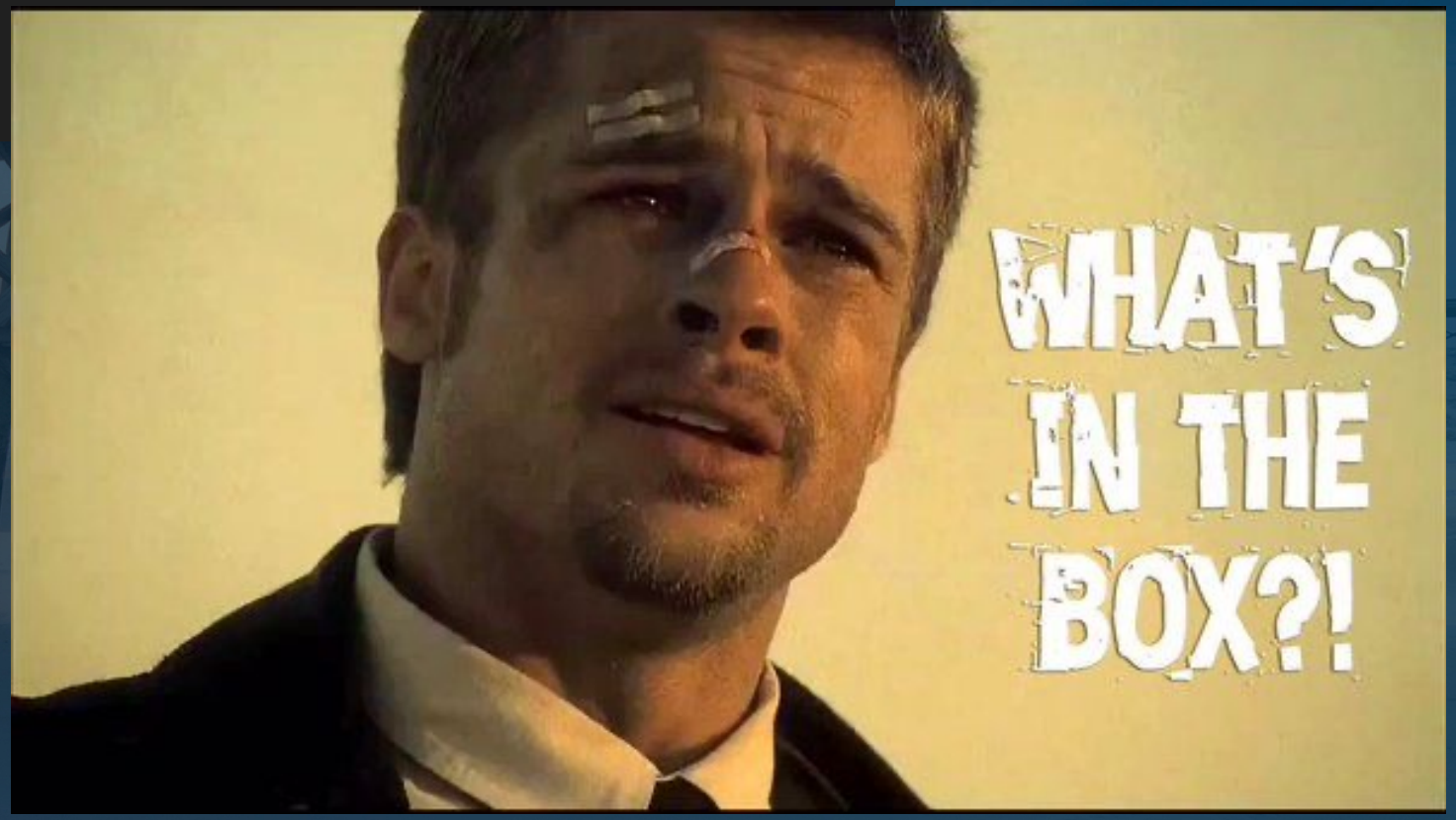
Check your binaries





USB Contents

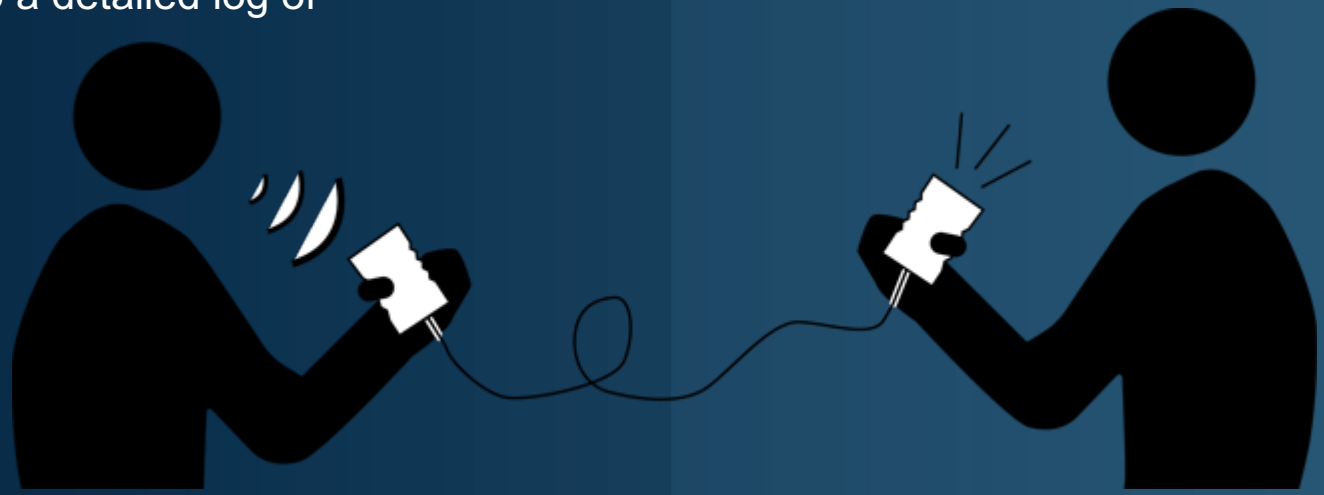




The Handoff

“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”



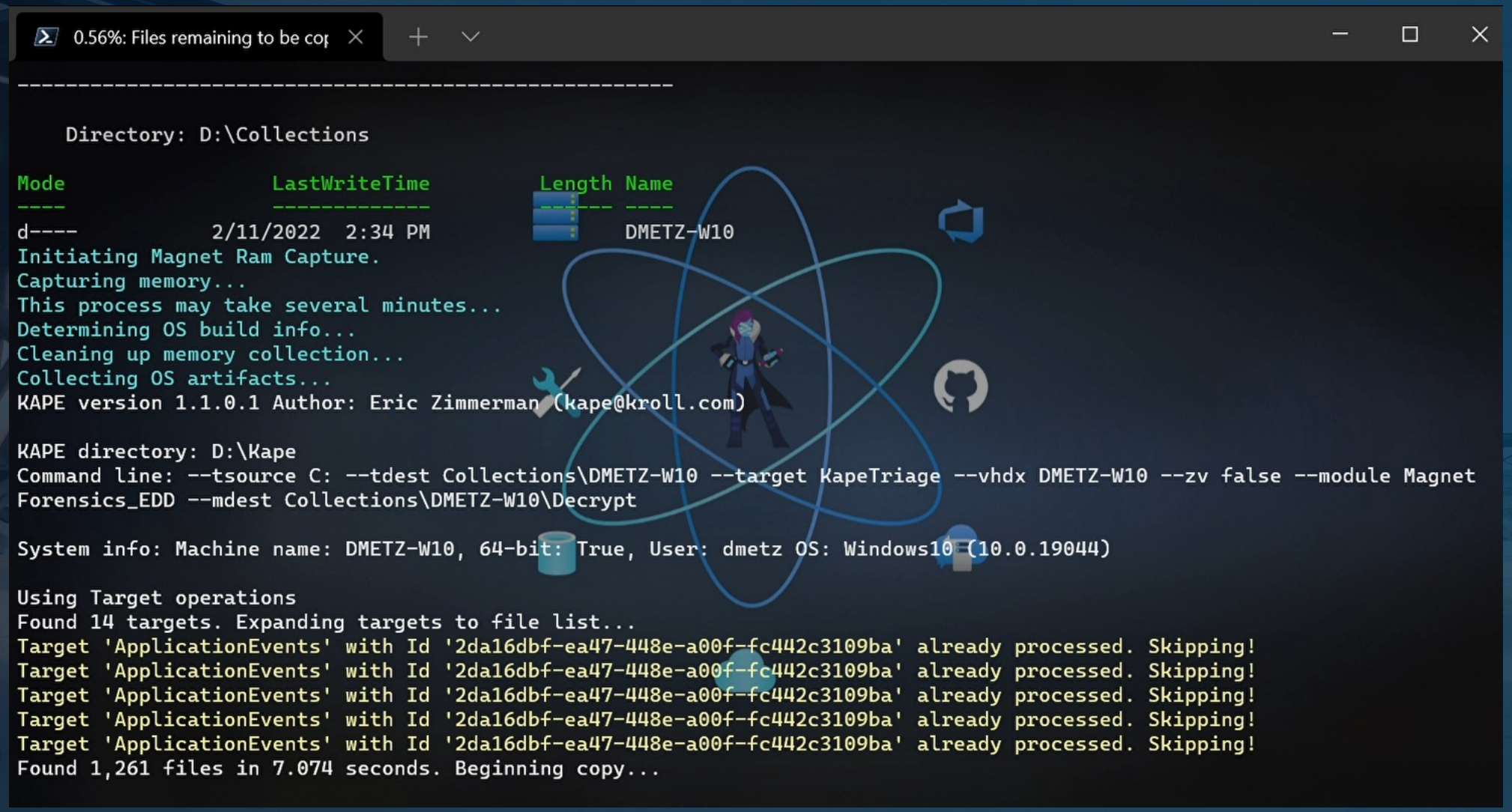
MAGNET FORENSICS — TECHNO SECURITY 2022

Script Walk Through

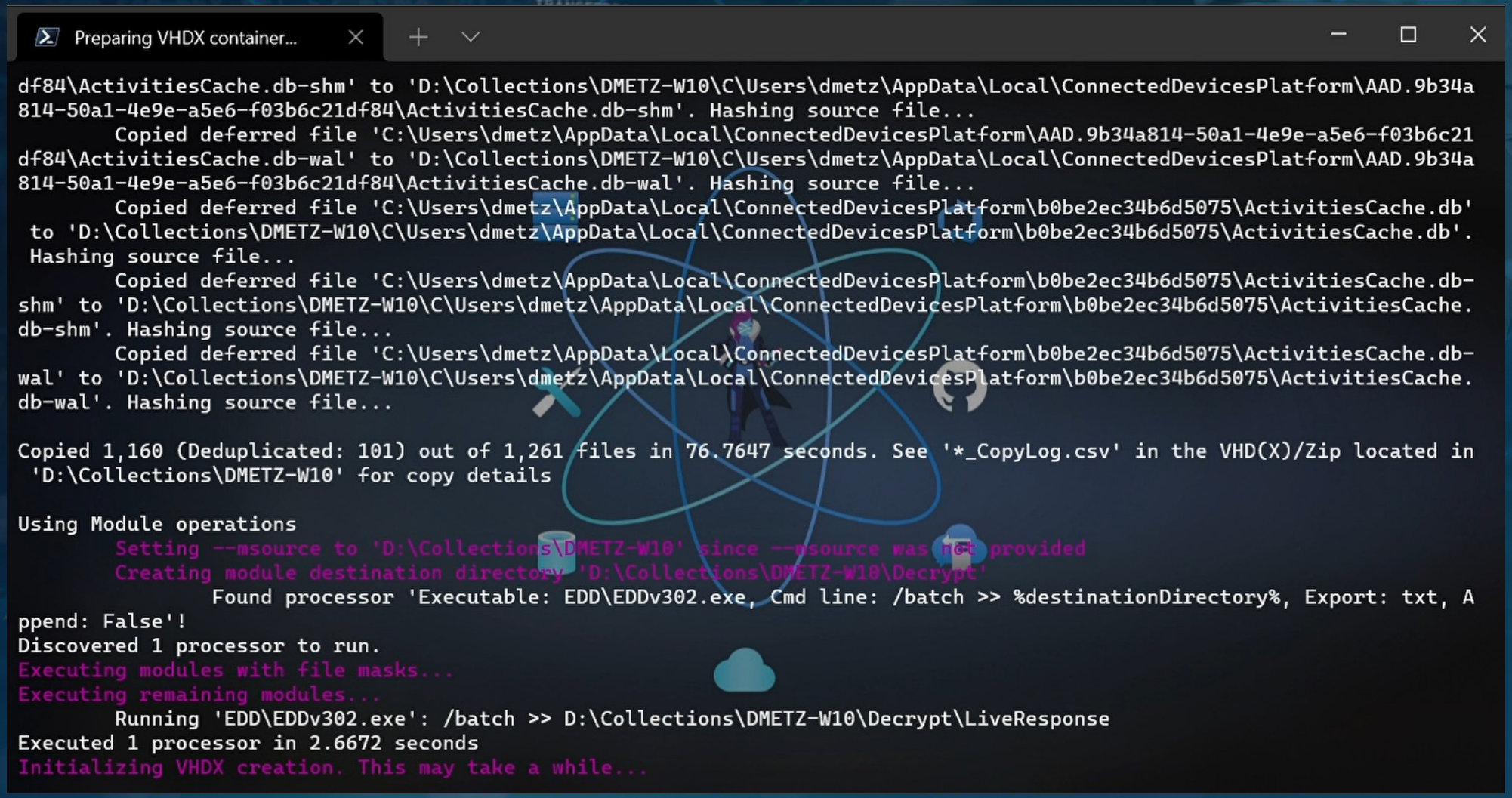
magnetforensics.com

Memory Collection

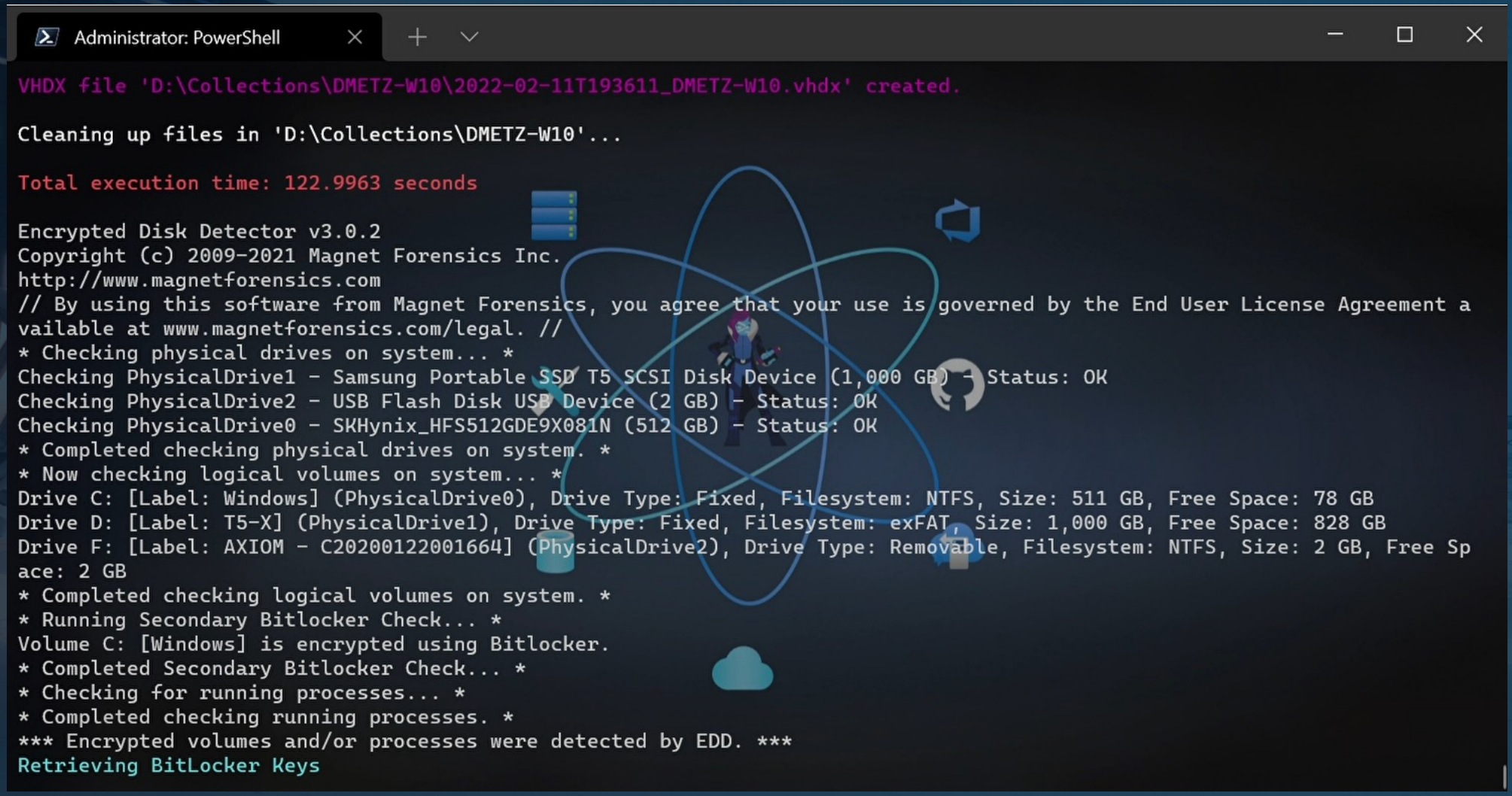
Build Info >>> KAPE Triage Execution



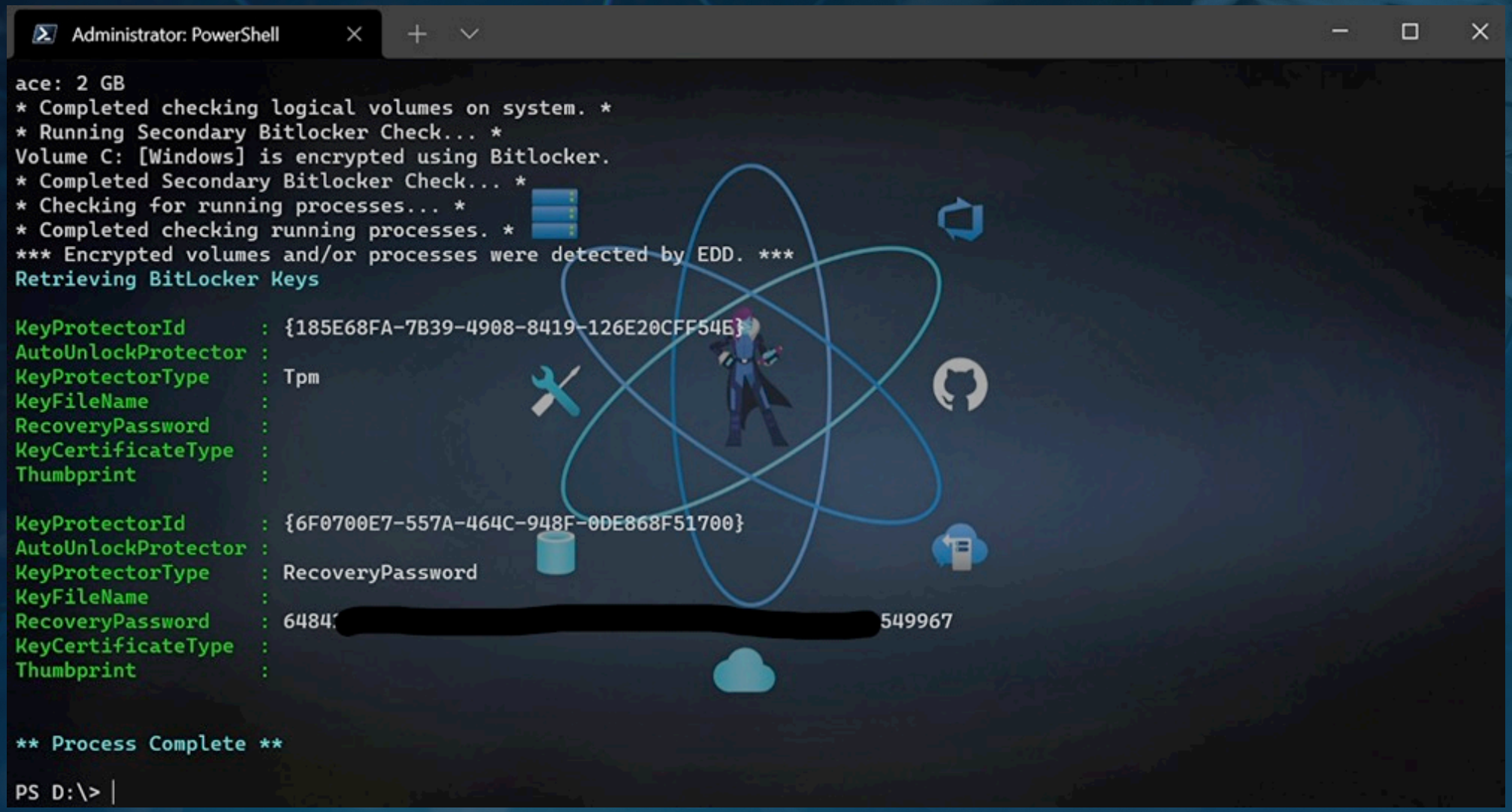
KAPE Modules (EDD) >>> .vhdx



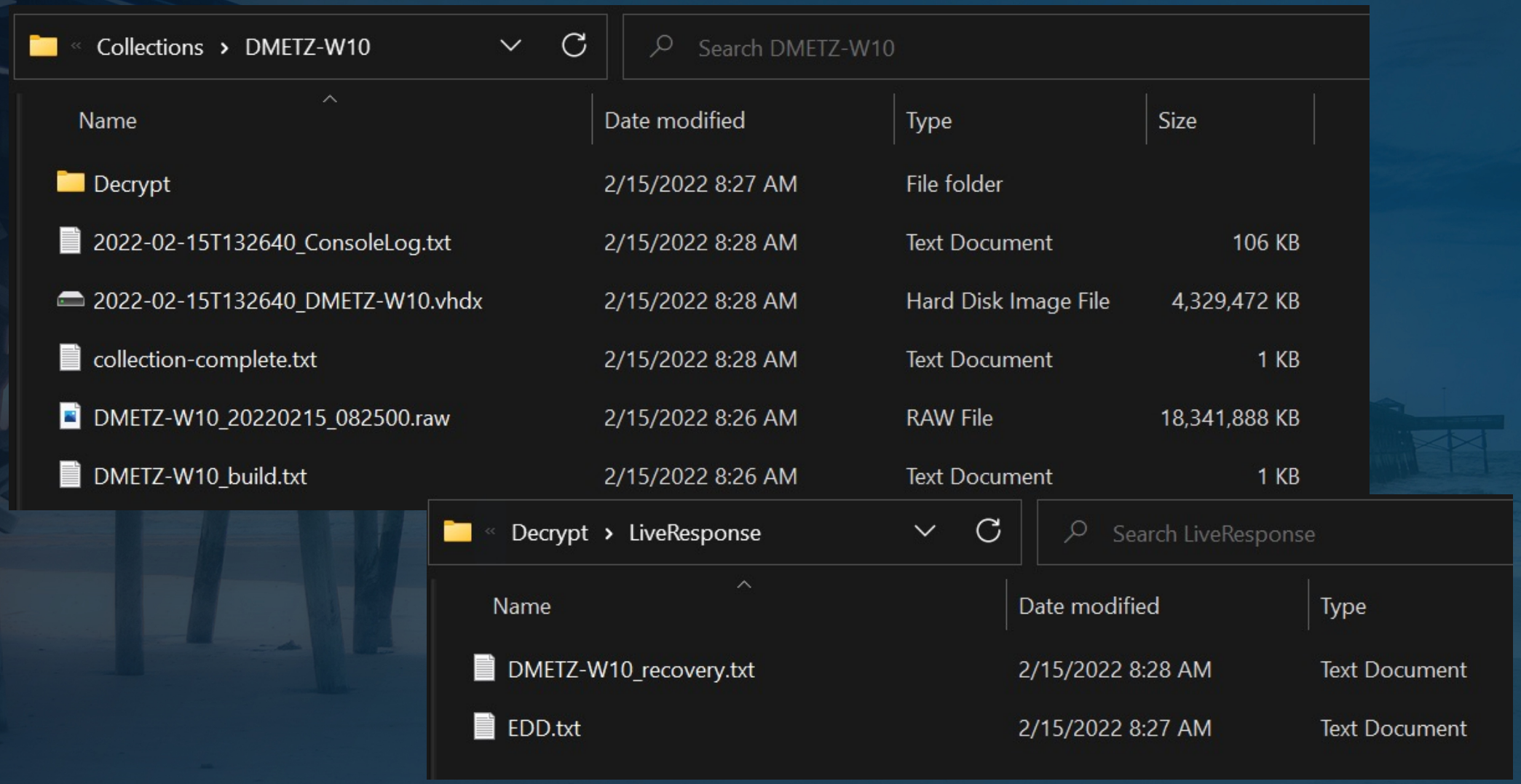
Encrypted Disk Detector (EDD)



Bitlocker Recovery Key Extraction



Collection Output



Hardware Choices

15:30 mem done

20:00 vhdx

25:48 done

1:45 mem done

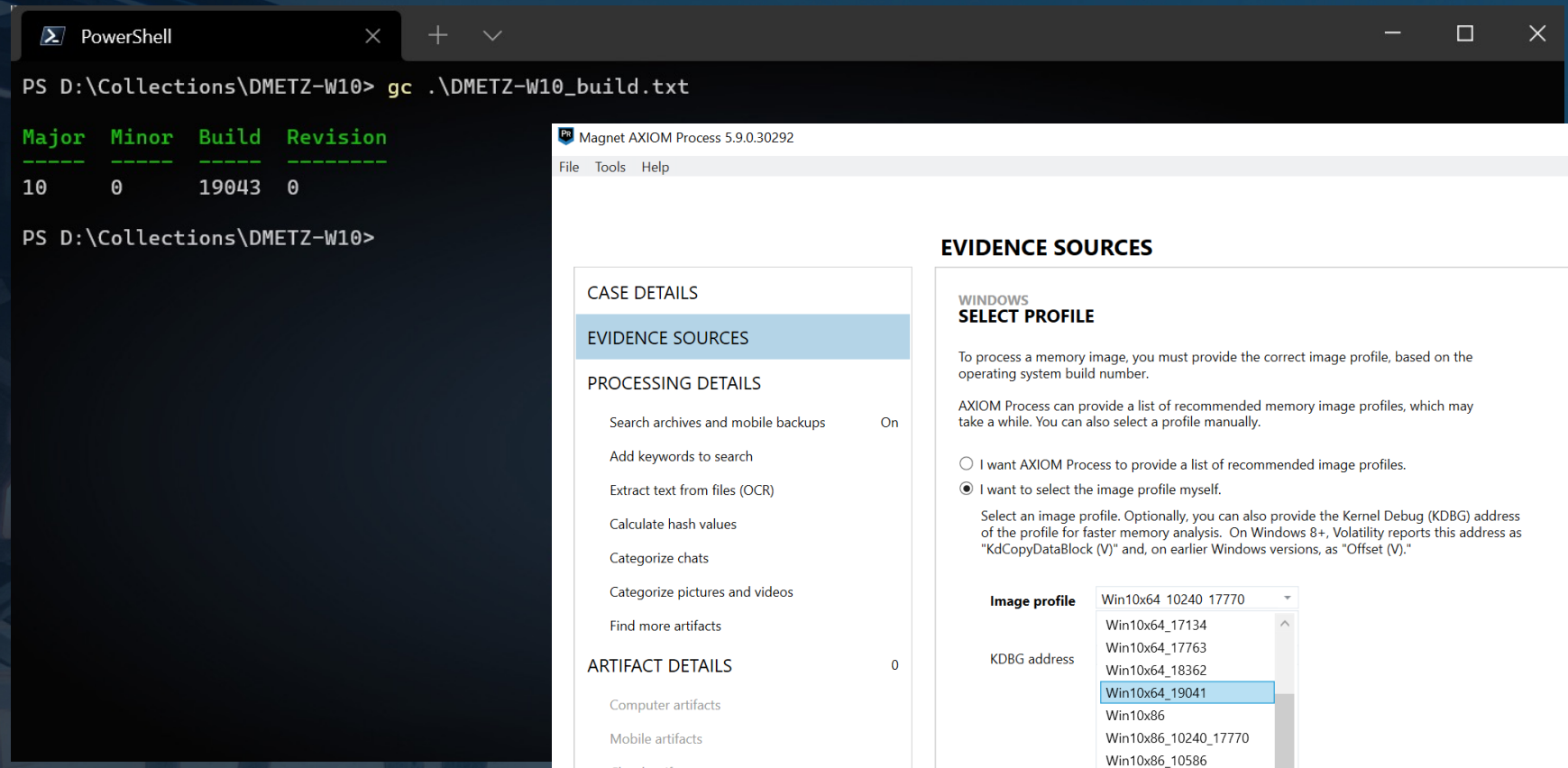
3:15 vhdx

3:55 done

Evidence Processing Tips

MAGNET FORENSICS — TECHNO SECURITY 2022

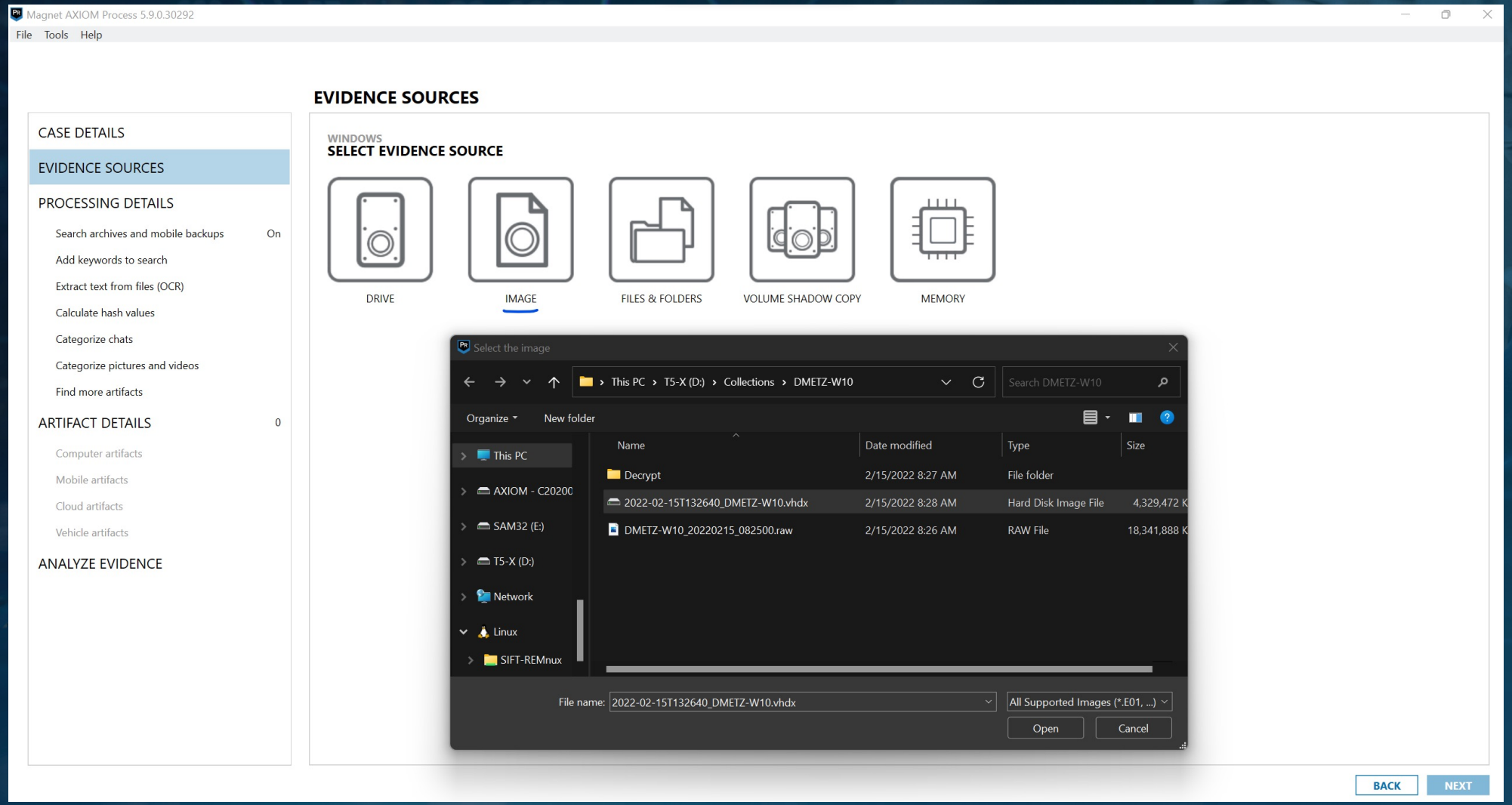
Memory Processing



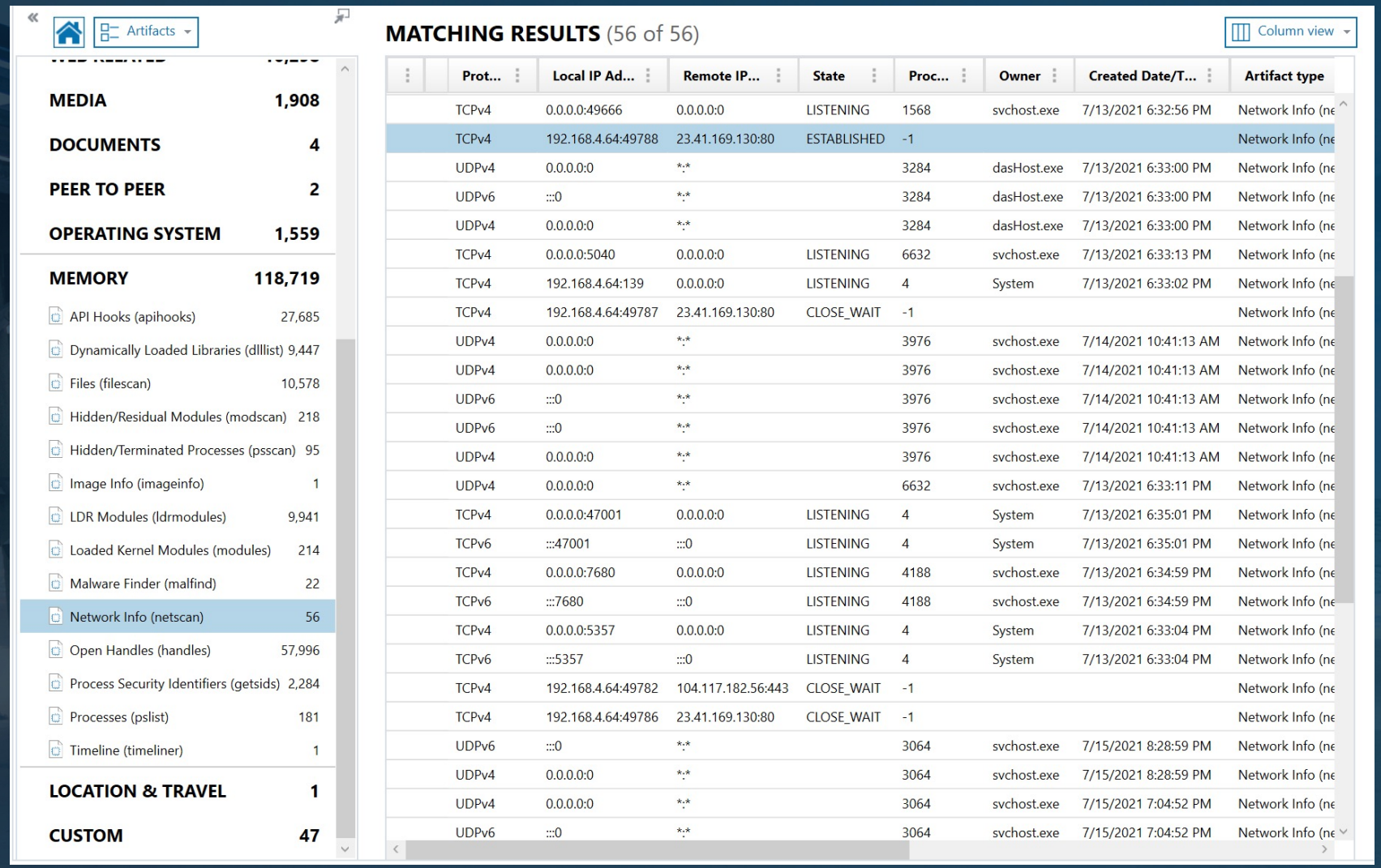
MAGNET FORENSICS — TECHNO SECURITY 2022

magnetforensics.com

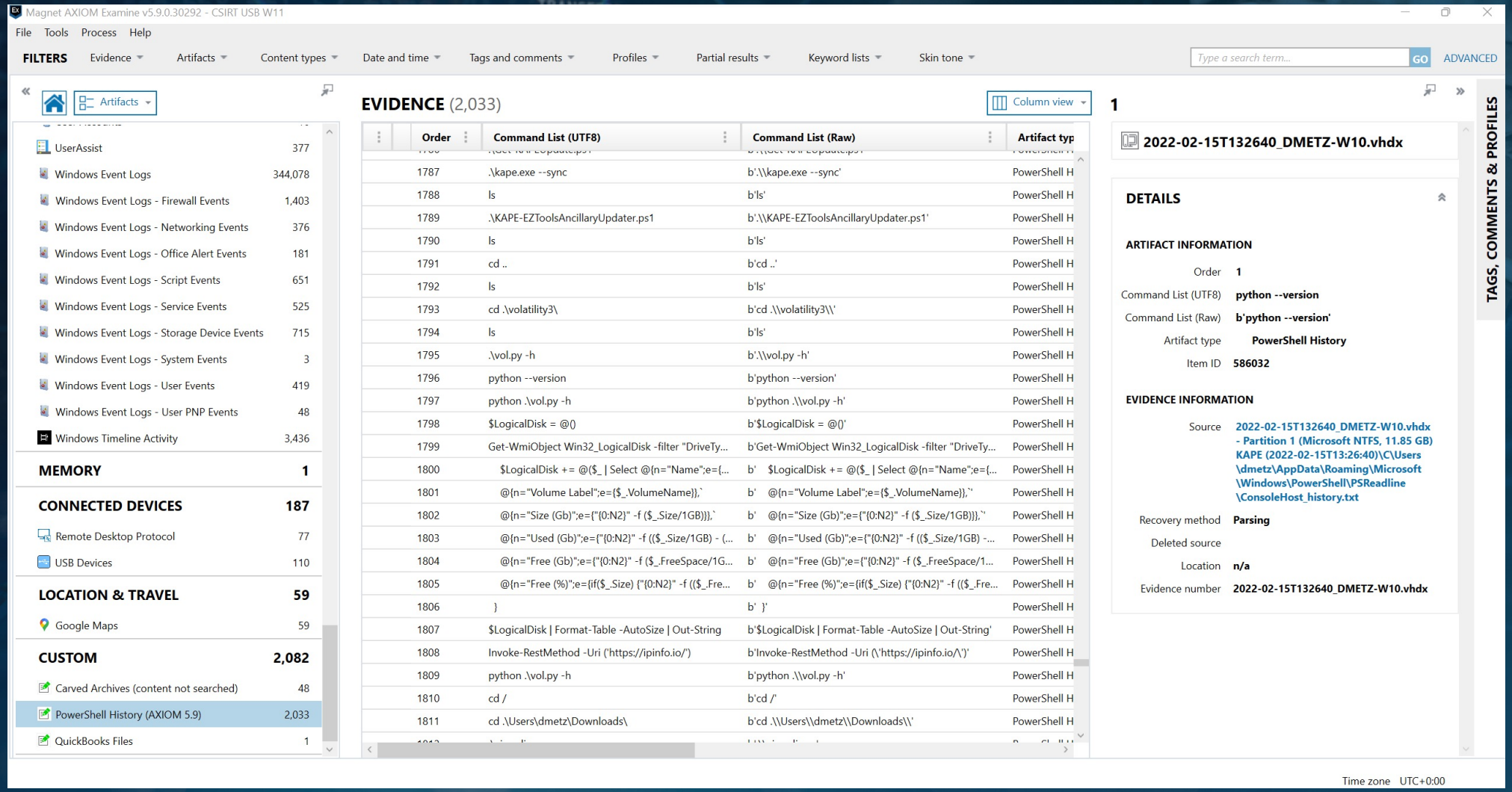
VMDK Image Processing



Memory Artifacts from Volatility

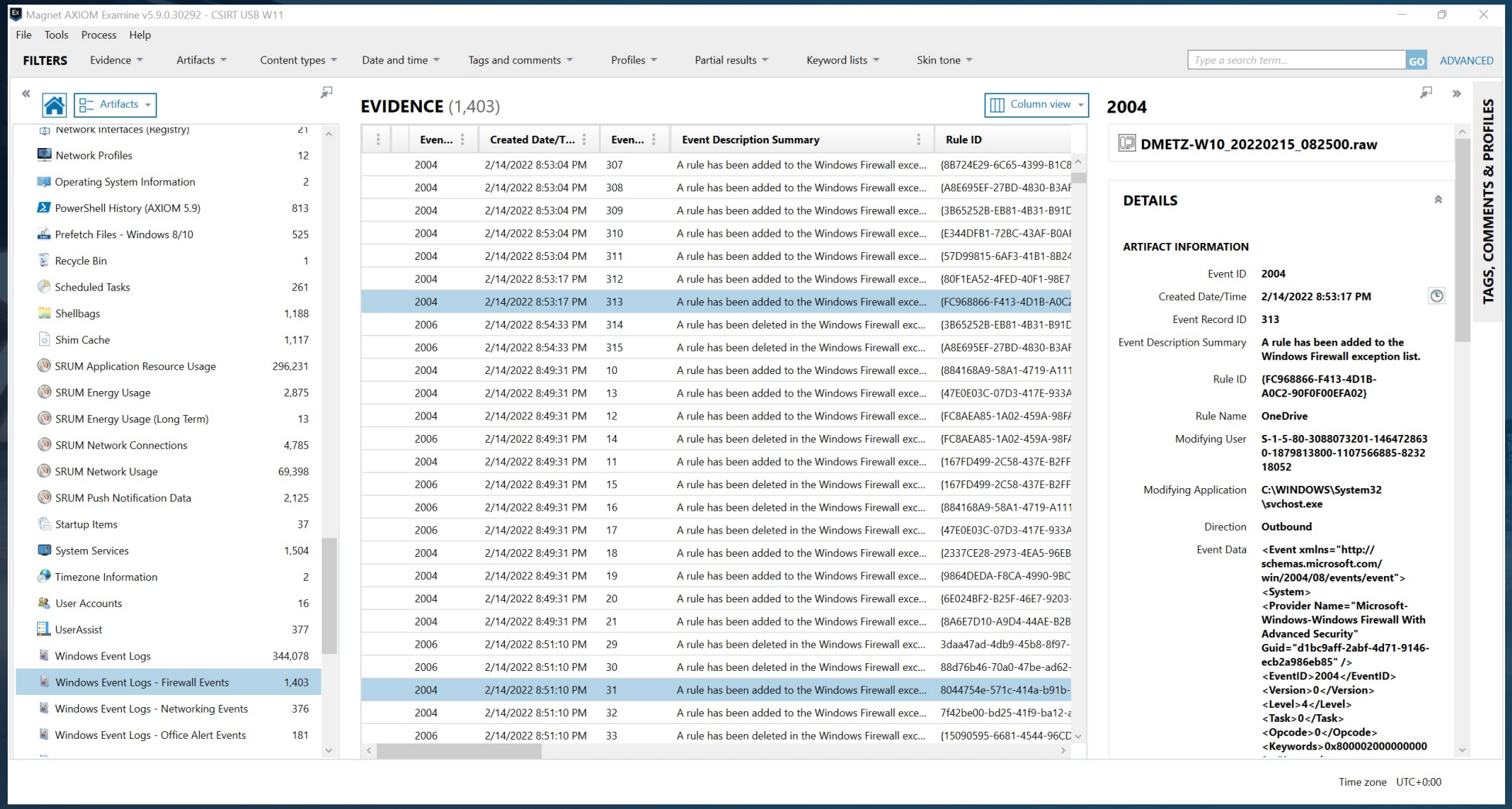


PowerShell History



MAGNET FORENSICS — TECHNO SECURITY 2022

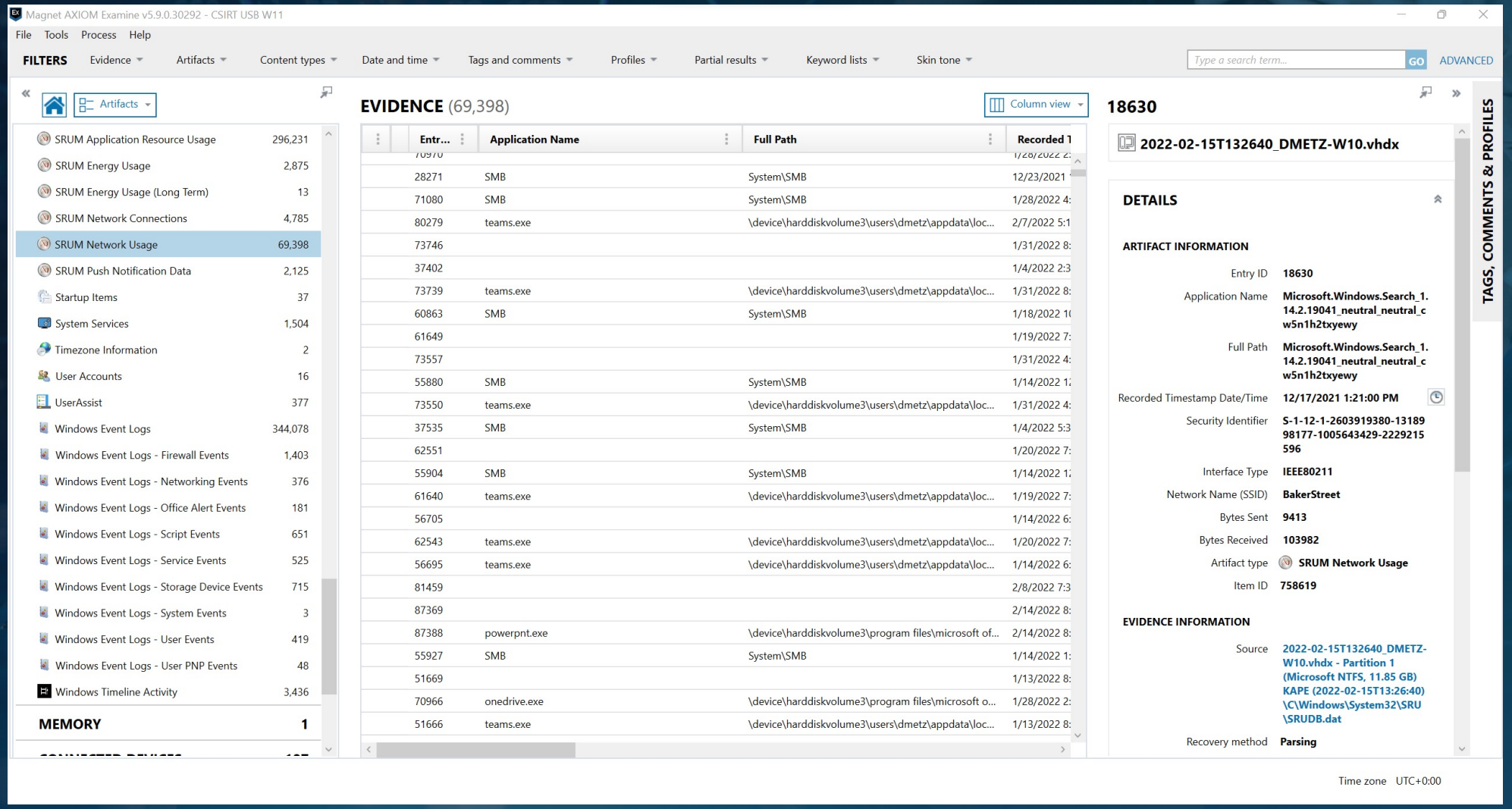
Firewall Events



MAGNET FORENSICS — TECHNO SECURITY 2022

magnetforensics.com

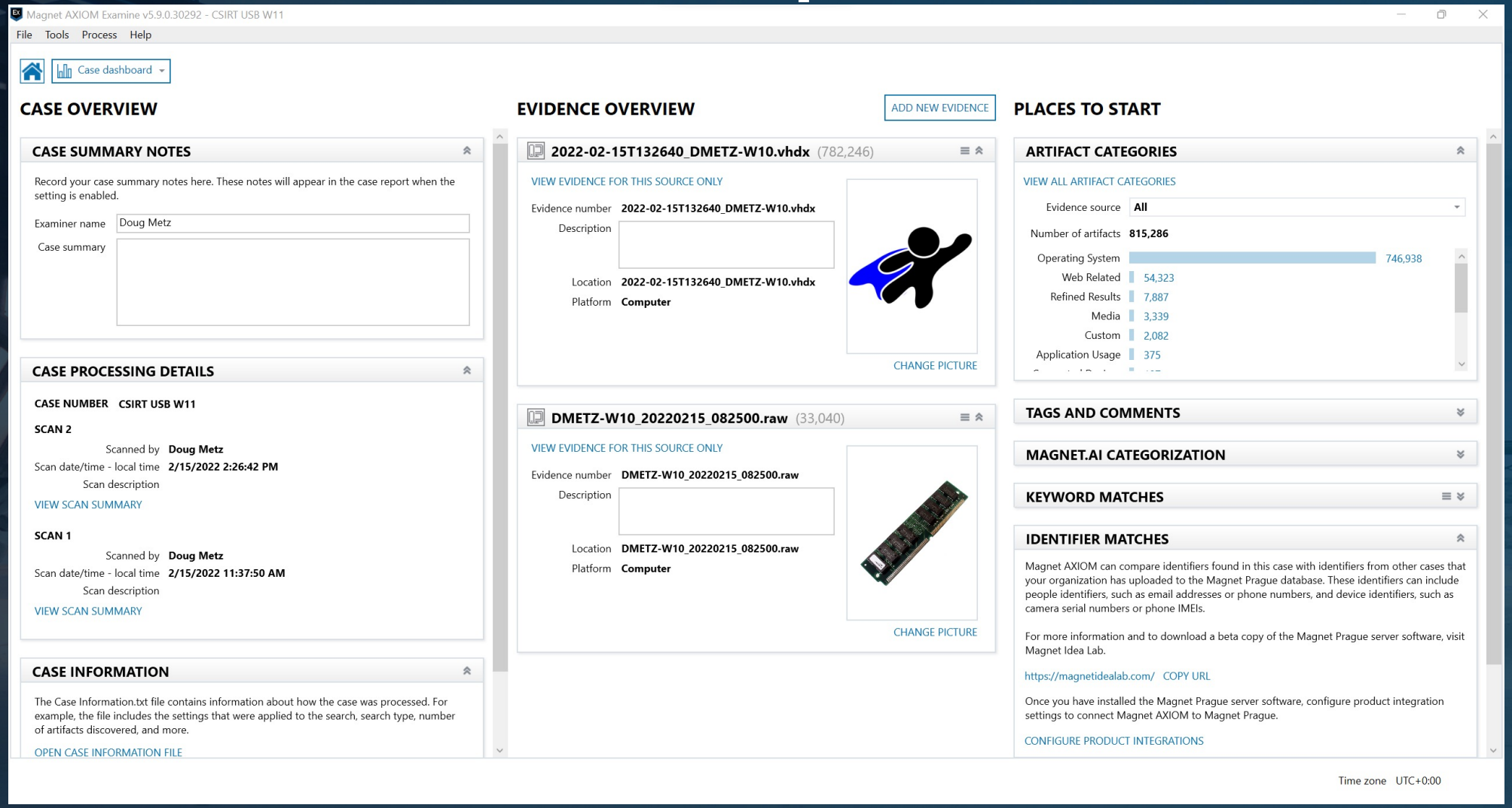
System Resource Usage Monitor (SRUM)



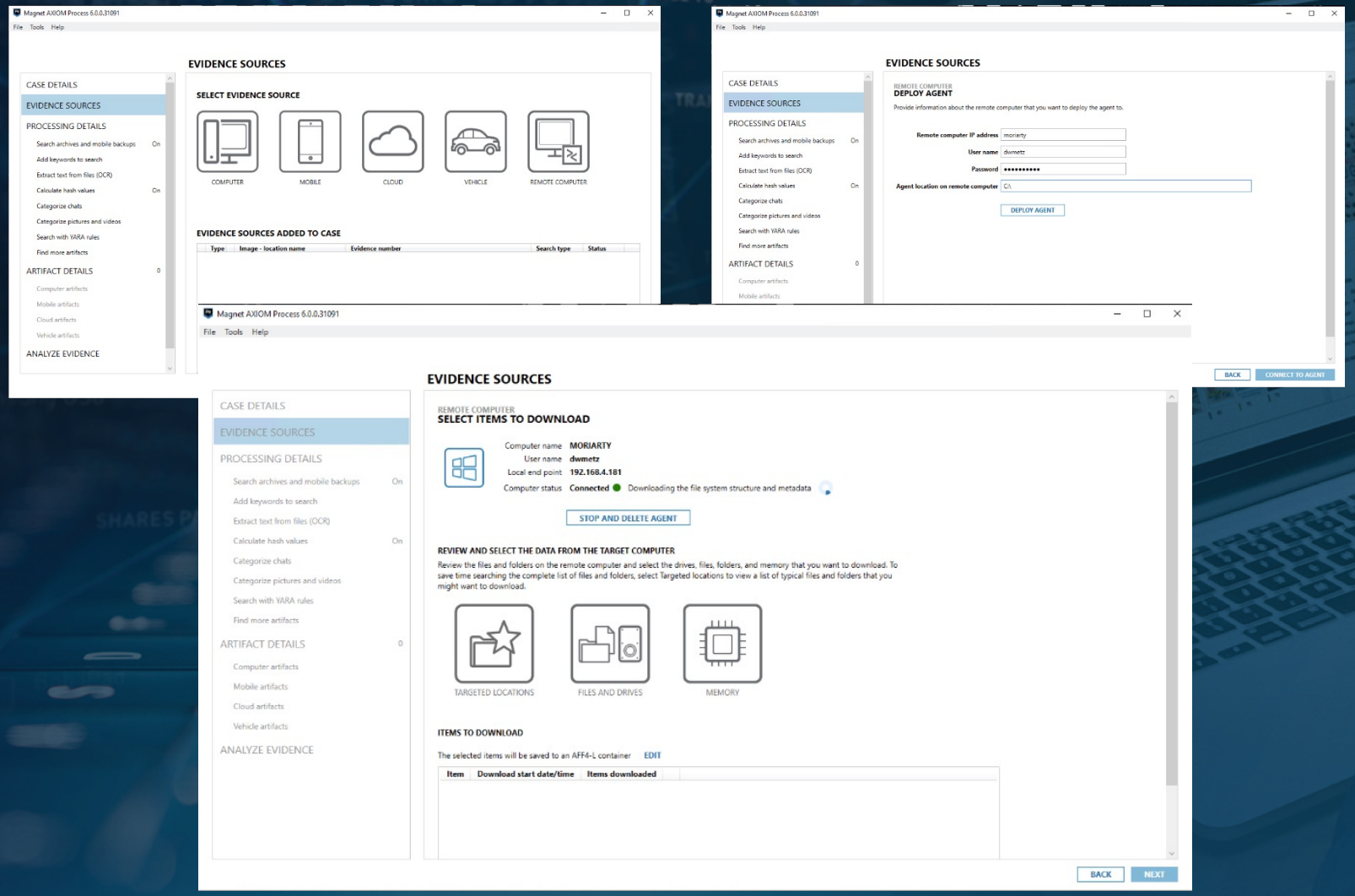
MAGNET FORENSICS — TECHNO SECURITY 2022

magnetforensics.com

Offline Collections Imported



Collecting more with AXIOM Cyber



MAGNET FORENSICS — TECHNO SECURITY 2022

magnetforensics.com

Thank You

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

@dwmetz

doug.metz@magnetforensics.com

https://bakerstreetforensics.com