Magnet2Go

Building a ‘Windows to Go’ Drive to Support Live and Offline Collections

Doug Metz, Security Forensics Consultant
Magnet Forensics

Who Am I

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


Security Forensics 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

Blog:     https://bakerstreetforensics.com
GitHub:   https://github.com/dwmetz

Mastodon: https://infosec.exchange/@dwmetz
LinkedIn: https://www.linkedin.com/in/dwmetz/
Twitter:  @dwmetz
```

SEEK JUSTICE. PROTECT THE INNOCENT.

BAKER STREET FORENSICS

D . F . I . R .

WHERE IRREGULARS ARE PART OF THE GAME

HTCIA

MAGNET FORENSICS®

magnetforensics.com

Objective

- A bootable Windows to Go drive that can boot and run **OUTRIDER** and **ACQUIRE** in dead-disk situations

- Includes syntax to mount drive(s) to acquire in **Read-Only** mode

- By incorporating other **Live Response** tools (RAM capture, EDD, Process Capture etc. on same drive) – you're ready for [nearly] any (collection) situation

Requirements

High capacity/speed **USB drive***

Rufus (open-source USB tool)
https://rufus.ie/en/

A **Windows 10** ISO file**

* Tested on:
    Samsung T5 1TB SSD
    Samsung T7 1TB SSD
    500GB NVME M.2 in enclosure

** If you don't have one, this can help:
https://www.microsoft.com/en-ca/software-download/windows10)

Rufus

Launch Rufus and set the options as indicated below.

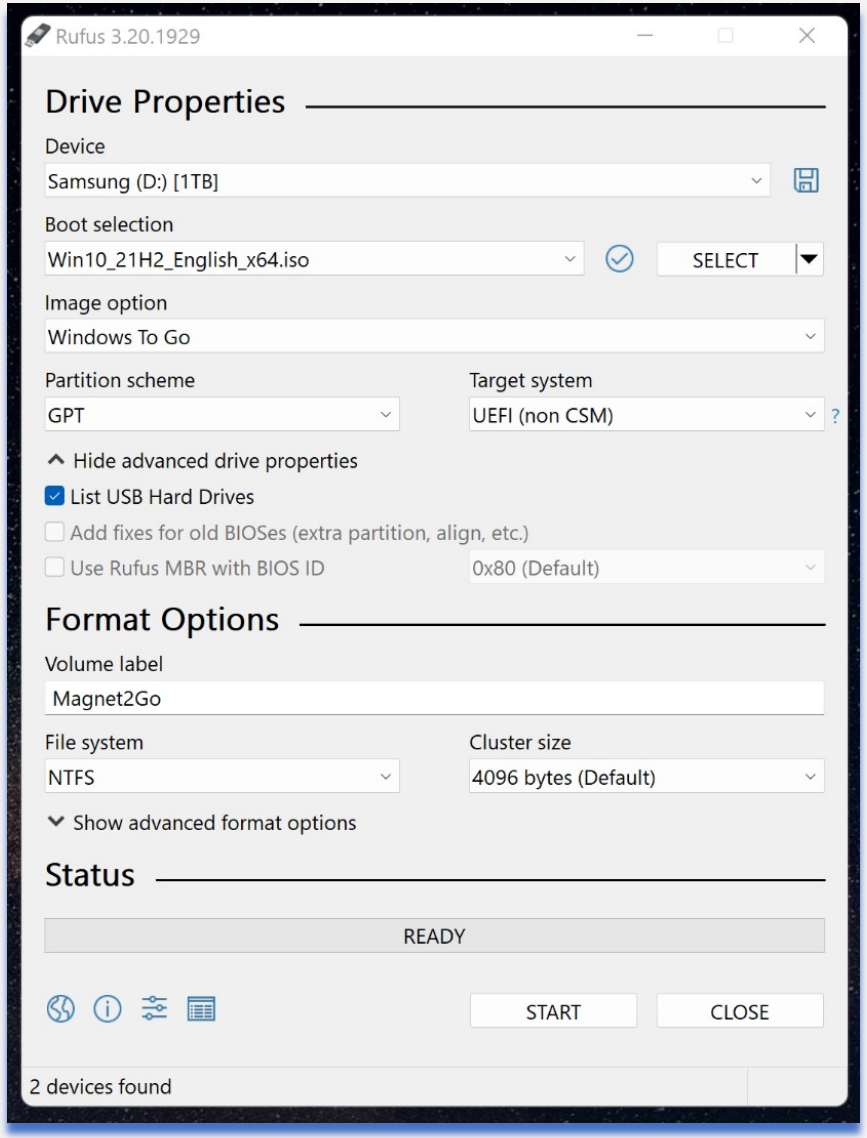
- **Device** The USB drive you want to use for Magnet2Go
- **Boot selection** Browse to and select the Window .iso file
- **Image option** Select **Windows to Go**

Note: you may need to select **"List USB Hard Drives"** in order to see the external drive as an option under **Device**.

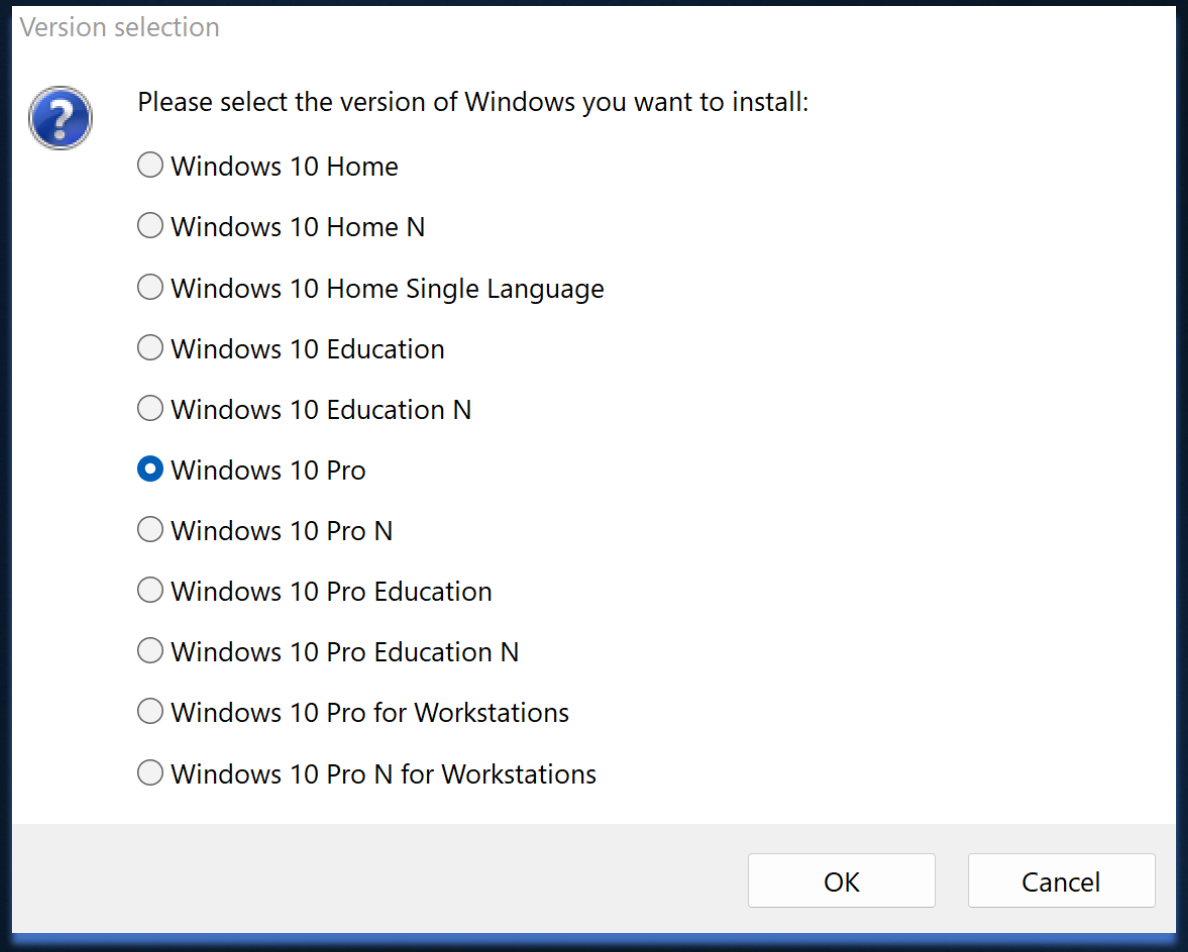
- **Volume label** **Magnet2Go**

Triple check your settings and then press Start.

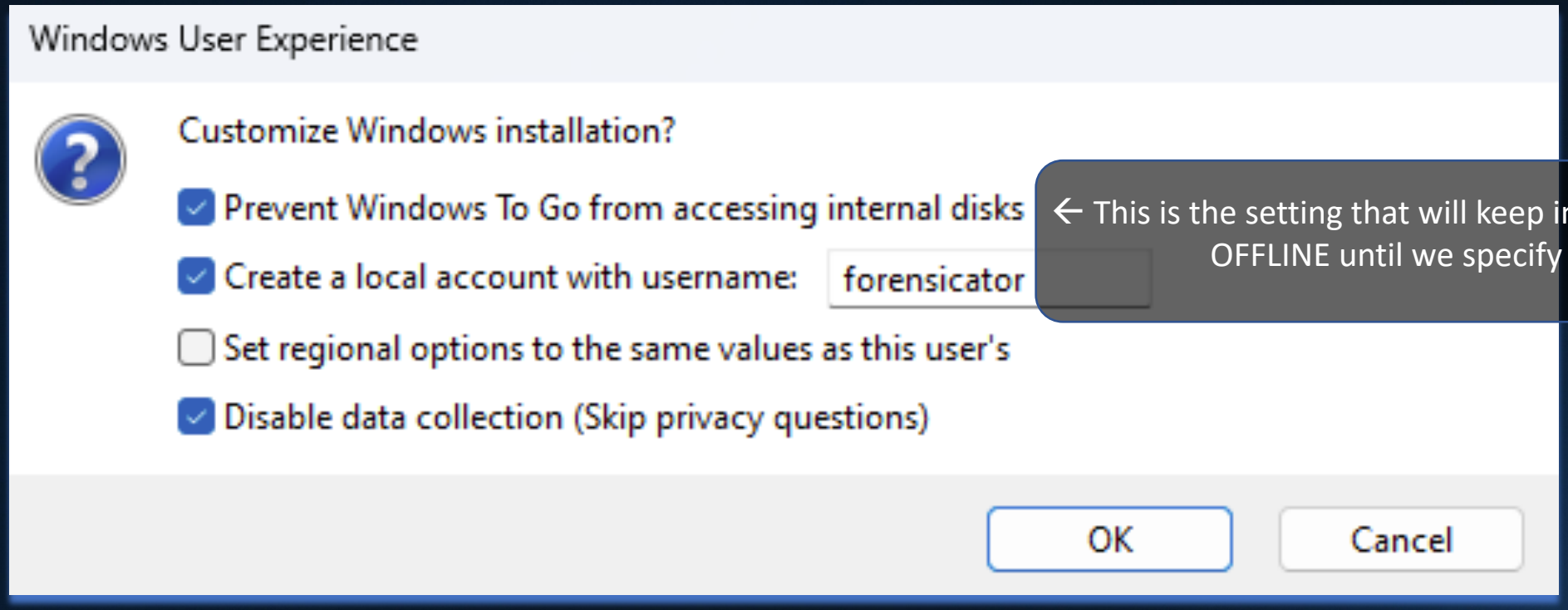
*Changing certain options like the **Image option** can reset the **Volume label** information back to default.*



Windows Version

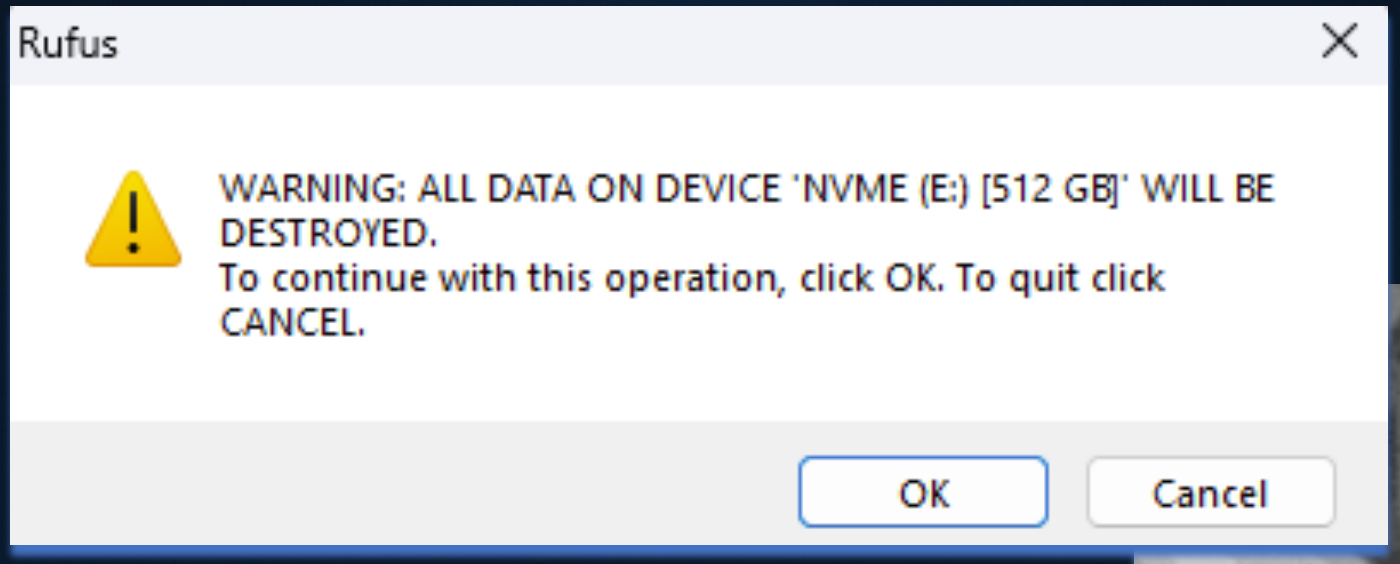


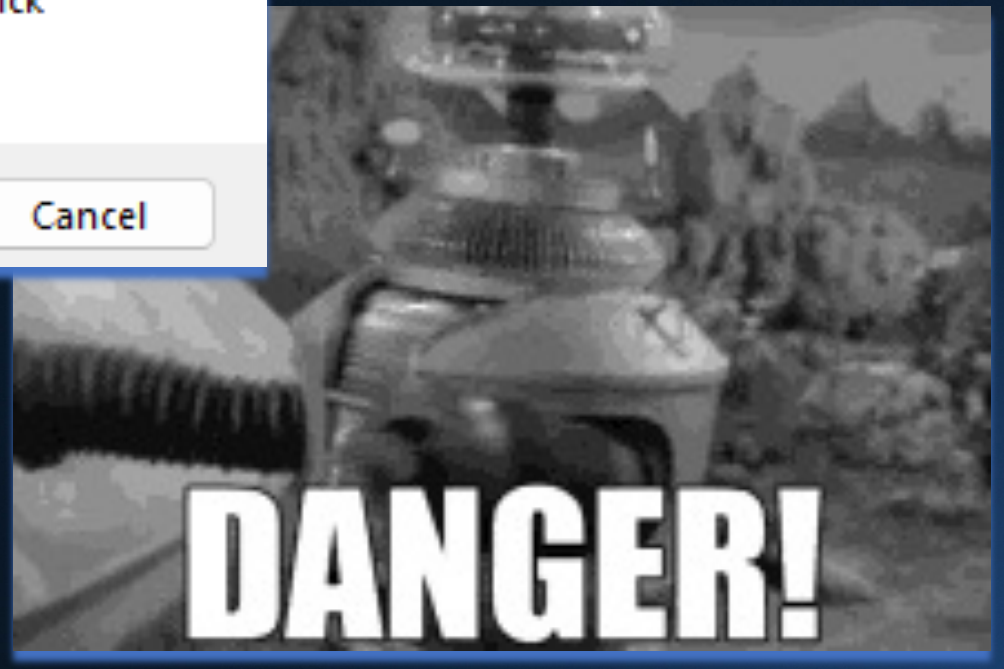
WUX



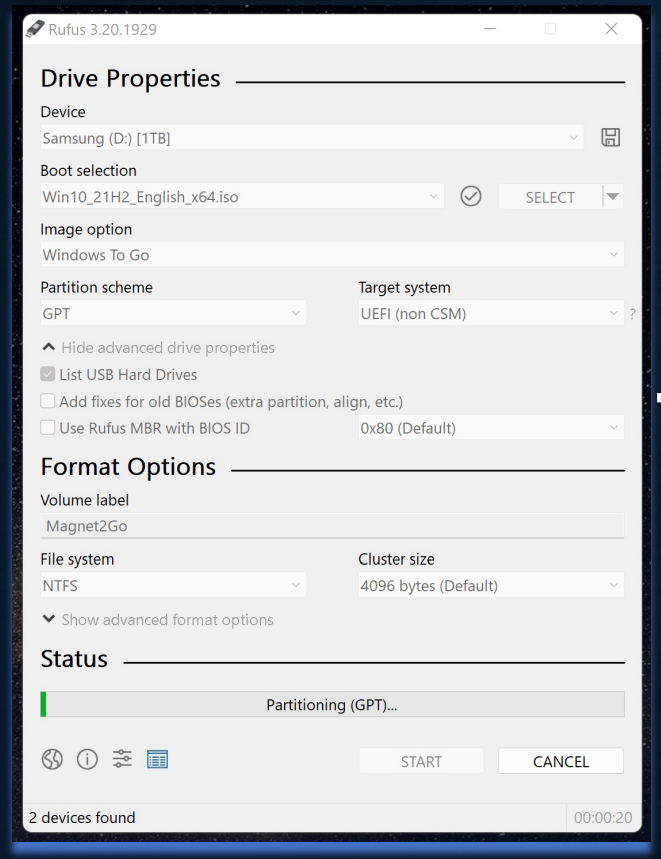
← This is the setting that will keep internal drives OFFLINE until we specify otherwise

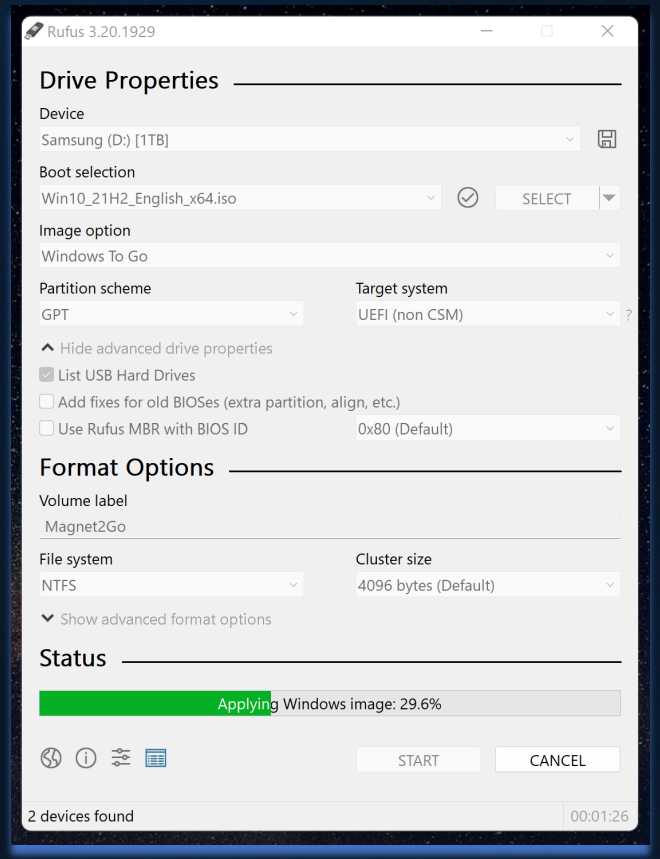
Danger, Will Robinson

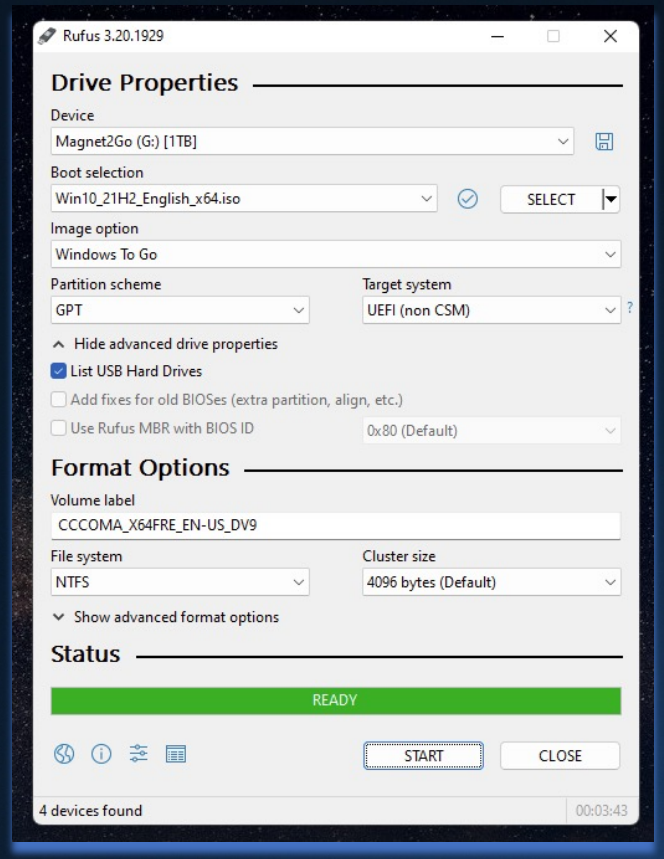




Partitioning… Applying Image… Complete.



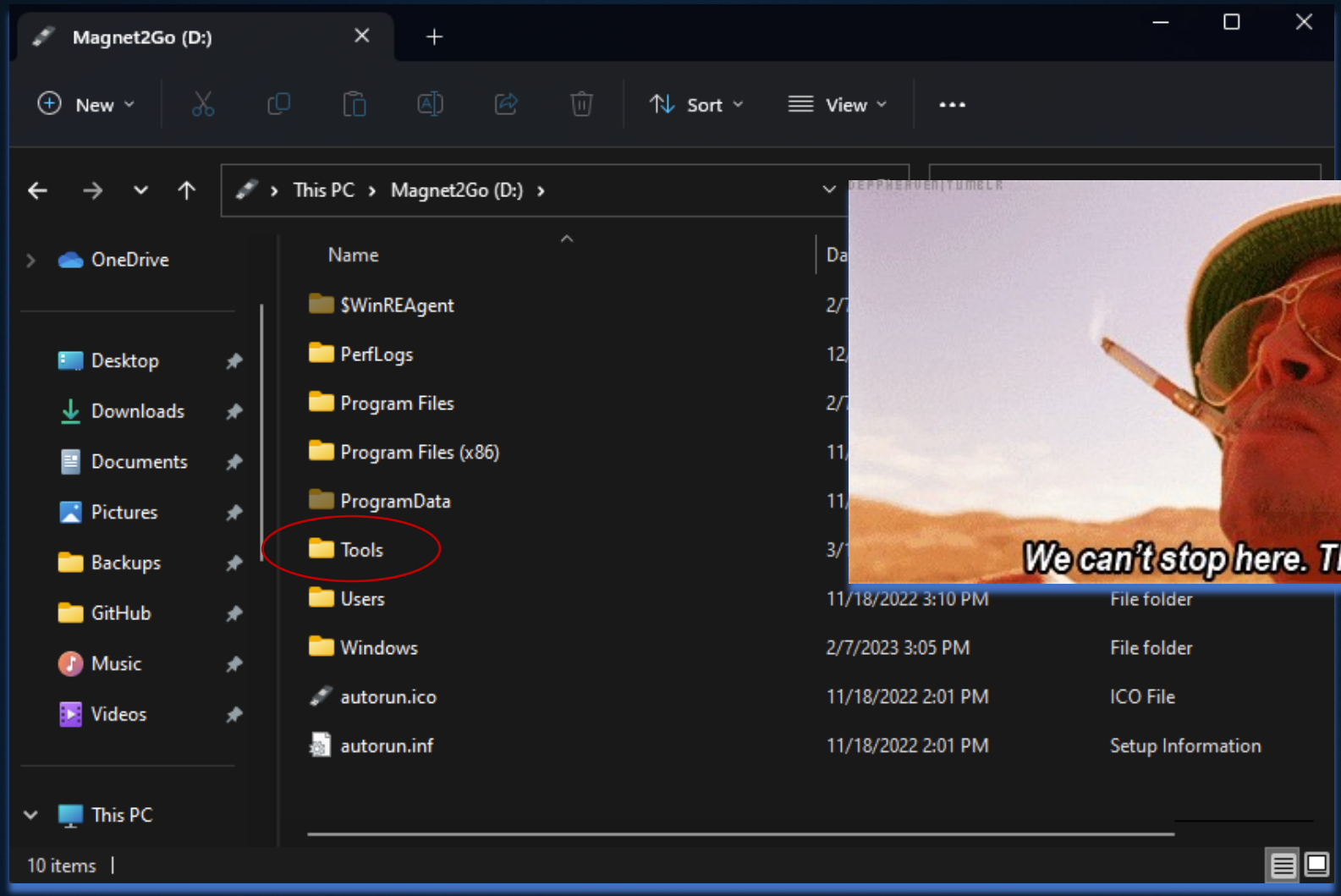




SEEK JUSTICE. PROTECT THE INNOCENT.

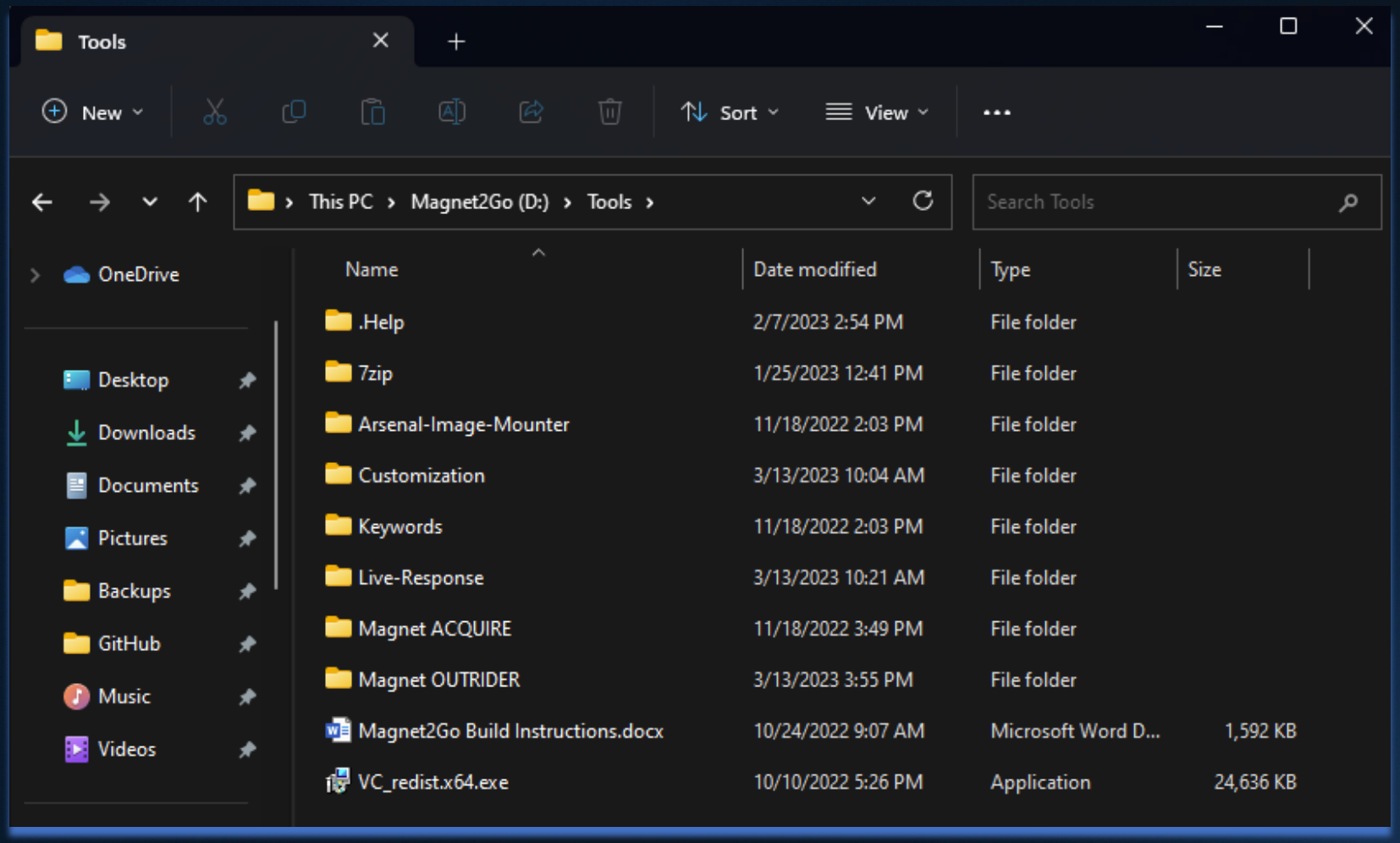
magnetforensics.com

Before You Go On…

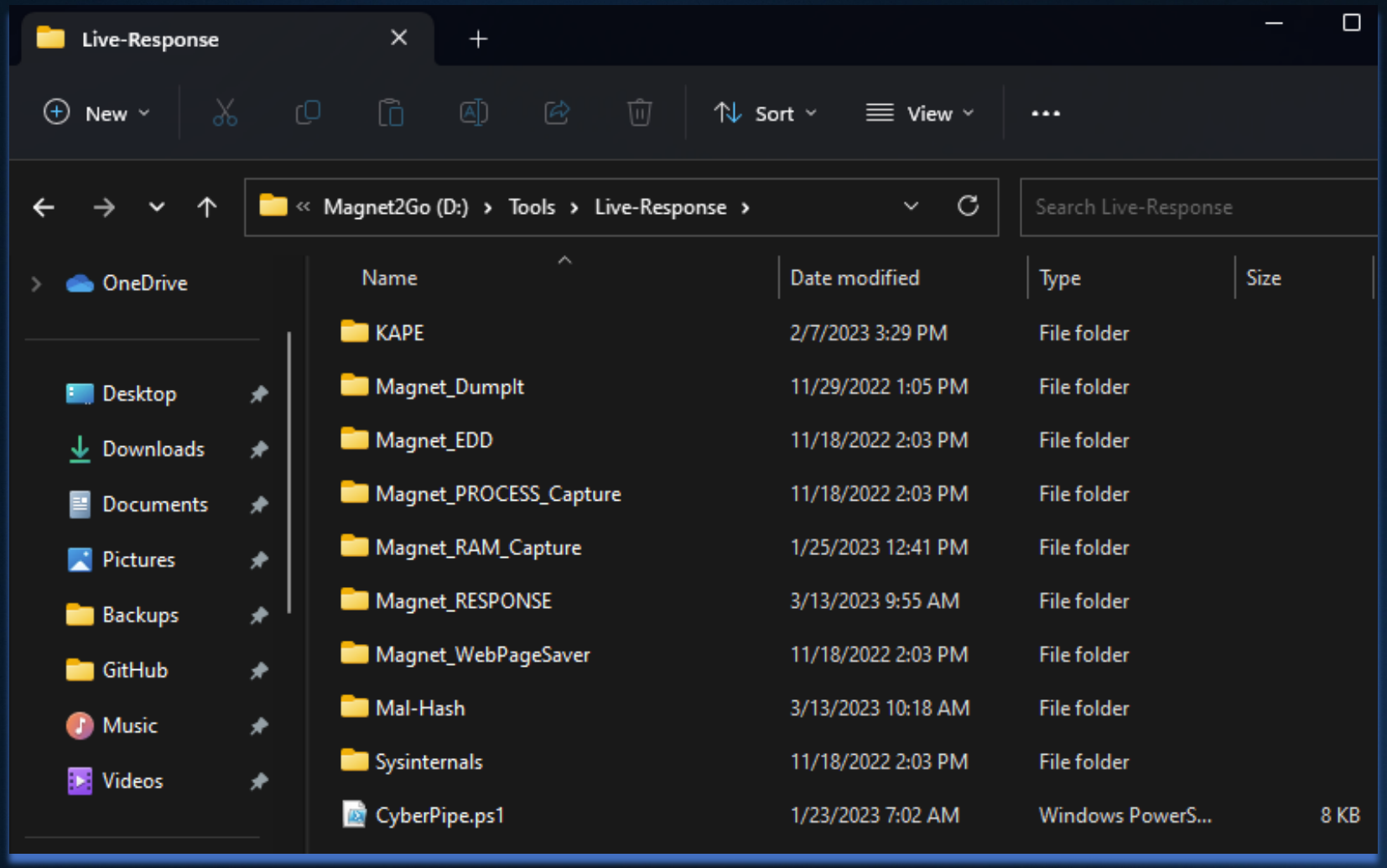


SEEK JUSTICE. PROTECT THE INNOCENT.

Tools Directory



Live Response Tools



SEEK JUSTICE. PROTECT THE INNOCENT.

Suggested Tools

- Magnet OUTRIDER – Free trial: https://www.magnetforensics.com/products/magnet-outrider

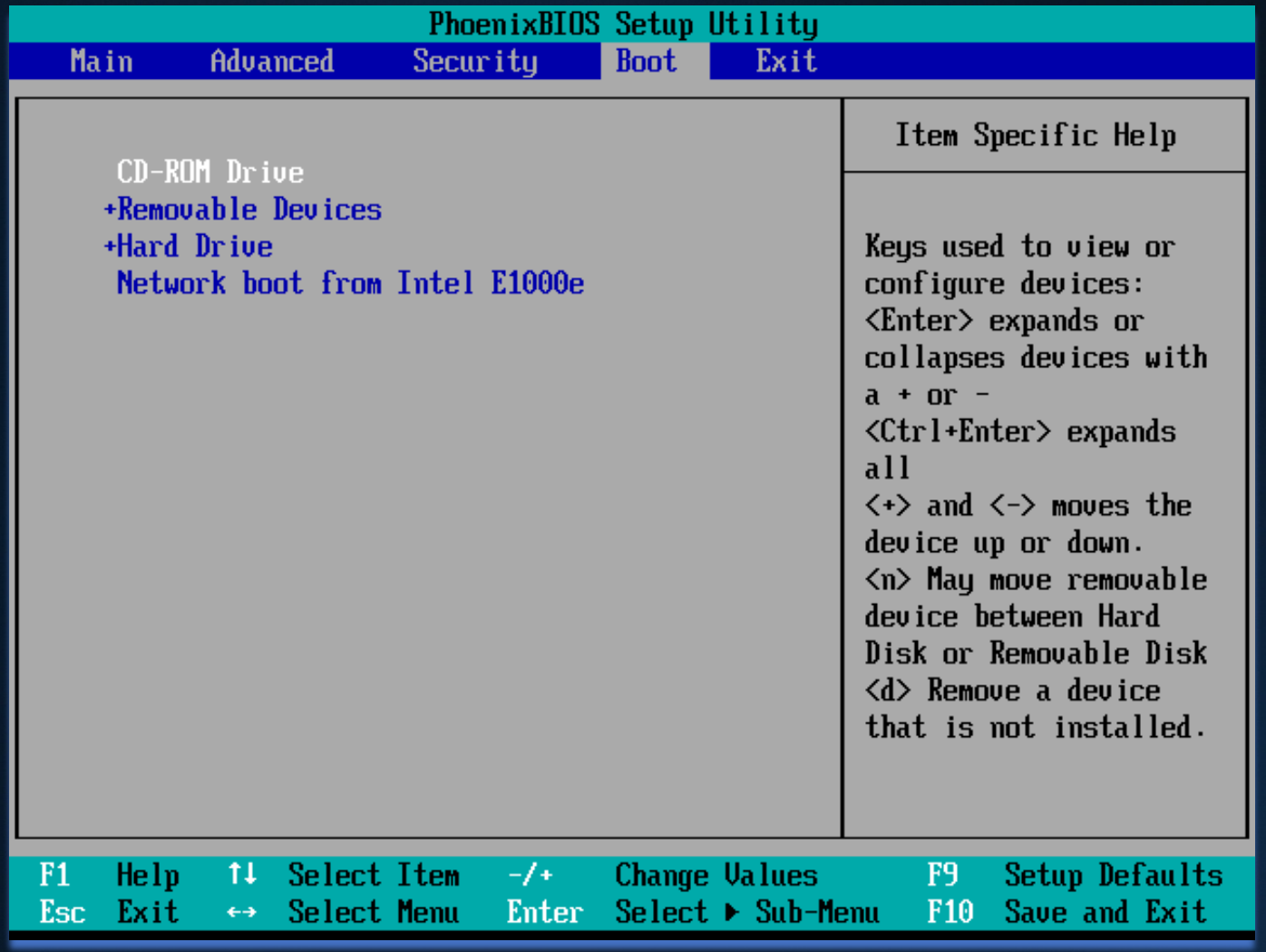
  Once you've set up OUTRIDER on another USB device, you can copy the USB contents to the Tools folder
- Magnet ACQUIRE – Installer for the latest version of Magnet ACQUIRE. https://support.magnetforensics.com/s/free-tools
- Latest version of Microsoft Visual C++ Redistributable (x64)

  This is a dependency for a number or the Magnet Forensics tools.
- Arsenal Image Mounter – (copied from existing installation); https://arsenalrecon.com/downloads/

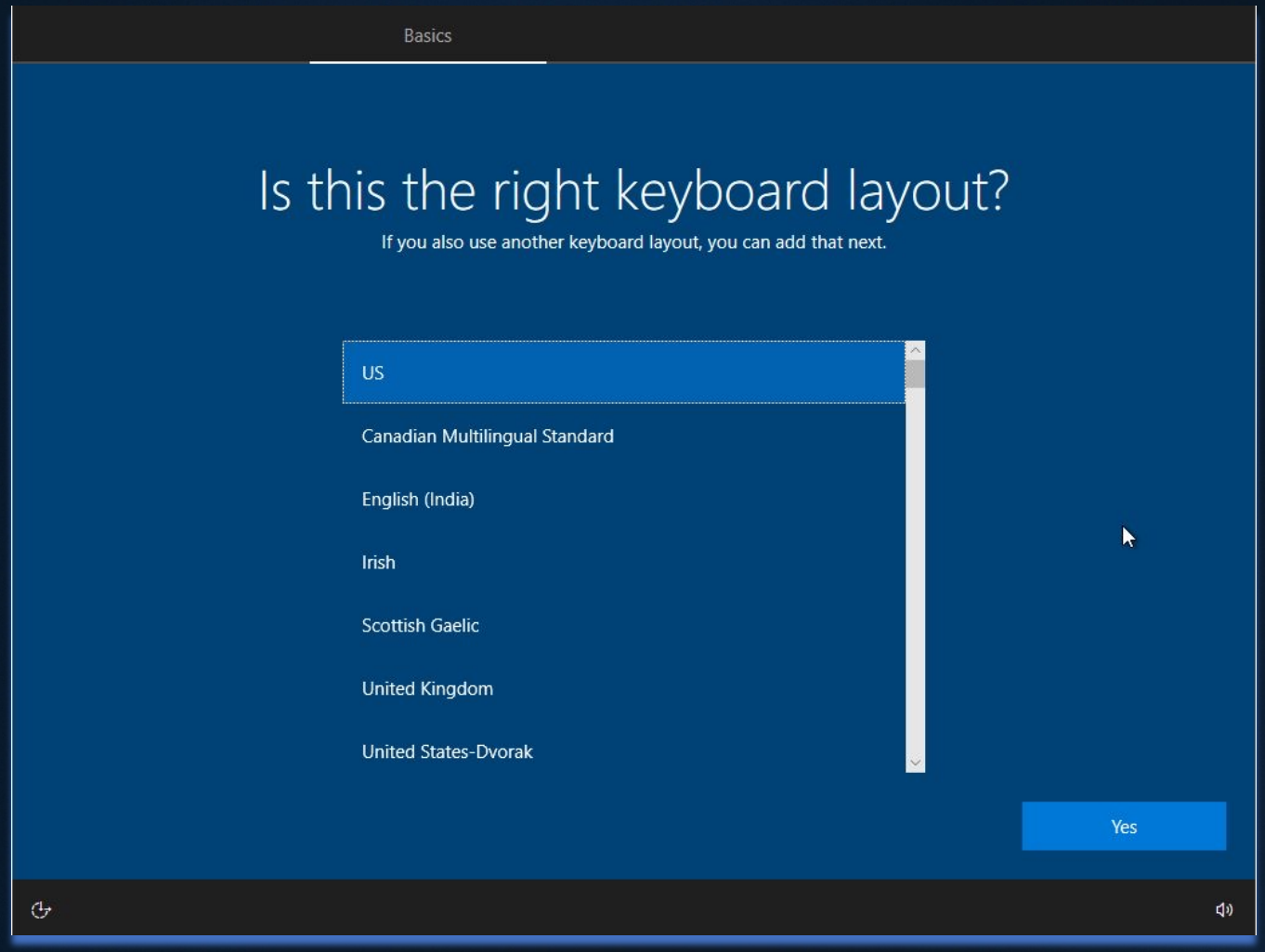
Live Response

- Magnet RAM Capture - https://support.magnetforensics.com/s/free-tools
- Magnet DumpIt for Windows - https://www.magnetforensics.com/blog/how-to-get-started-with-comae/
- Magnet Encrypted Disk Detector - https://support.magnetforensics.com/s/free-tools
- Magnet Process Capture - https://support.magnetforensics.com/s/free-tools
- Magnet Web Page Saver - https://support.magnetforensics.com/s/free-tools
- Magnet RESPONSE - https://support.magnetforensics.com/s/free-tools
- CyberPipe - https://github.com/dwmetz/CyberPipe

Boot from Magnet2Go



First Boot (Setup)

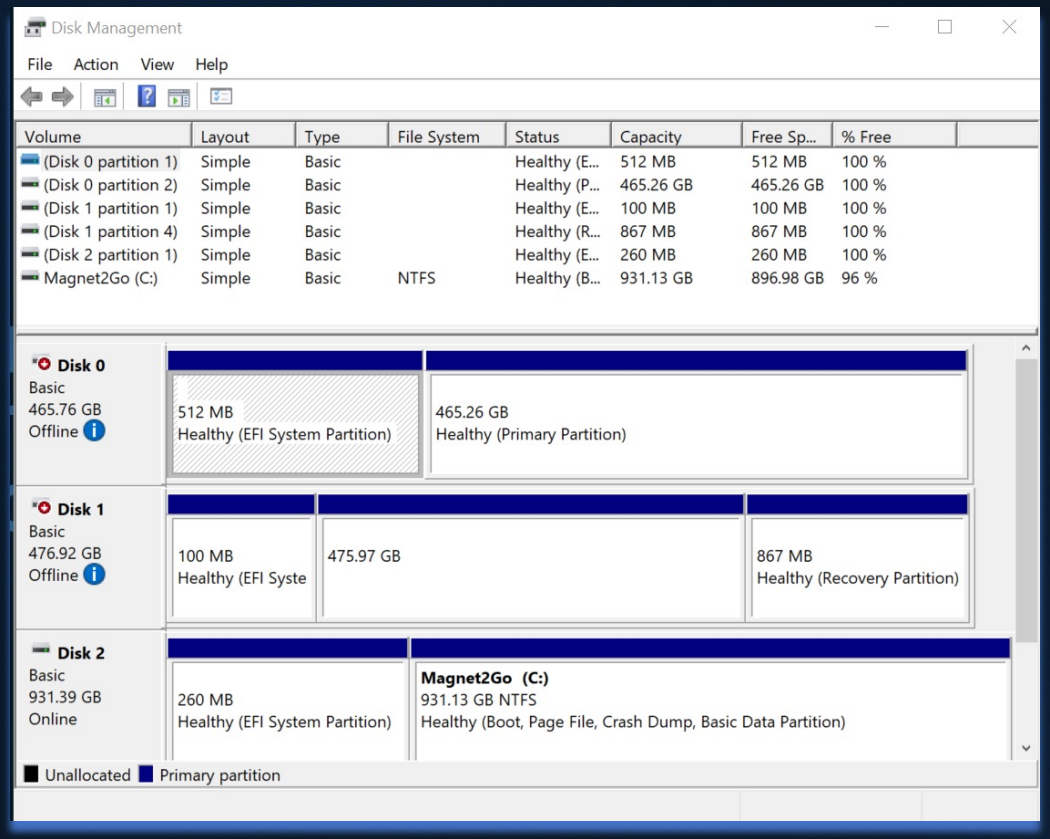


SEEK JUSTICE. PROTECT THE INNOCENT.

First Boot (Windows Configuration)

1. Run the ***VC-redistributable*** first
2. Run the installer for **Magnet ACQUIRE**
3. **Install any .NET updates as needed**
4. **Launch Arsenal Image Mounter and enable driver installation**
5. **Run installers for any additional tools**
6. **Customize wallpaper, desktop, dark-mode, etc.**

Safely Accessing the Target Hard Drive(s)



When we boot from Magnet2Go, any other drives attached to the system will be Offline when we boot.

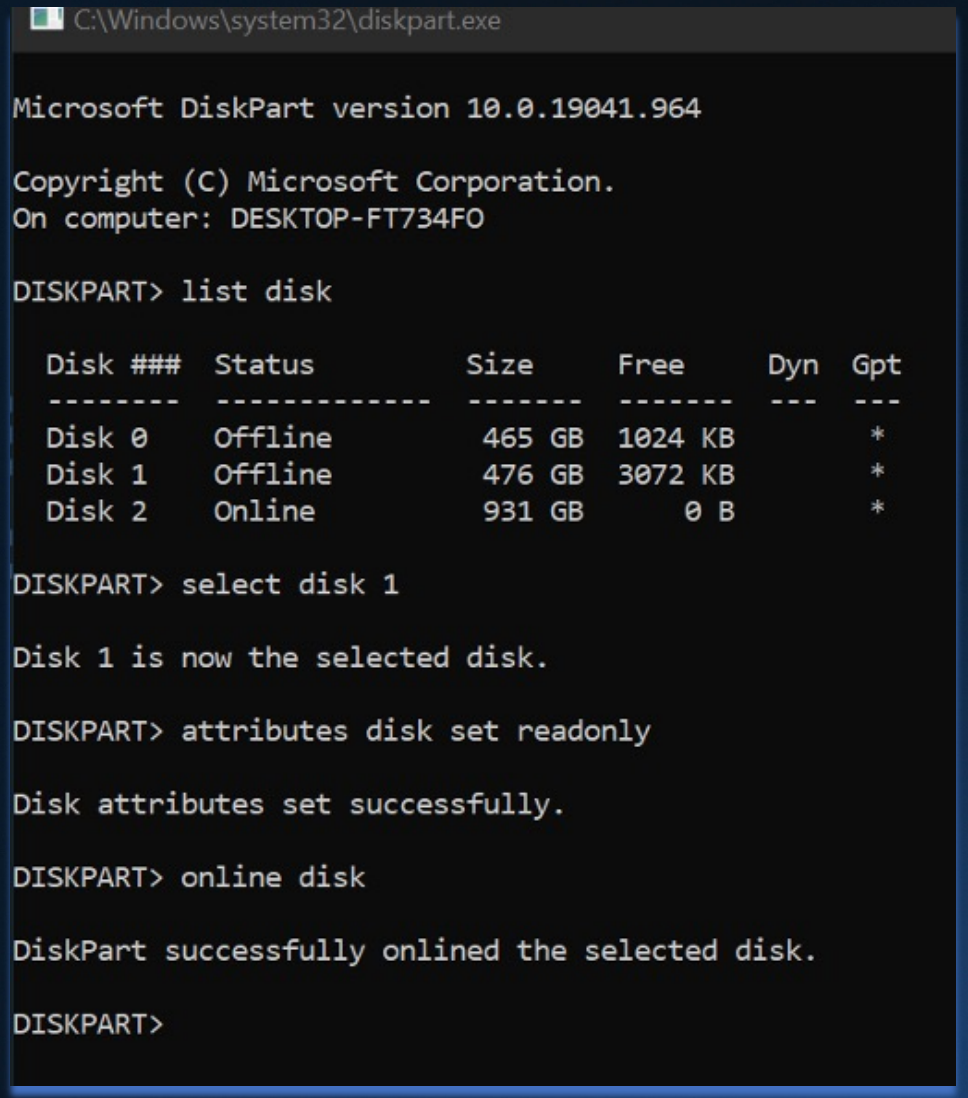
Diskpart Syntax

- **List disk** will list the different disk sources attached to the computer. In this example there are 3 drives present. Disk 0 and Disk 1 are hard disks installed in the target computer. Disk 2 is the USB device we've booted from. In this case the drive I want to be able to collect from is Disk 1.

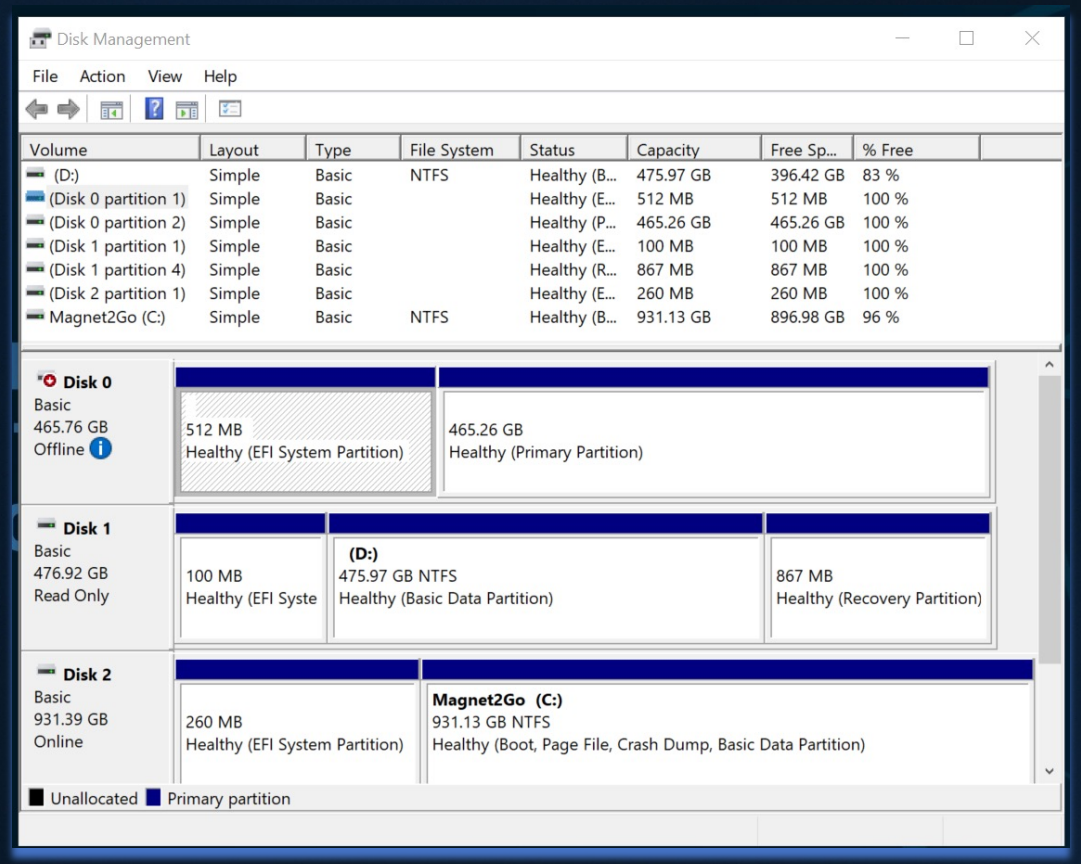
- **Select disk 1** will select the specified disk number.

- Once selected, **attributes disk set readonly**, will ensure that the specified disk cannot be written to once mounted.

- **Online disk** will bring the disk online and make it available to Windows.

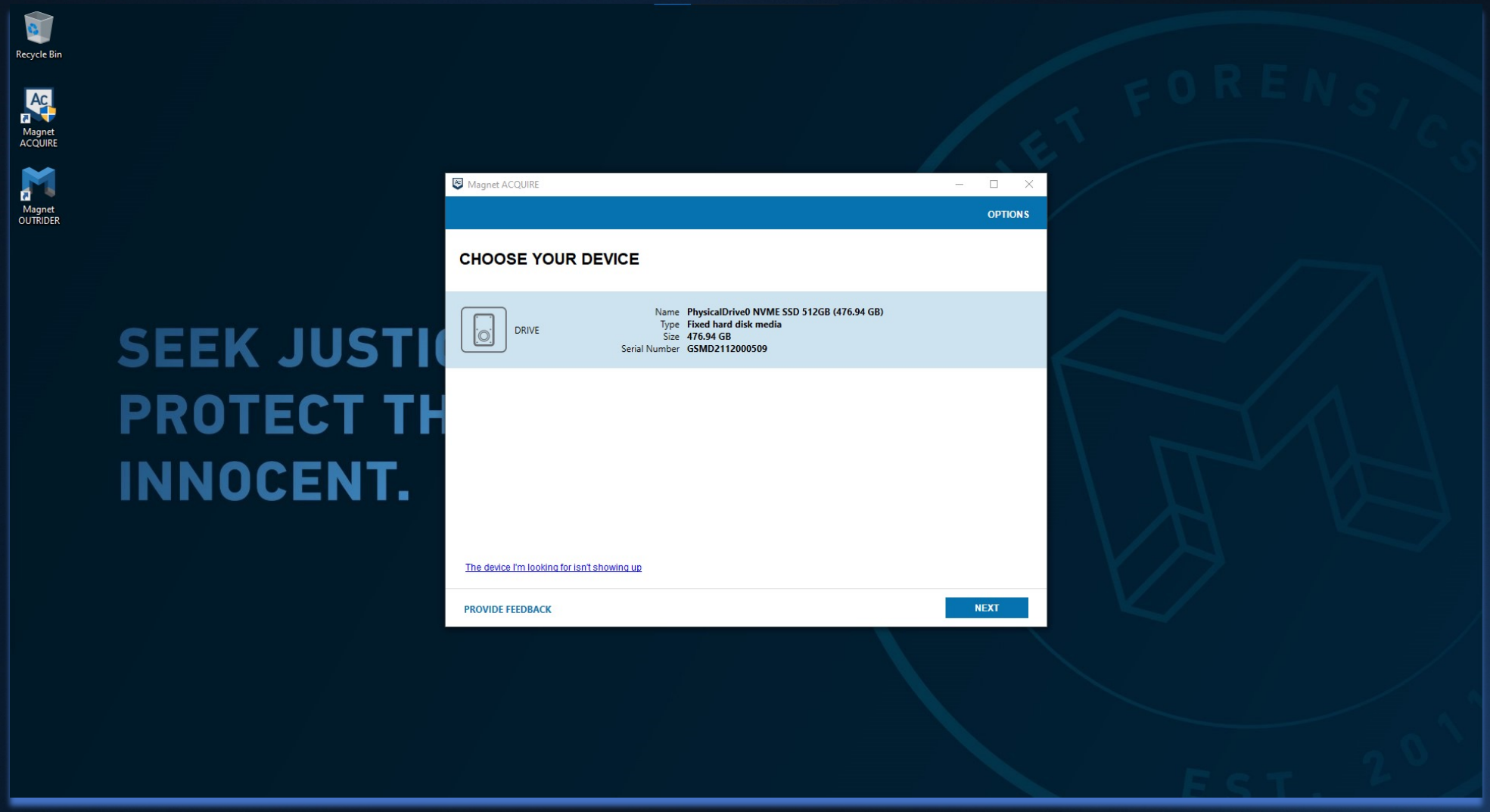


Verify READ-ONLY

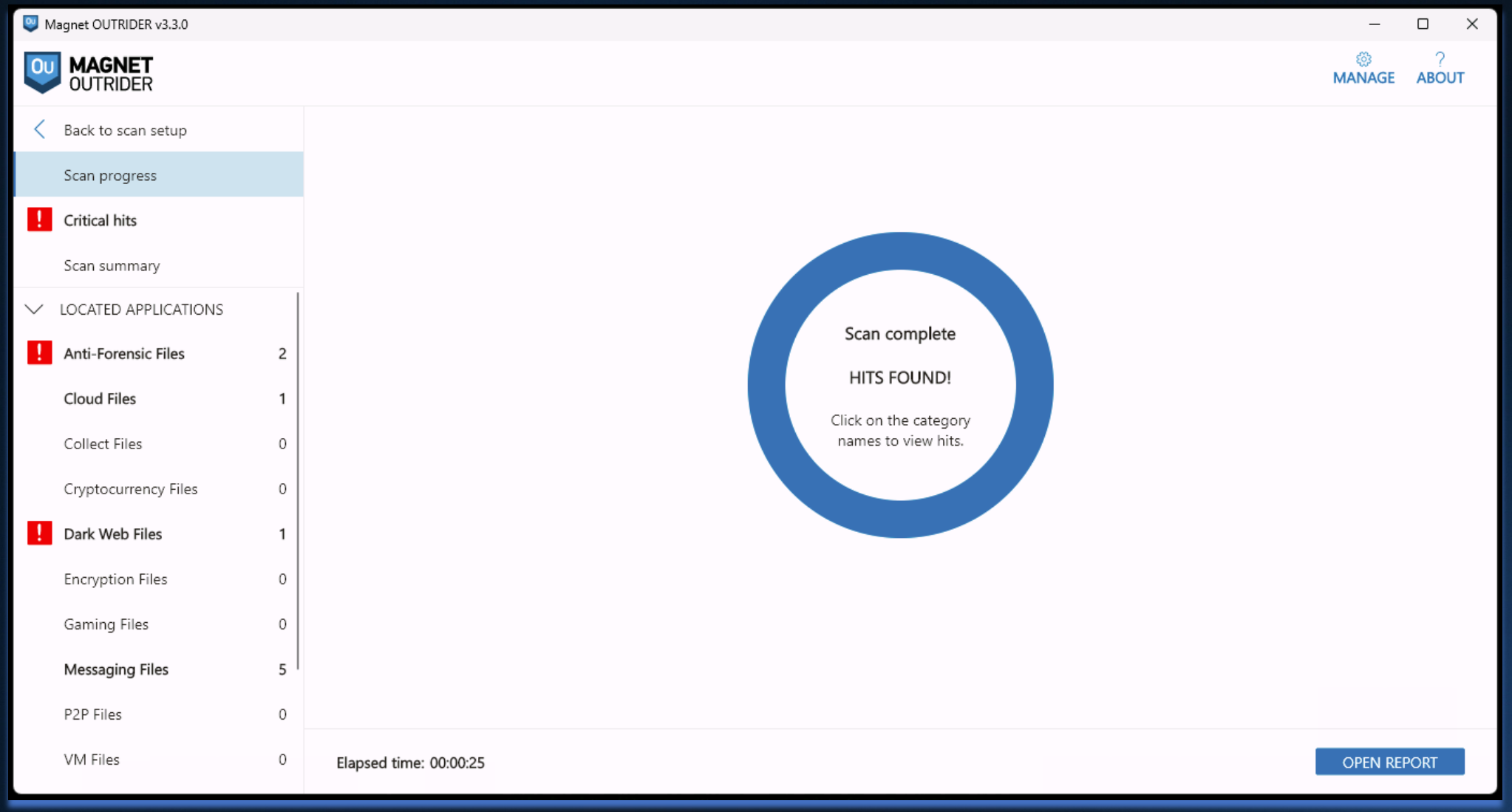


You can verify the status of the disks in Disk Management (diskmgmt.msc)

Disk Acquisition – Magnet ACQUIRE



Triage for Illicit Content – Magnet OUTRIDER



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

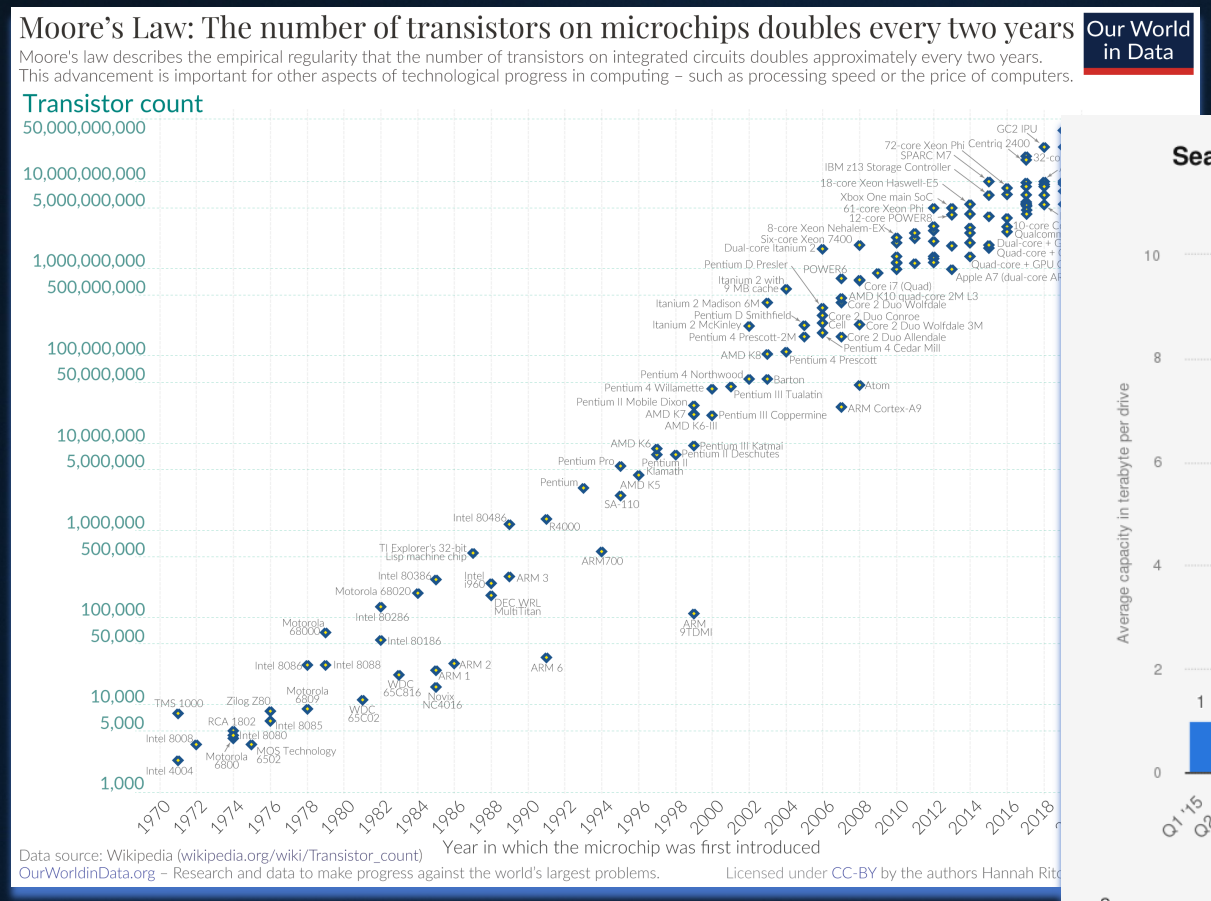
Live Response

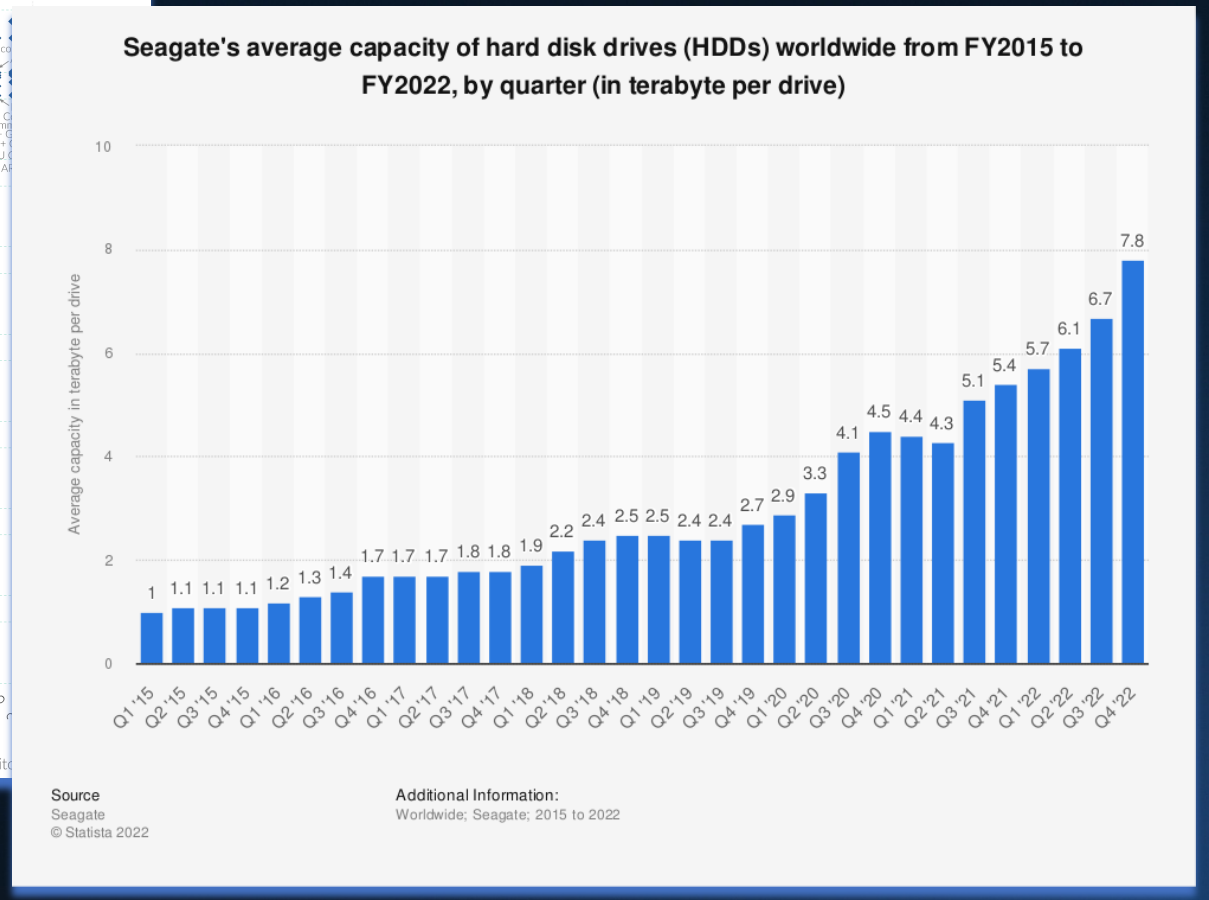
Triage collections for On and Off Network

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

Magnitudes of Data





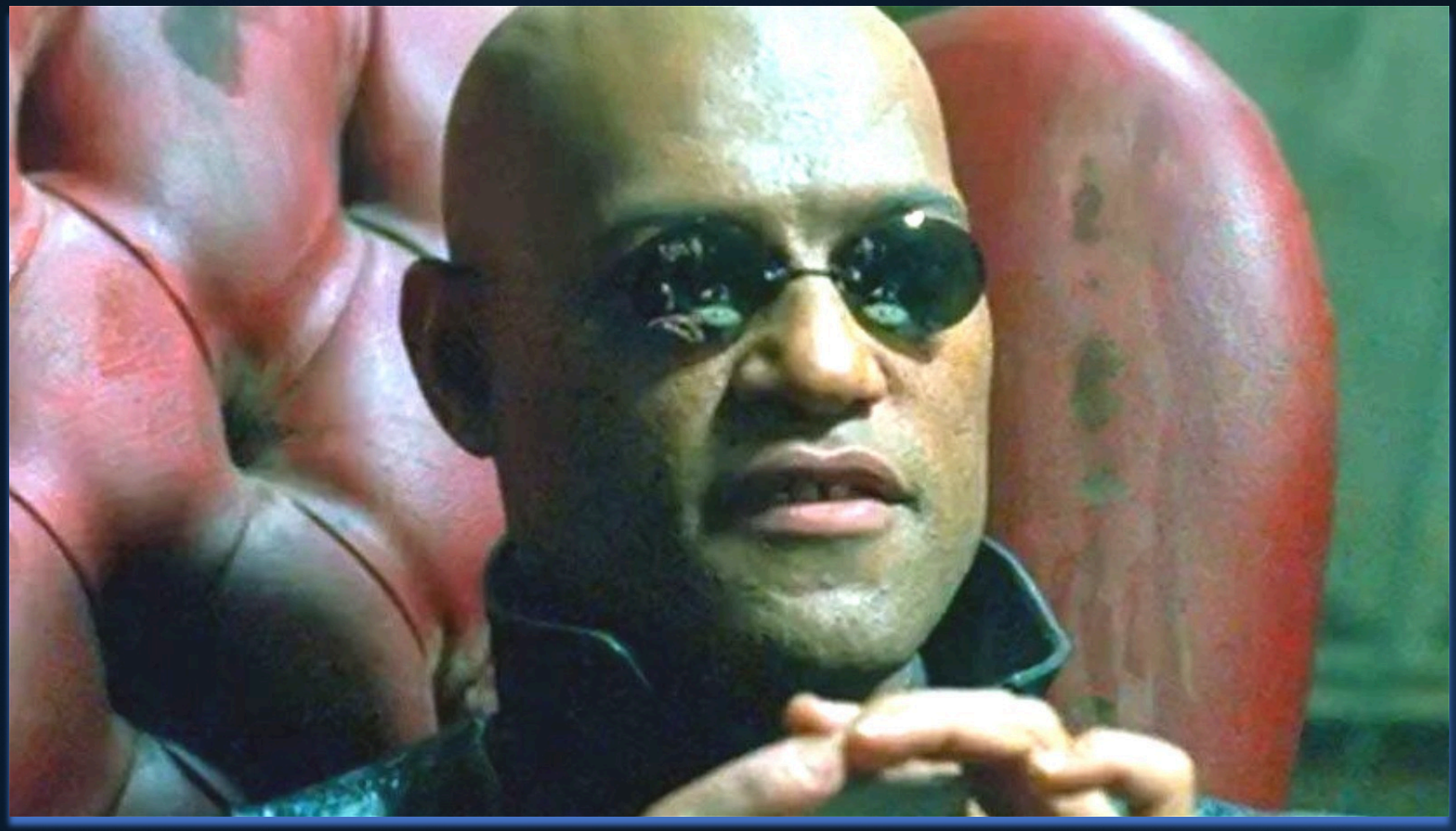
Sources:
https://en.wikipedia.org/wiki/Moore%27s_law#/
https://www.statista.com/statistics/795748/worldwide-seagate-average-hard-disk-drive-capacity/

SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.com

What If I told You

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



triage noun

tri·age trē-ˈäzh ˈtrē-ˌäzh

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

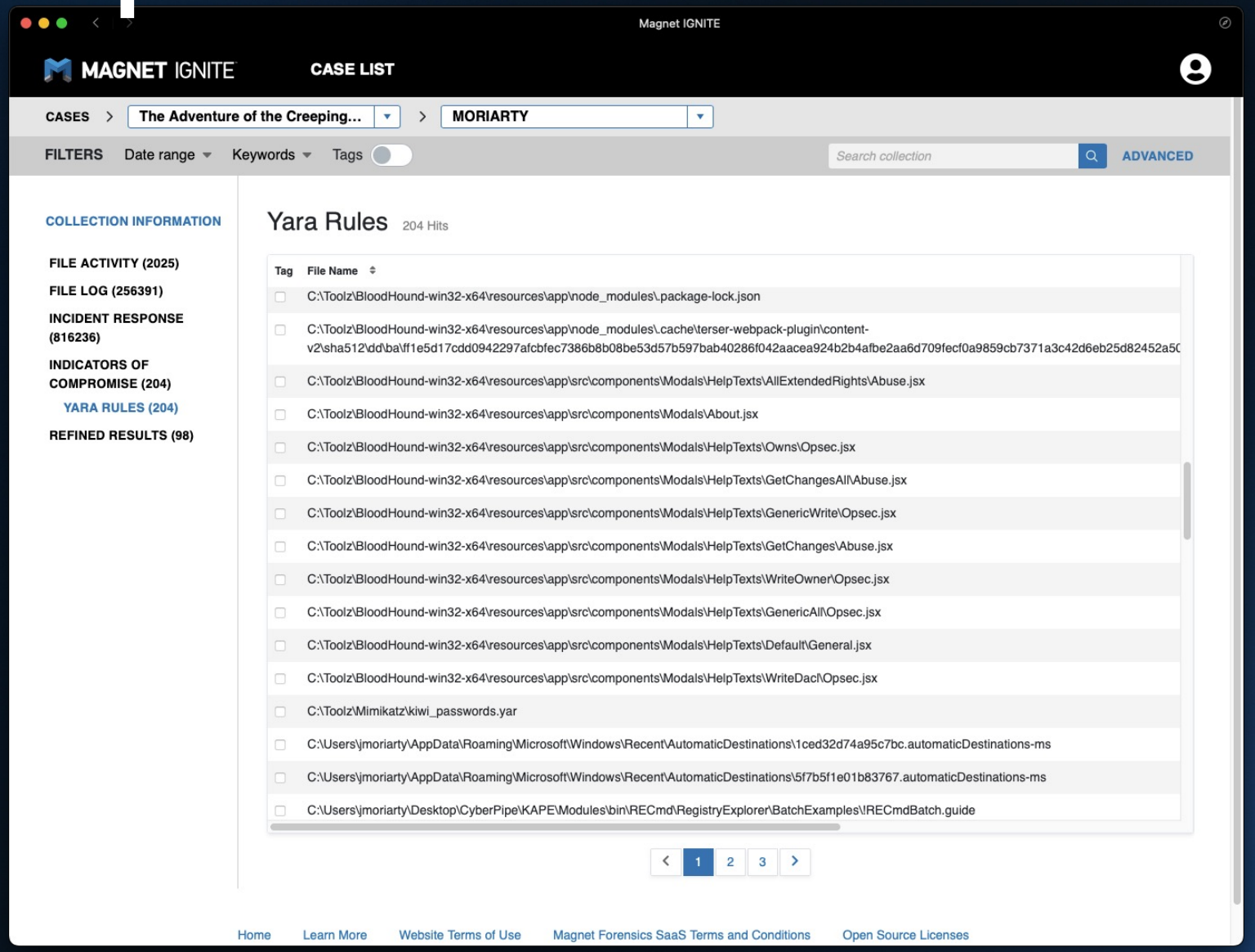
2 : the assigning of priority order to projects on the basis of where funds and other resources can be best used, are most needed, or are most likely to achieve success

triage transitive verb

Source: https://www.merriam-webster.com/dictionary/triage

Online Triage Acquisition

- Magnet IGNITE
- Magnet AXIOM Cyber
- Magnet AUTOMATE Enterprise



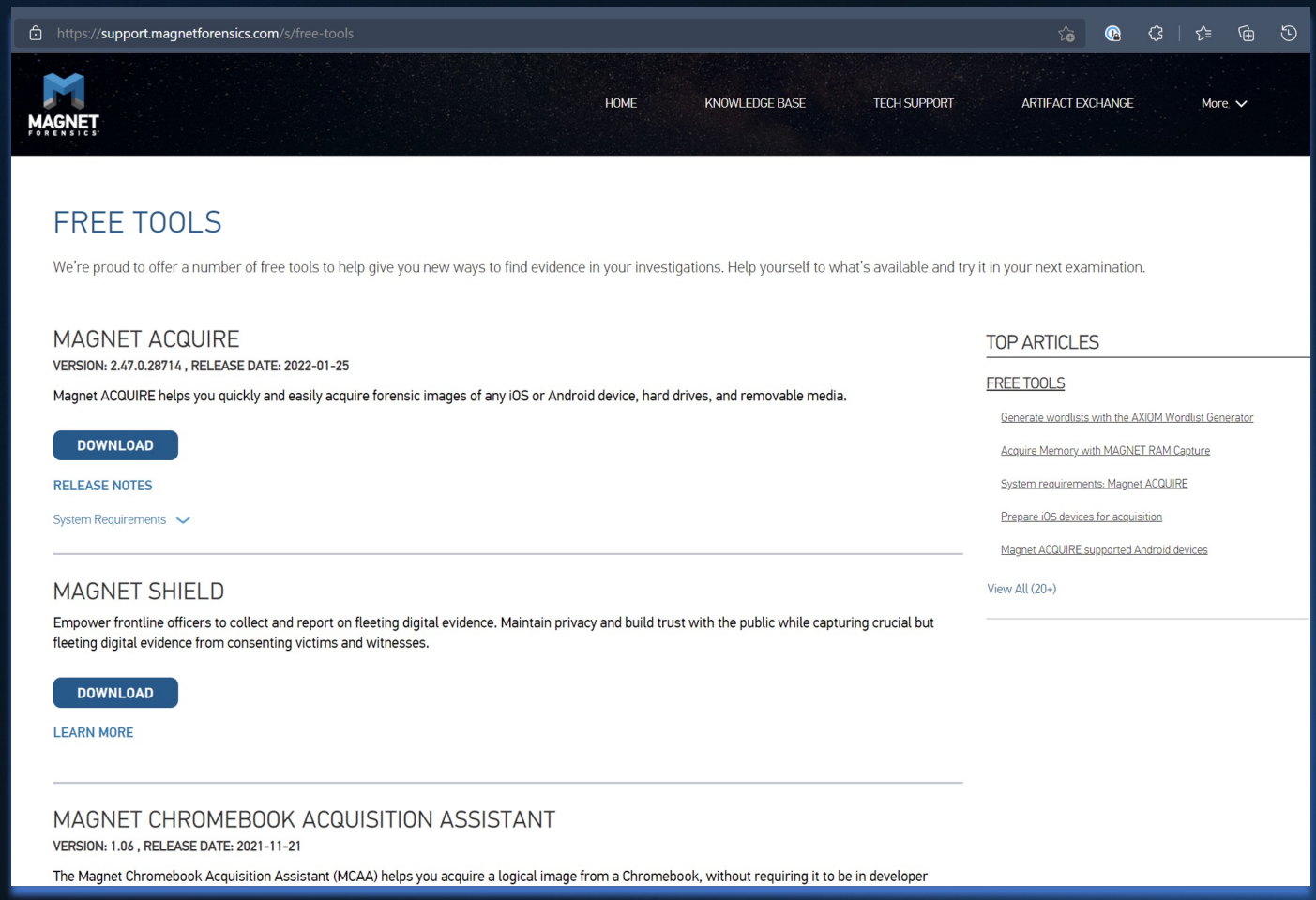
MAGNET FORENSICS®

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet Free Tools

https://www.magnetforensics.com/free-tools/

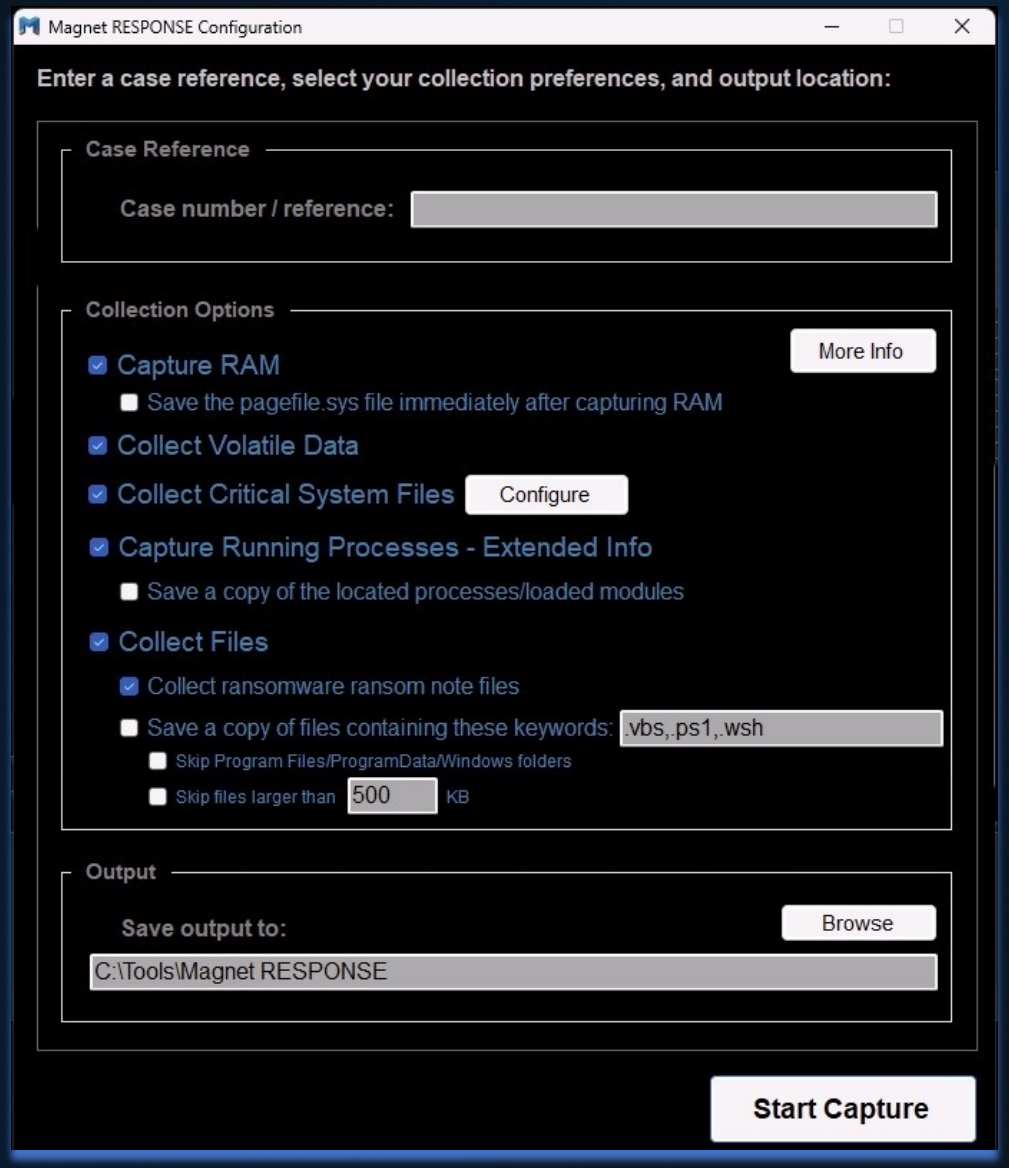
- Magnet RESPONSE
- Magnet ACQUIRE
- Magnet DumpIt for Windows
- Magnet RAM Capture
- *…. (more)*



MAGNET FORENSICS®

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet RESPONSE



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

Minimal to no training is required—it's as simple as entering a case name, selecting the collection options and then "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/

Magnet RESPONSE

Highlights:

•Easy-To-Use: A guided two-step process and progress bar is straightforward for even non-technical users to use

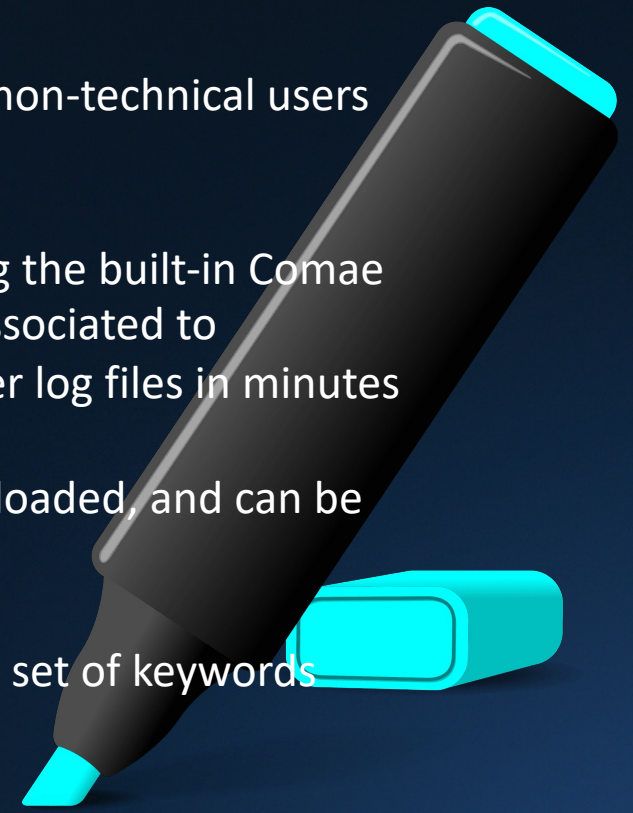
•Fast & Comprehensive: Collect and preserve data starting with the most volatile using the built-in Comae RAM capture (MAGNET DumpIt) functionality, and volatile data and files commonly associated to cybercrime, such as Windows Event Logs, Registry Hives, Jumplist files, and many other log files in minutes

•Portable: It is compromised of a single executable file (less than 2MB), is easily downloaded, and can be stored and run from a USB drive

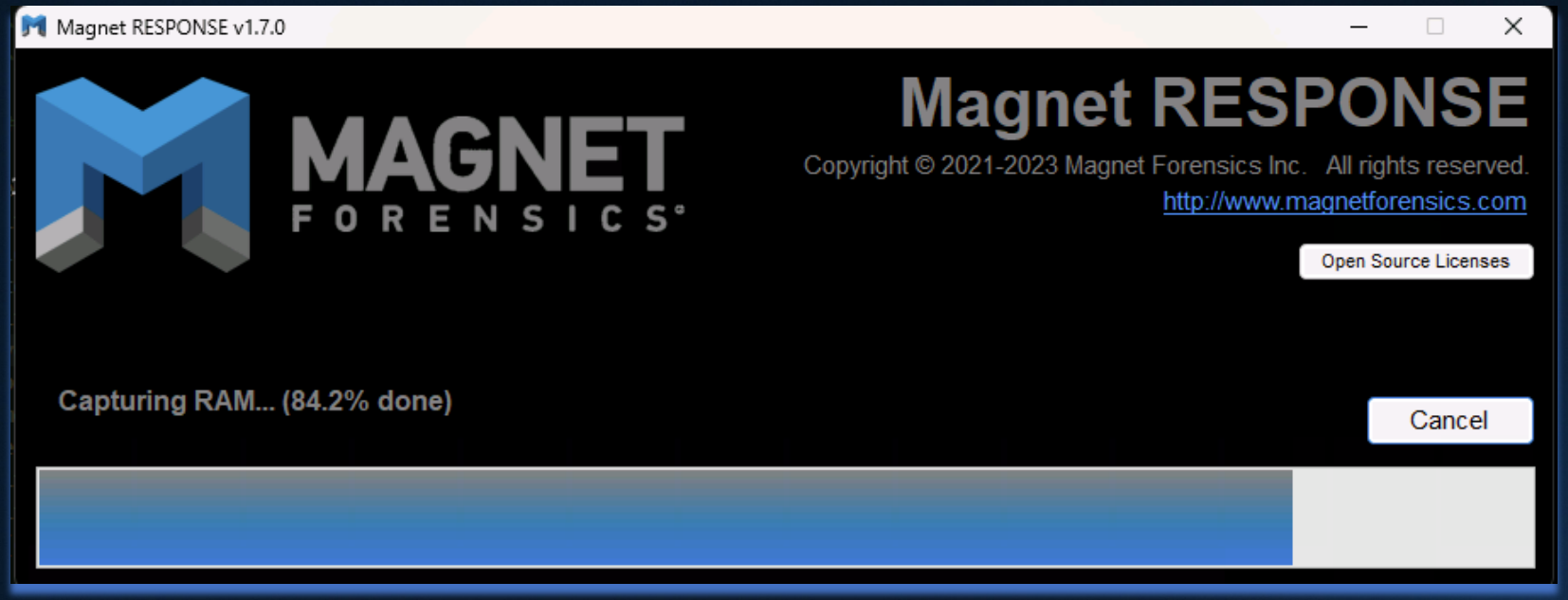
•Collect by Keyword & Skip Large Files: configure free-form collections using your own set of keywords with the option to limit the size of files collected to maintain speed

•Consolidated Output: Output is consolidated and saved as a .zip file for easy delivery or processing and analysis, manually, in Magnet AXIOM Cyber and with Magnet Automate Enterprise

•Data Integrity: An embedded hash value is provided to verify the integrity of the data



Magnet RESPONSE



SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet RESPONSE

Auto-collect Options

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

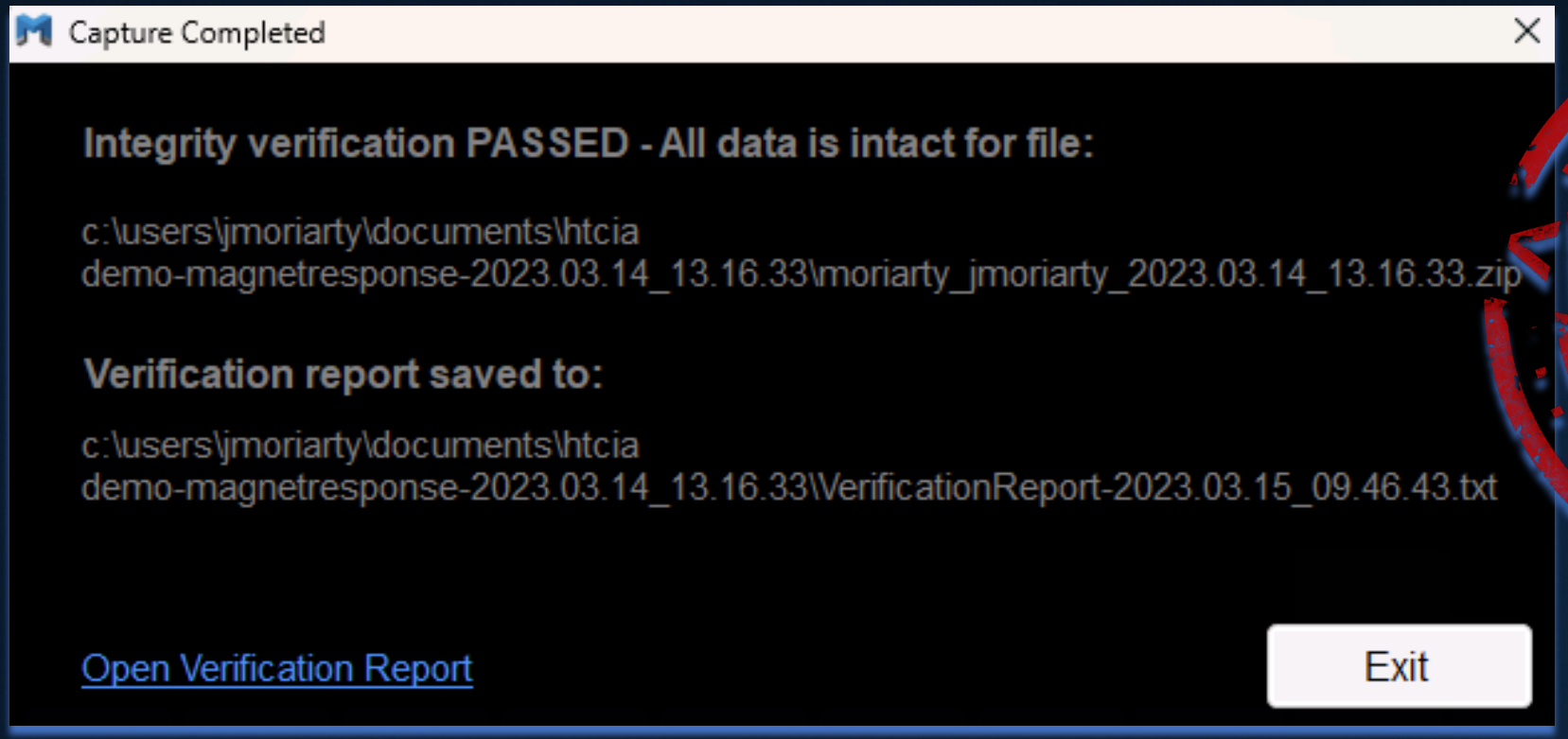
- Option 1 - Capture Everything Rename the executable to have the text "AutoCapture" (no quotes) anywhere in the filename. All options will be enabled, and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs 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. 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

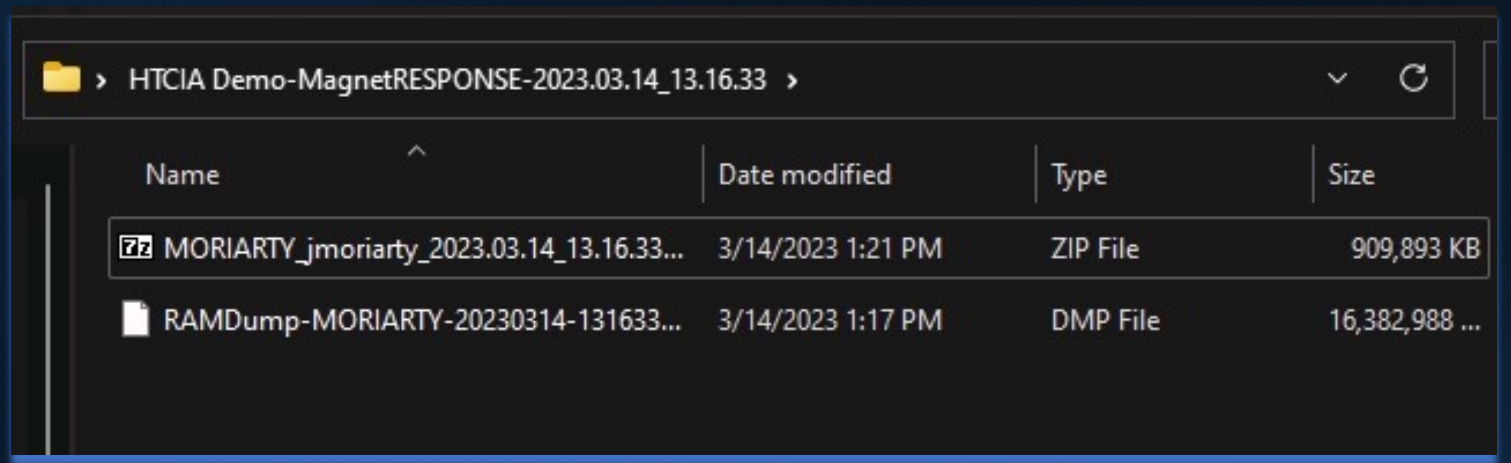
To verify the ZIP, simply drag and drop it on to the RESPONSE executable. RESPONSE will launch as normal and go directly into a verification process, providing a message at the end indicating if the verification was successful. A text file containing details of the verification is saved to the same folder.

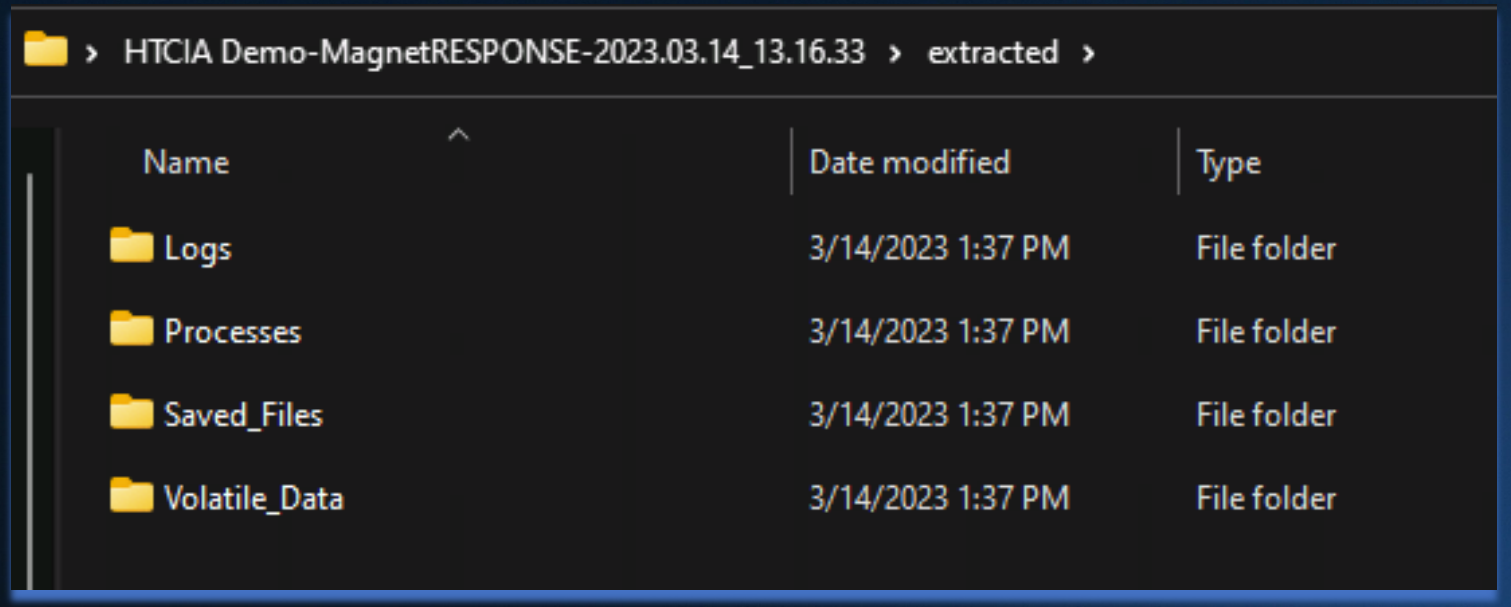


HARDWARE CHOICES

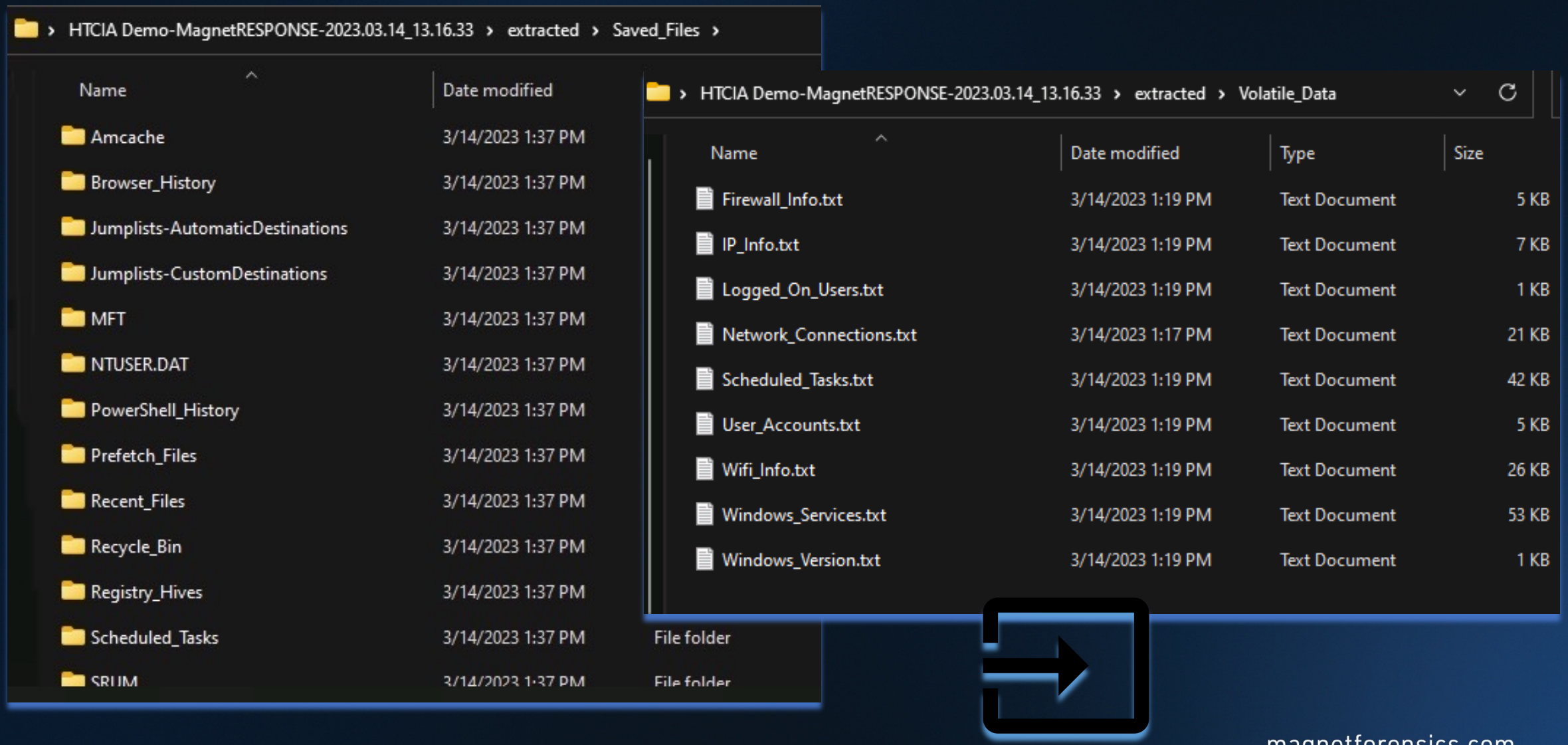
- Samsung T5 or T7

Magnet RESPONSE Output



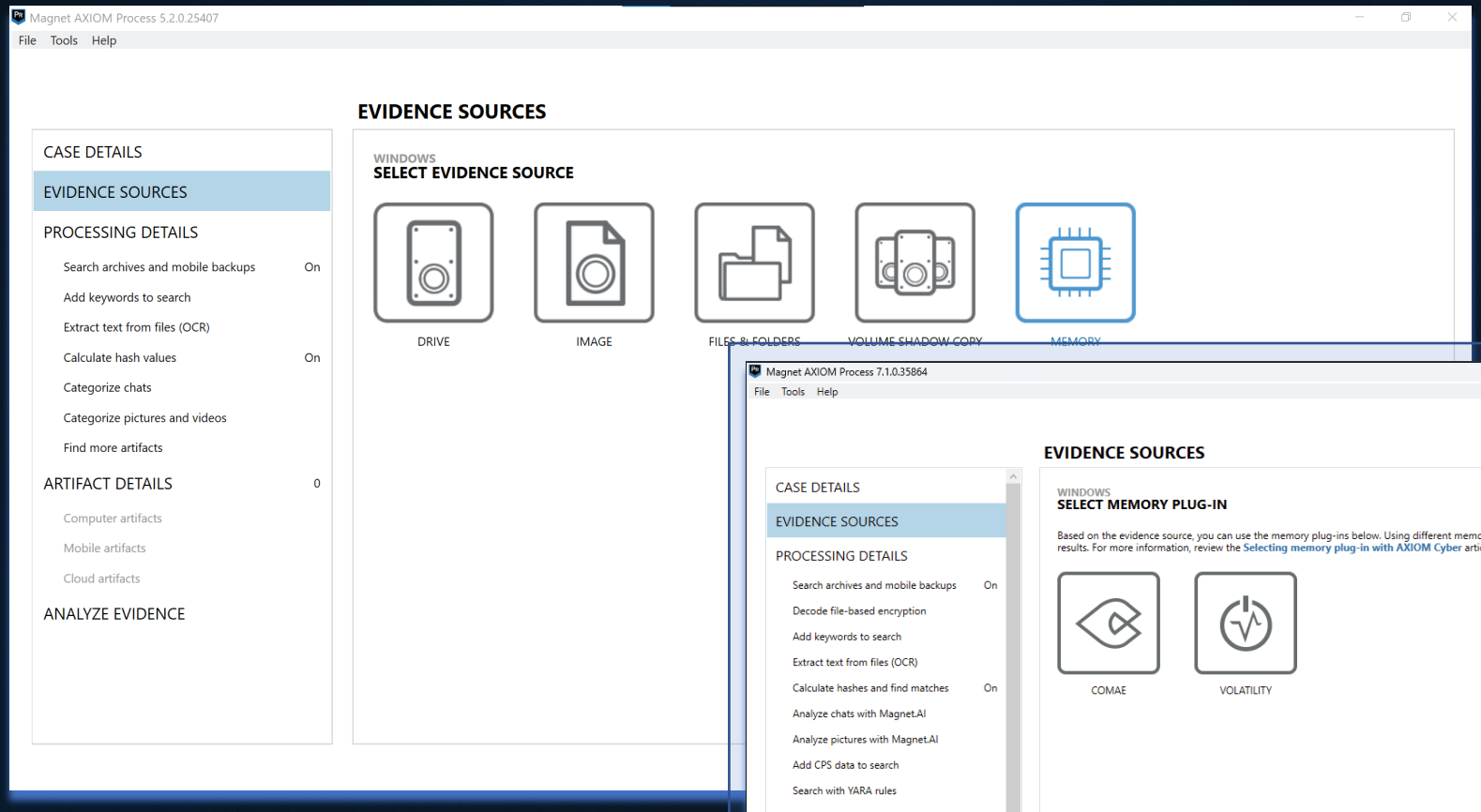


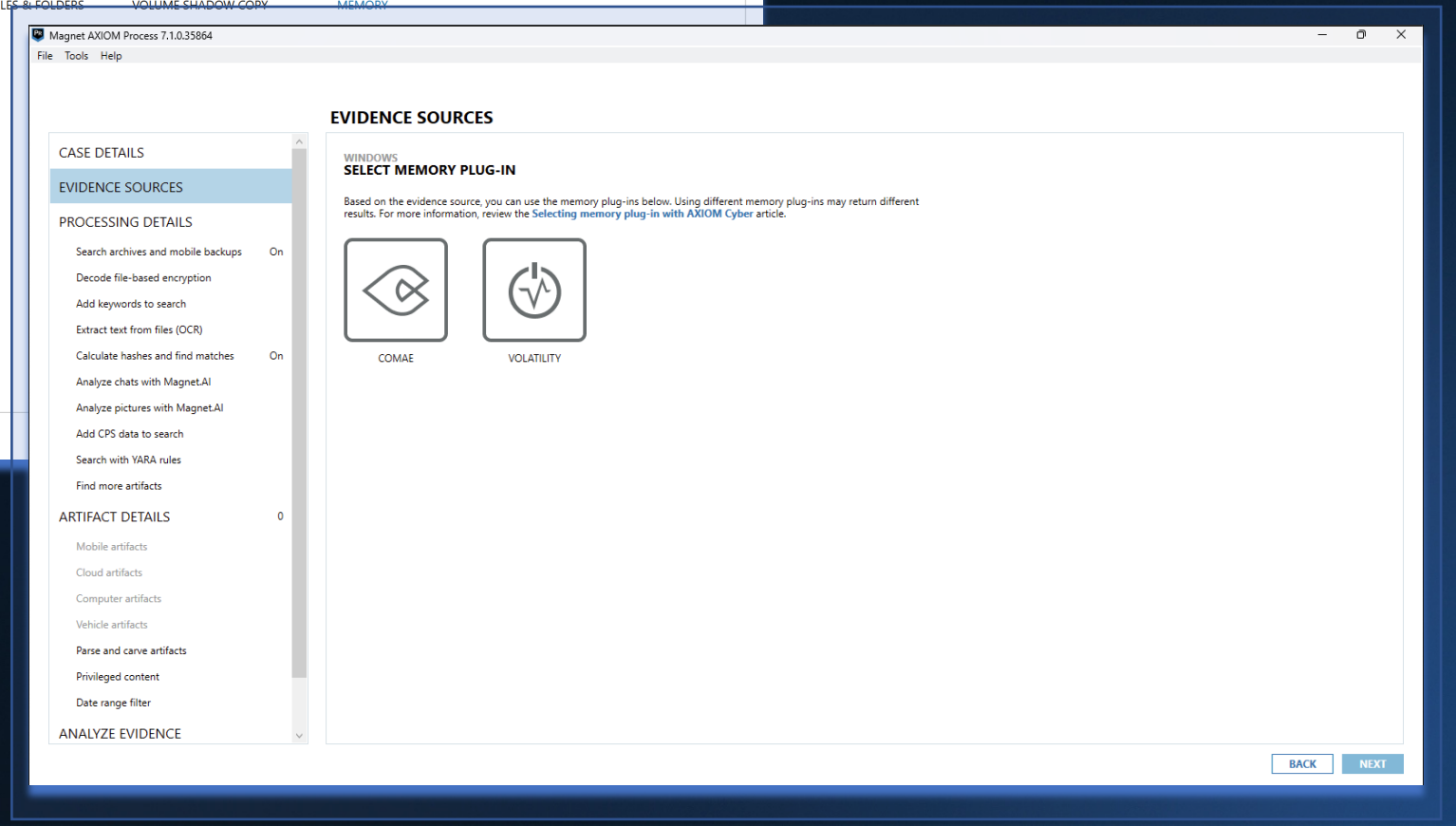
Magnet RESPONSE Output



Evidence Processing Tips

Memory Processing

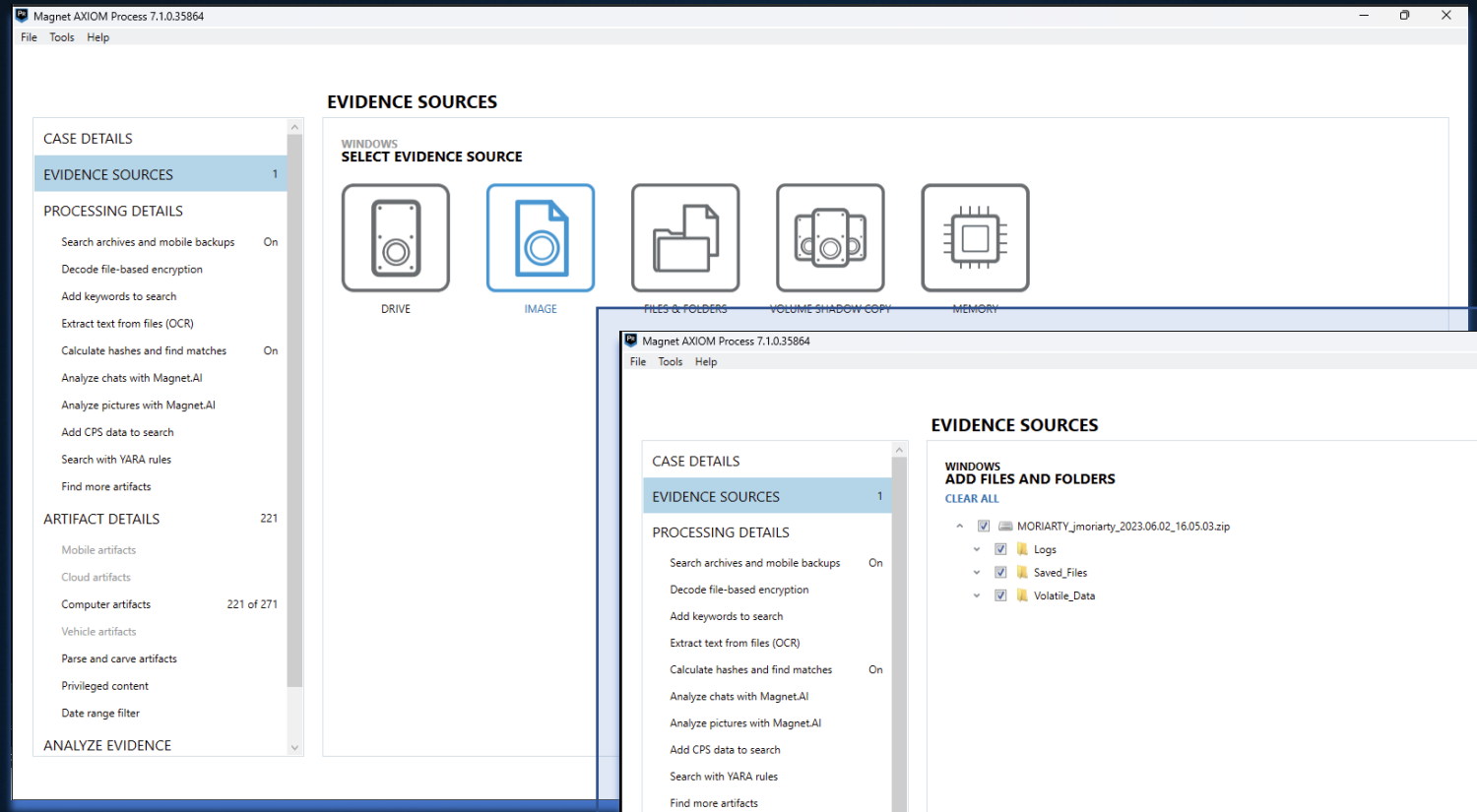


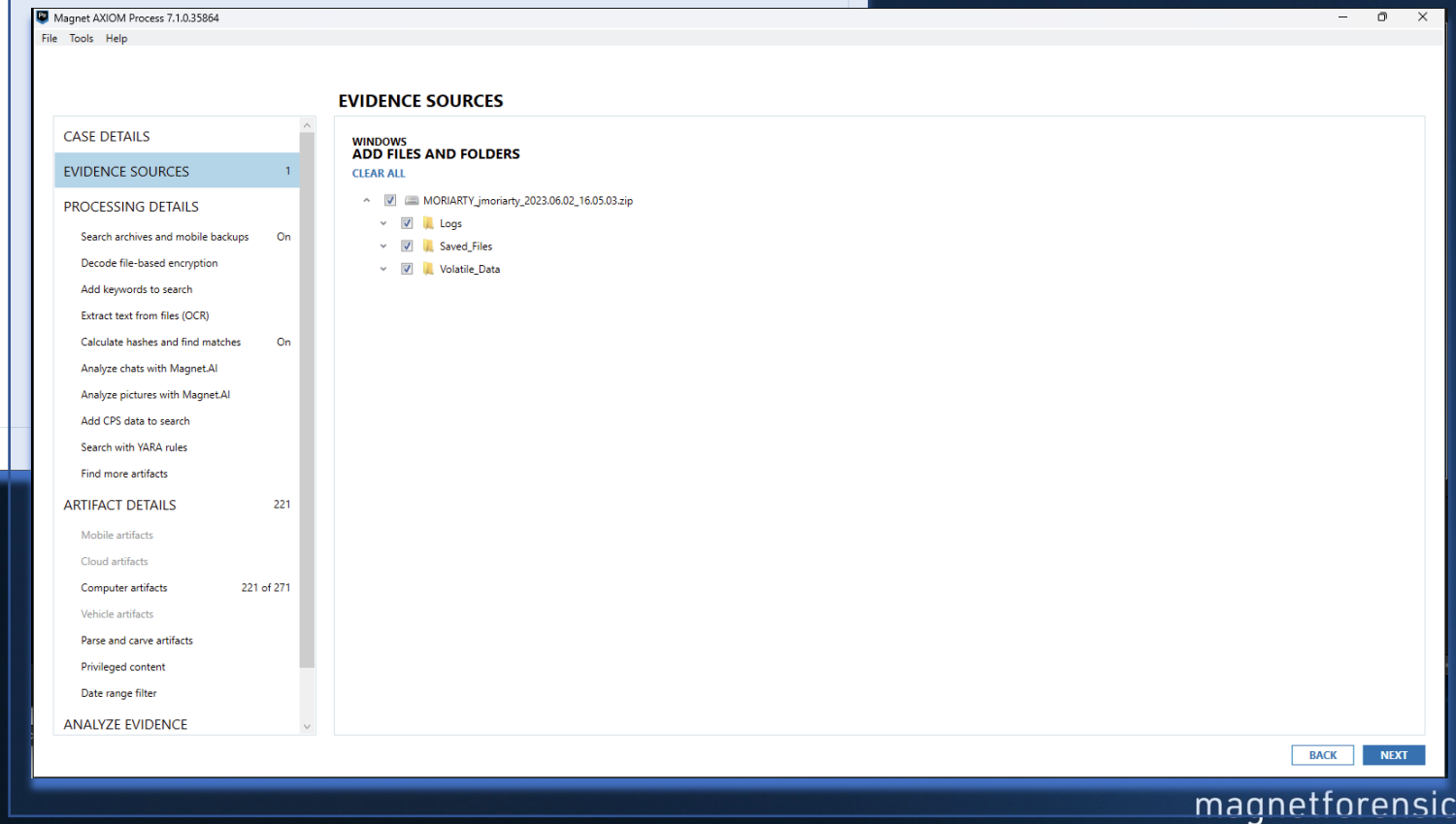


SEEK JUSTICE. PROTECT THE INNOCENT.

Image Processing

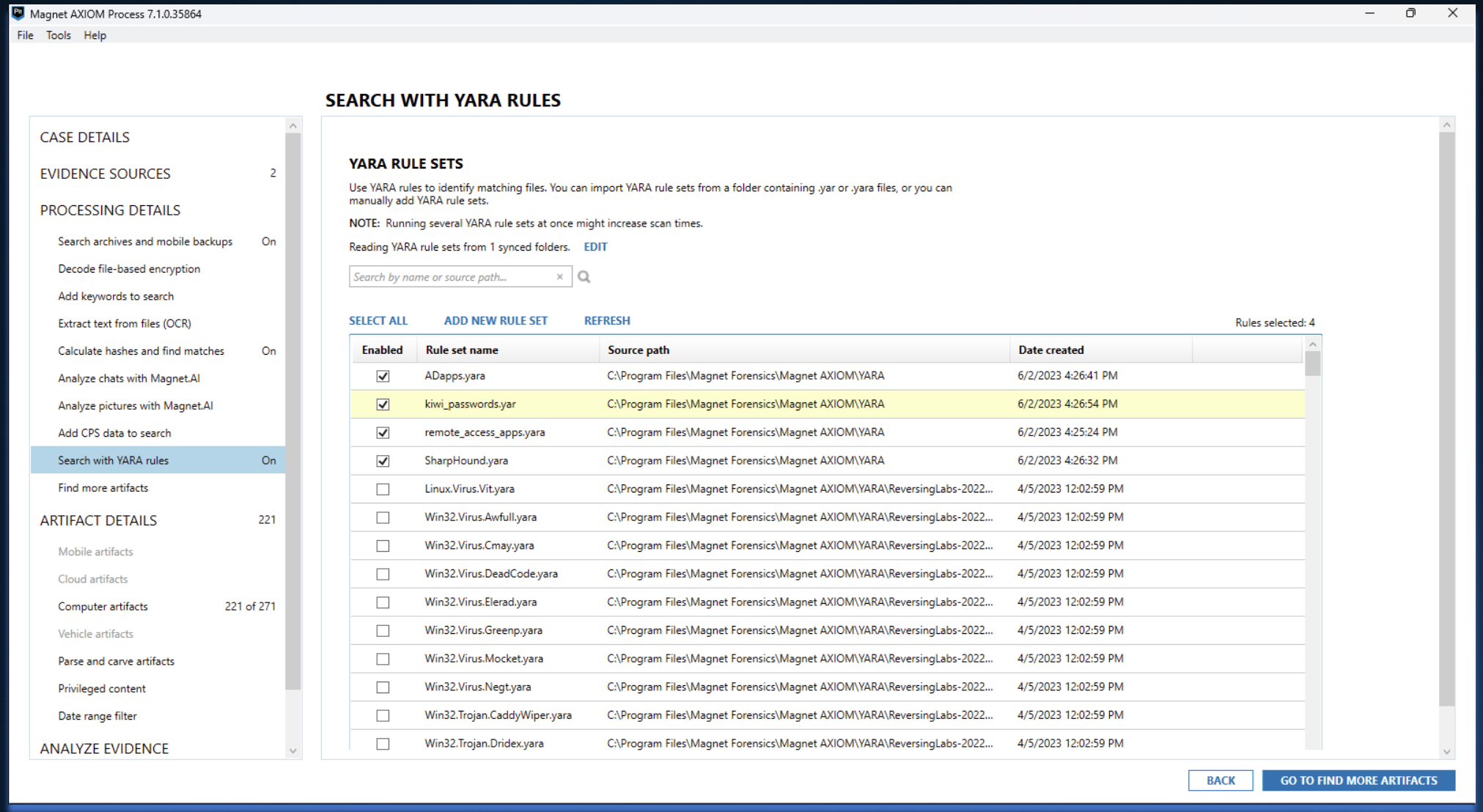
Computer > Windows > Load Evidence > IMAGE





SEEK JUSTICE. PROTECT THE INNOCENT.

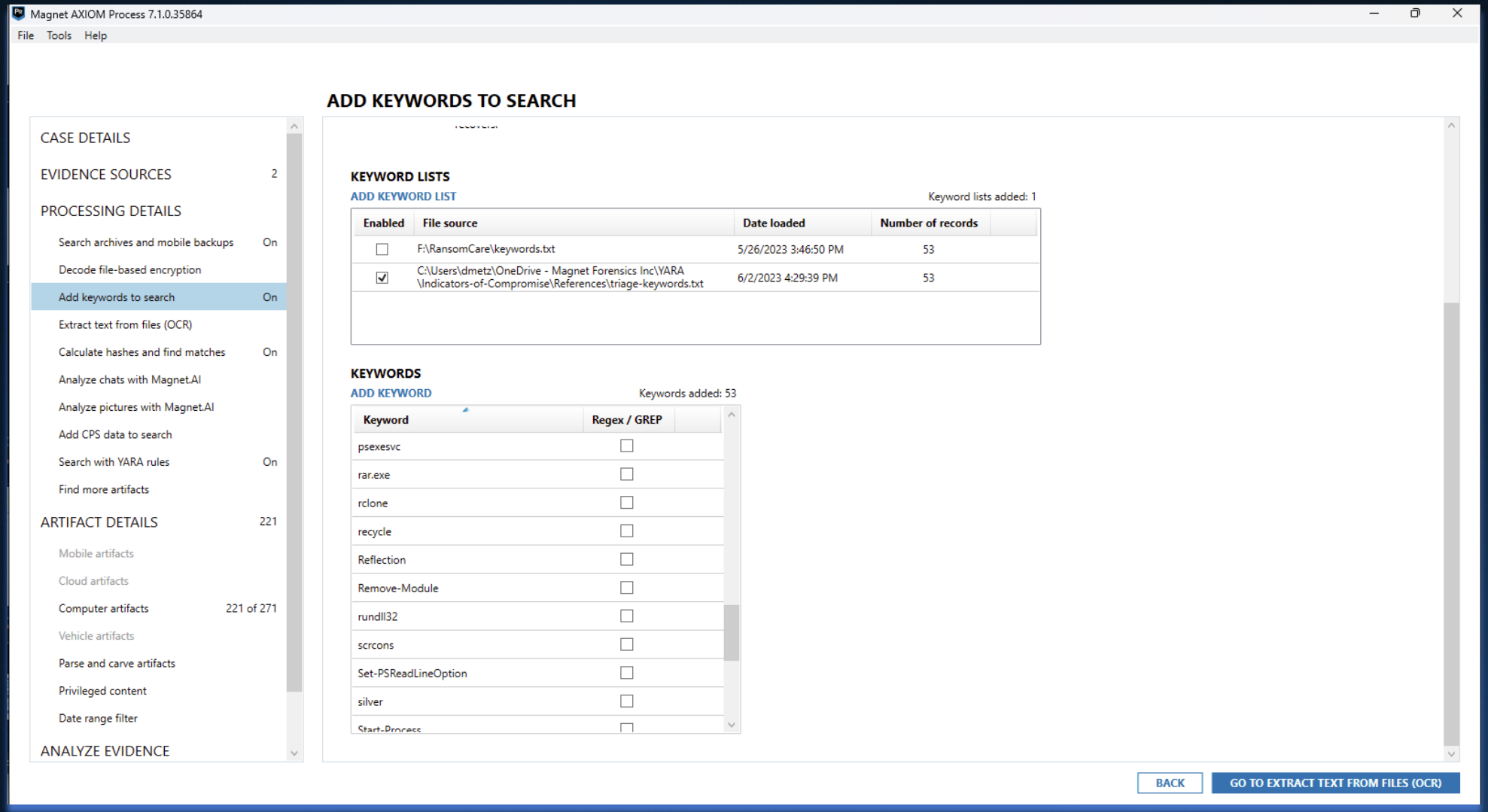
YARA



SEEK JUSTICE. PROTECT THE INNOCENT.

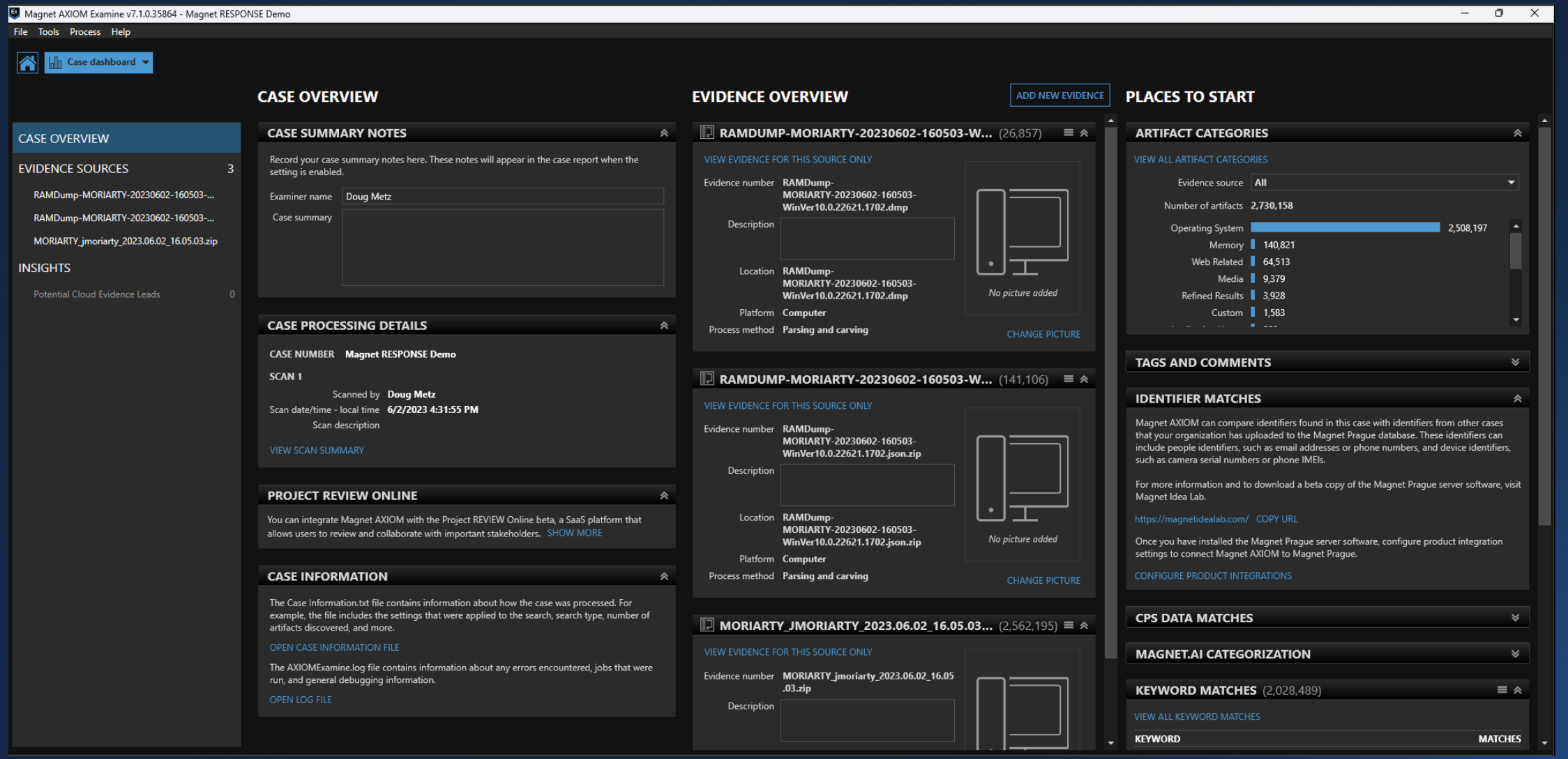
magnetforensics.com

Keywords



SEEK JUSTICE. PROTECT THE INNOCENT.

Artifacts from RESPONSE Triage



SEEK JUSTICE. PROTECT THE INNOCENT.

magnetforensics.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

SEEK JUSTICE. PROTECT THE INNOCENT.

MAGNET FORENSICS®

magnetforensics.com