MAGNET USER SUMMIT 2023

Magnet2Go

Building a 'Windows to Go' Drive to Support Offline Collections

Doug Metz, Professional Services Consultant
Magnet Forensics

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

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

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

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.

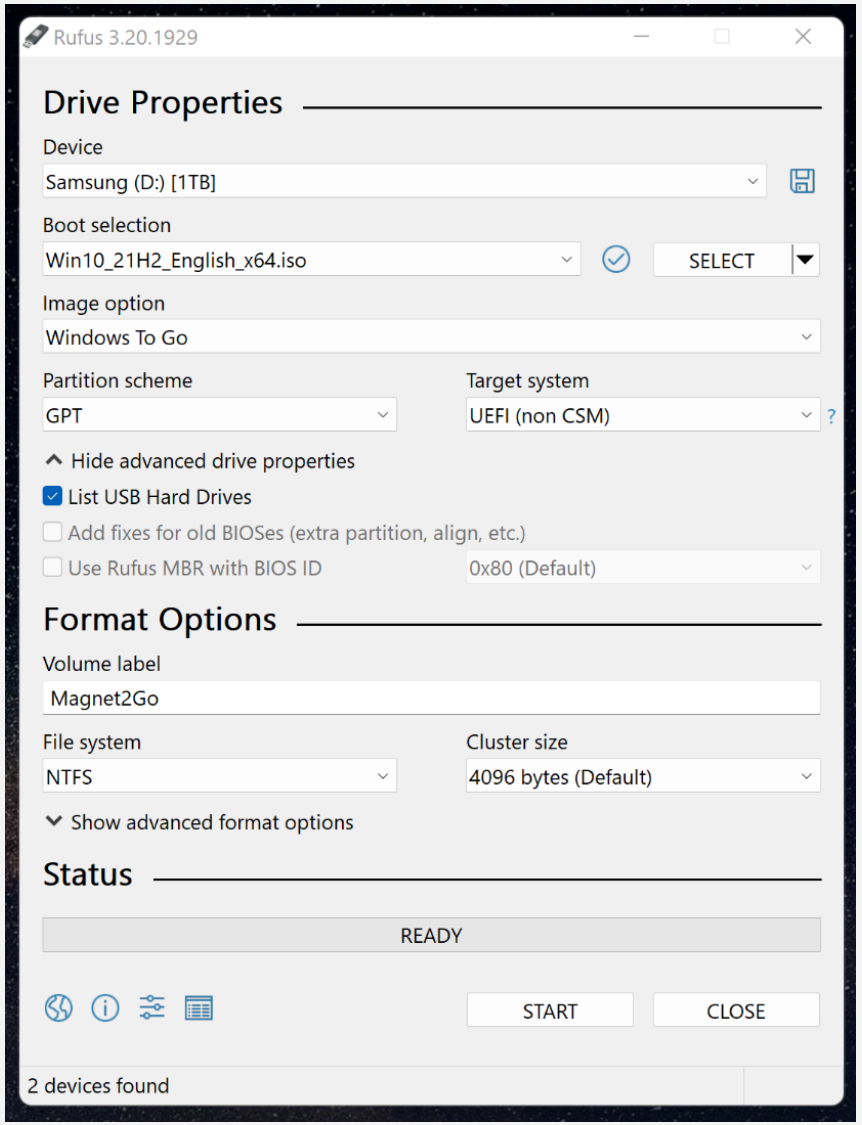
- **Device** The USB drive you want to use for Magnet2Go
- **Boot selection** Browse to and select the Window .iso file
- **Image option** Select **Windows to Go**

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

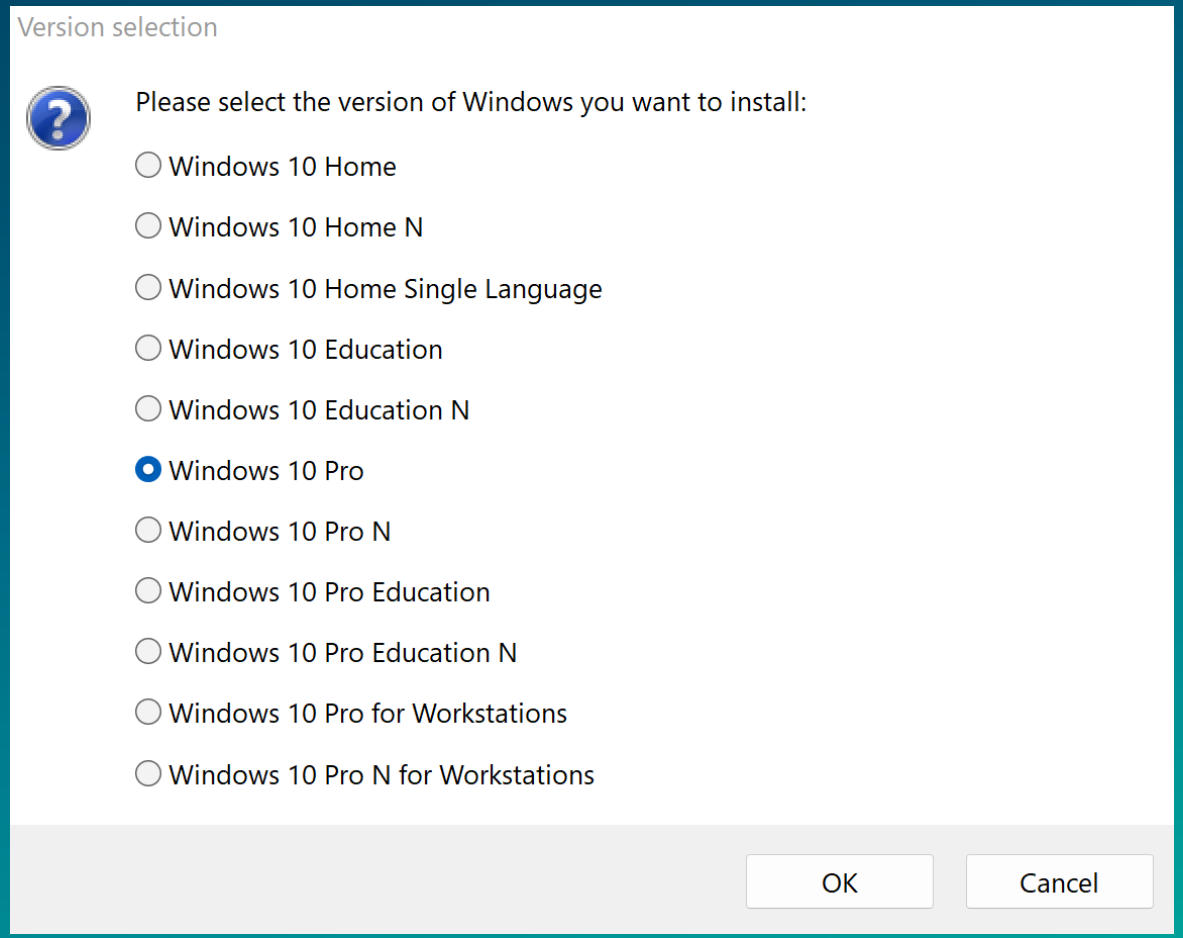
- **Volume label** **Magnet2Go**

Triple check your settings and then press Start.

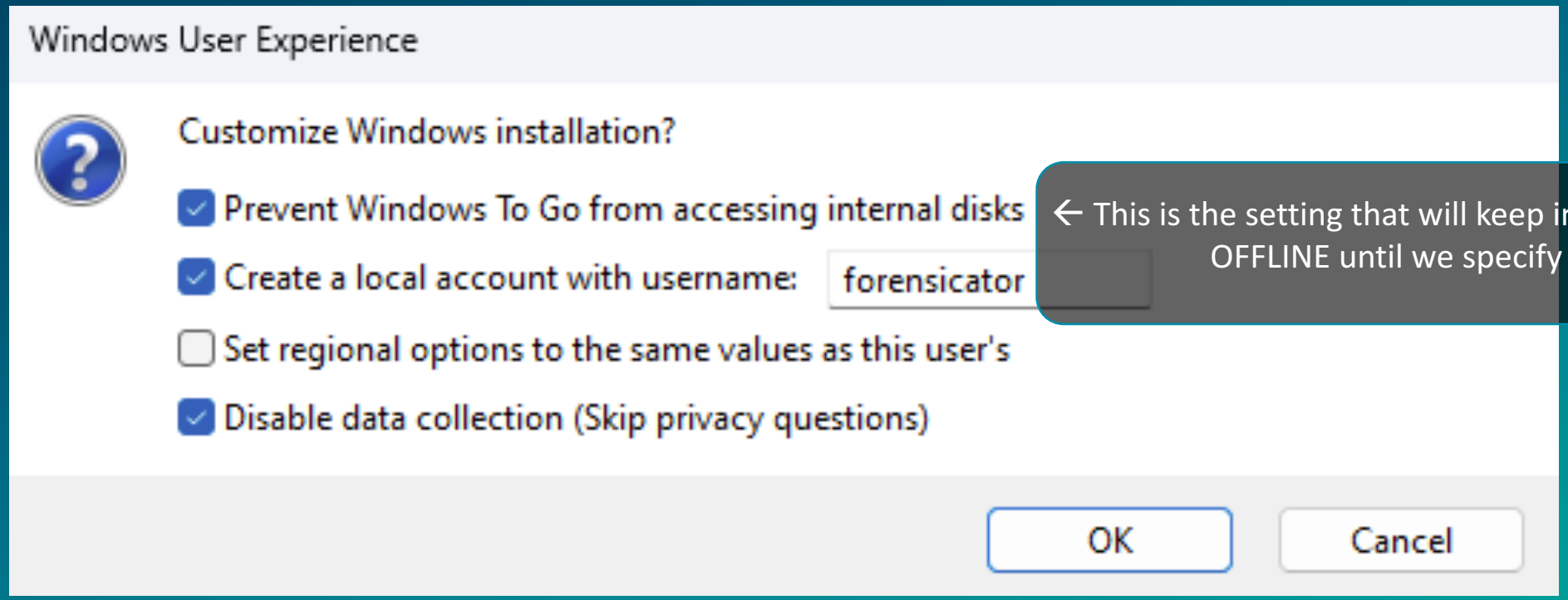
*Changing certain options like the **Image option** can reset the **Volume label** information back to default.*



Windows Version

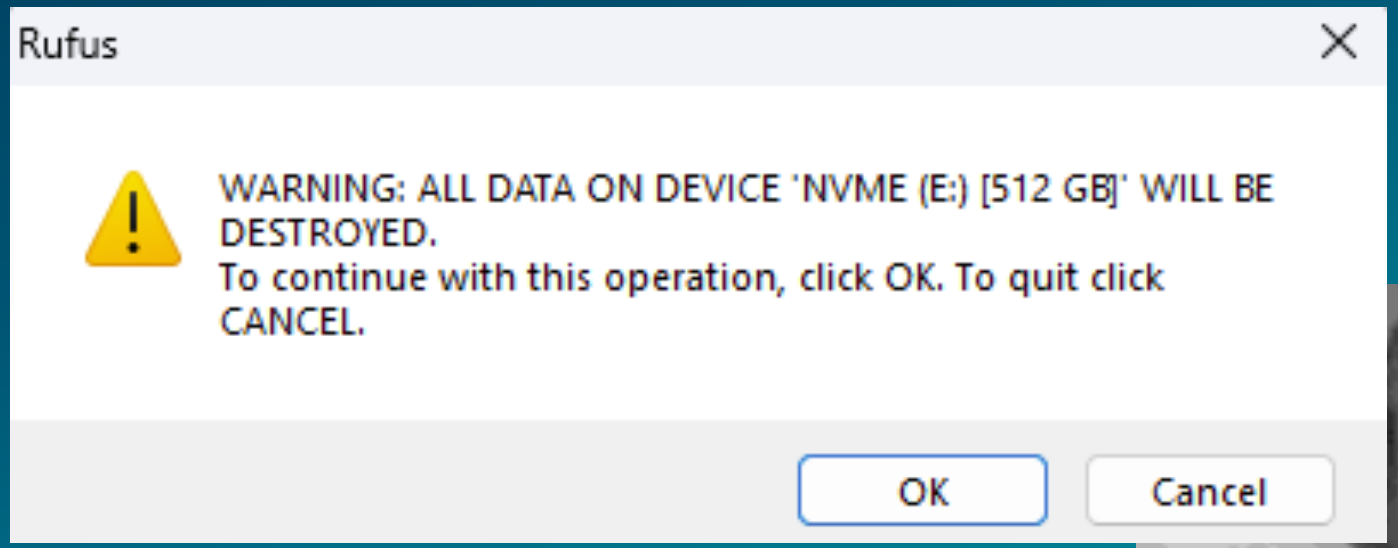


WUX

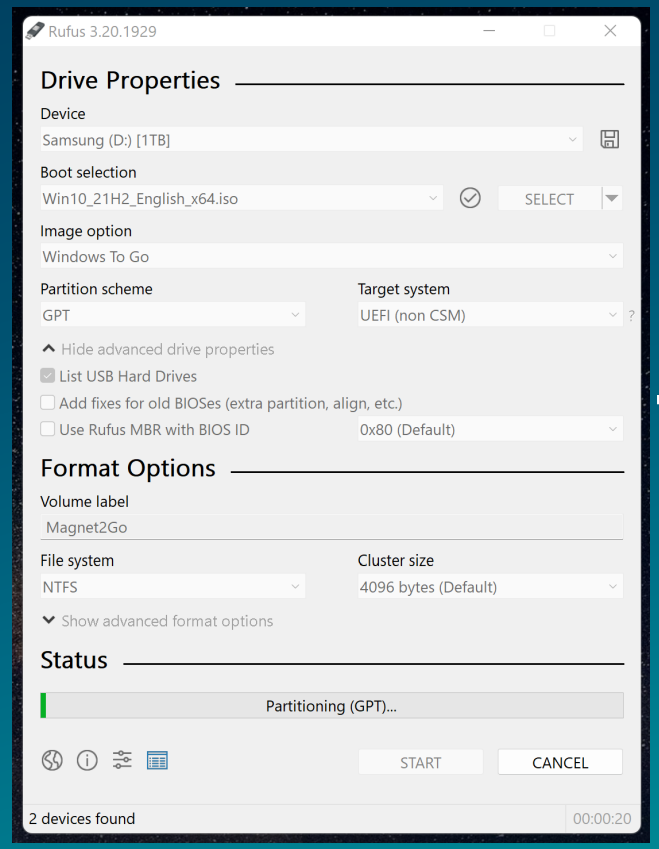


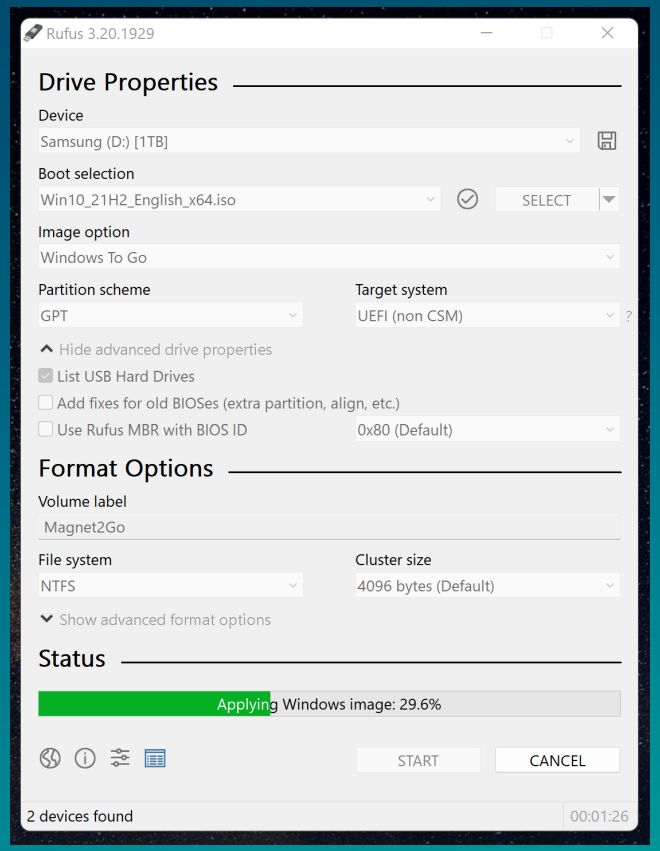
← This is the setting that will keep internal drives OFFLINE until we specify otherwise

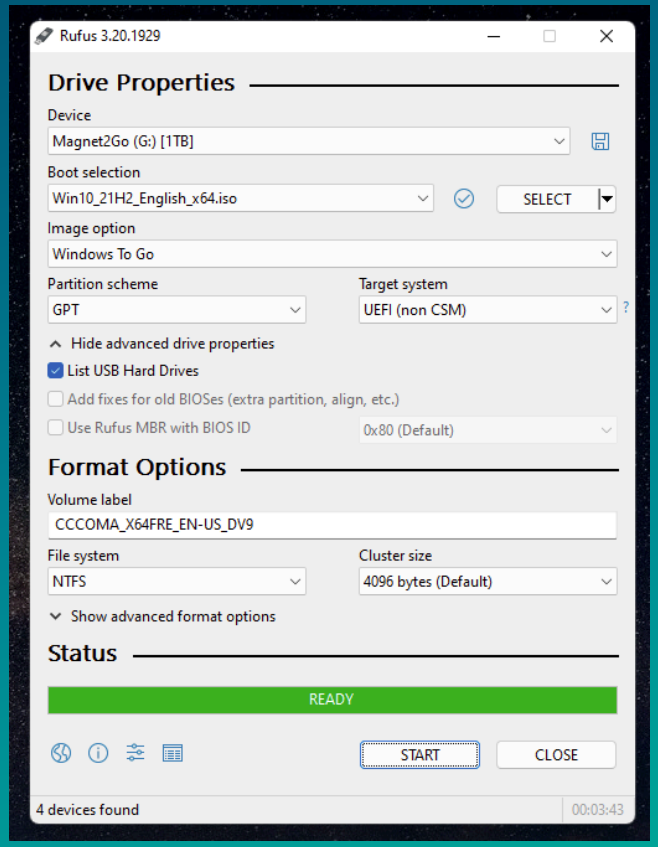
Danger, Will Robinson



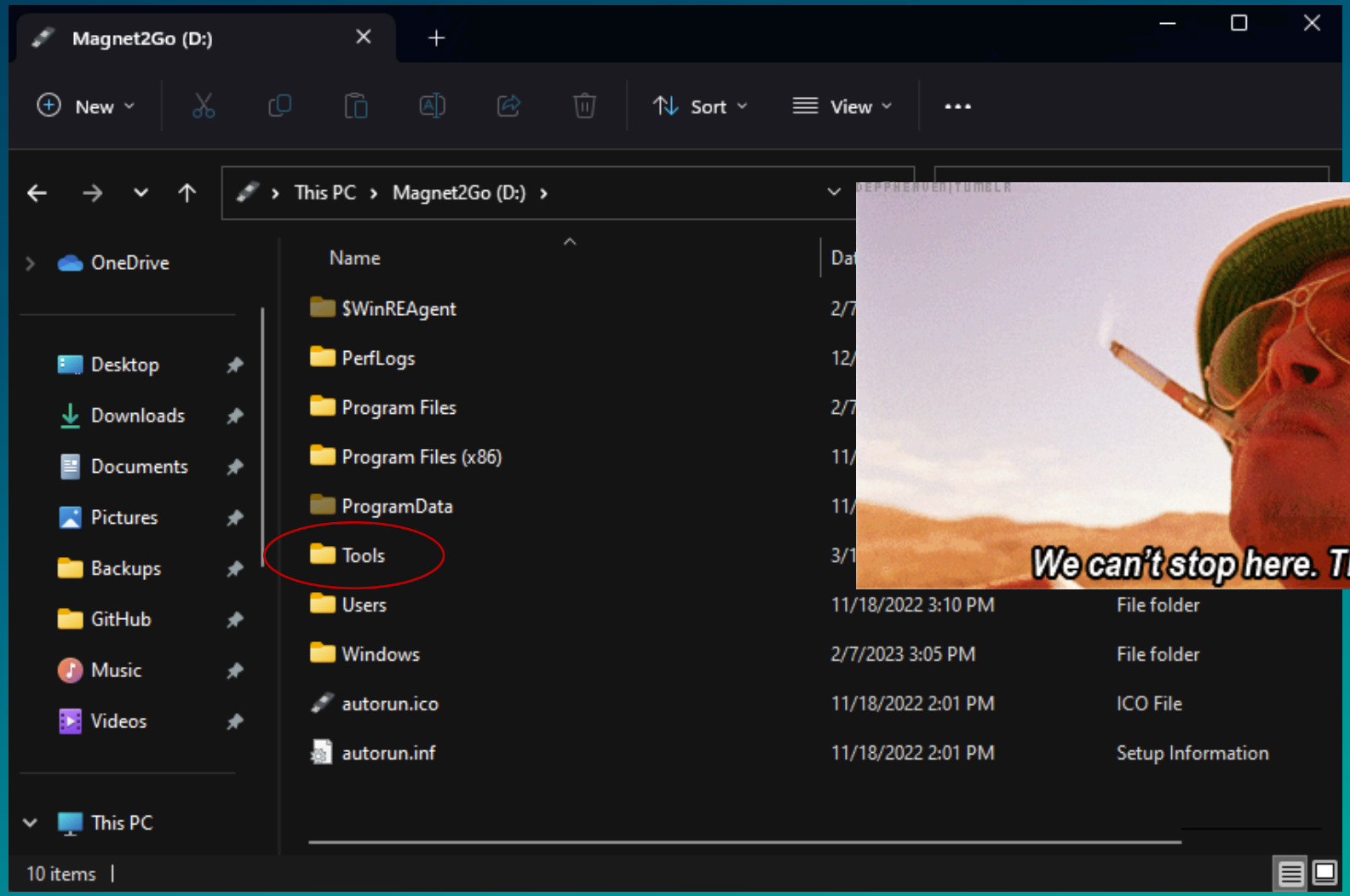
Partitioning… Applying Image… Complete.



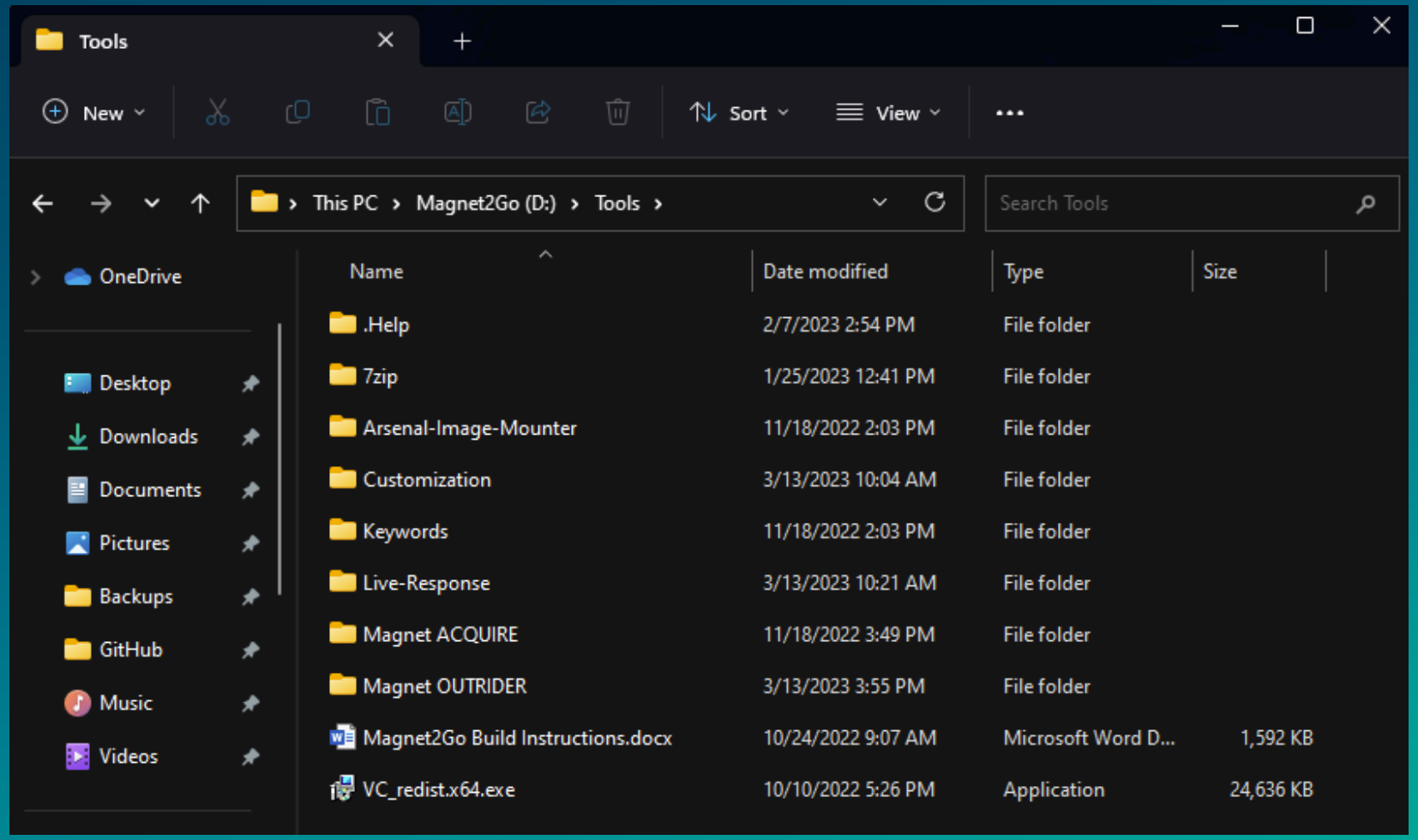




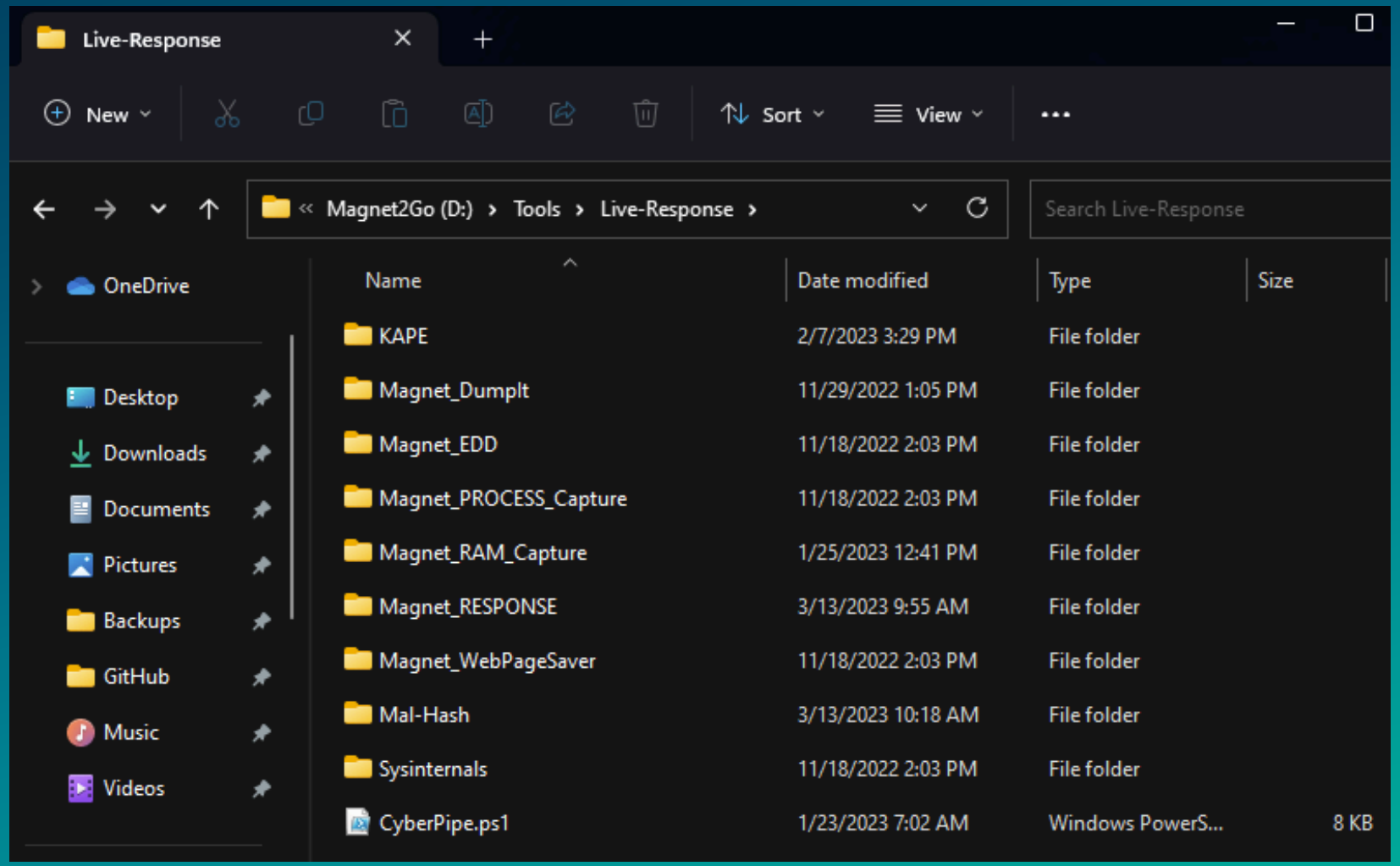
Before You Go On...



Tools Directory



Live Response Tools



Suggested Tools

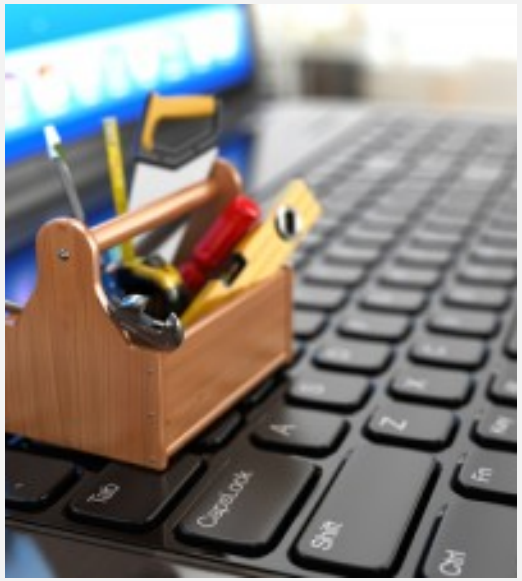
- Magnet OUTRIDER –. Free trial: https://www.magnetforensics.com/products/magnet-outrider

  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)

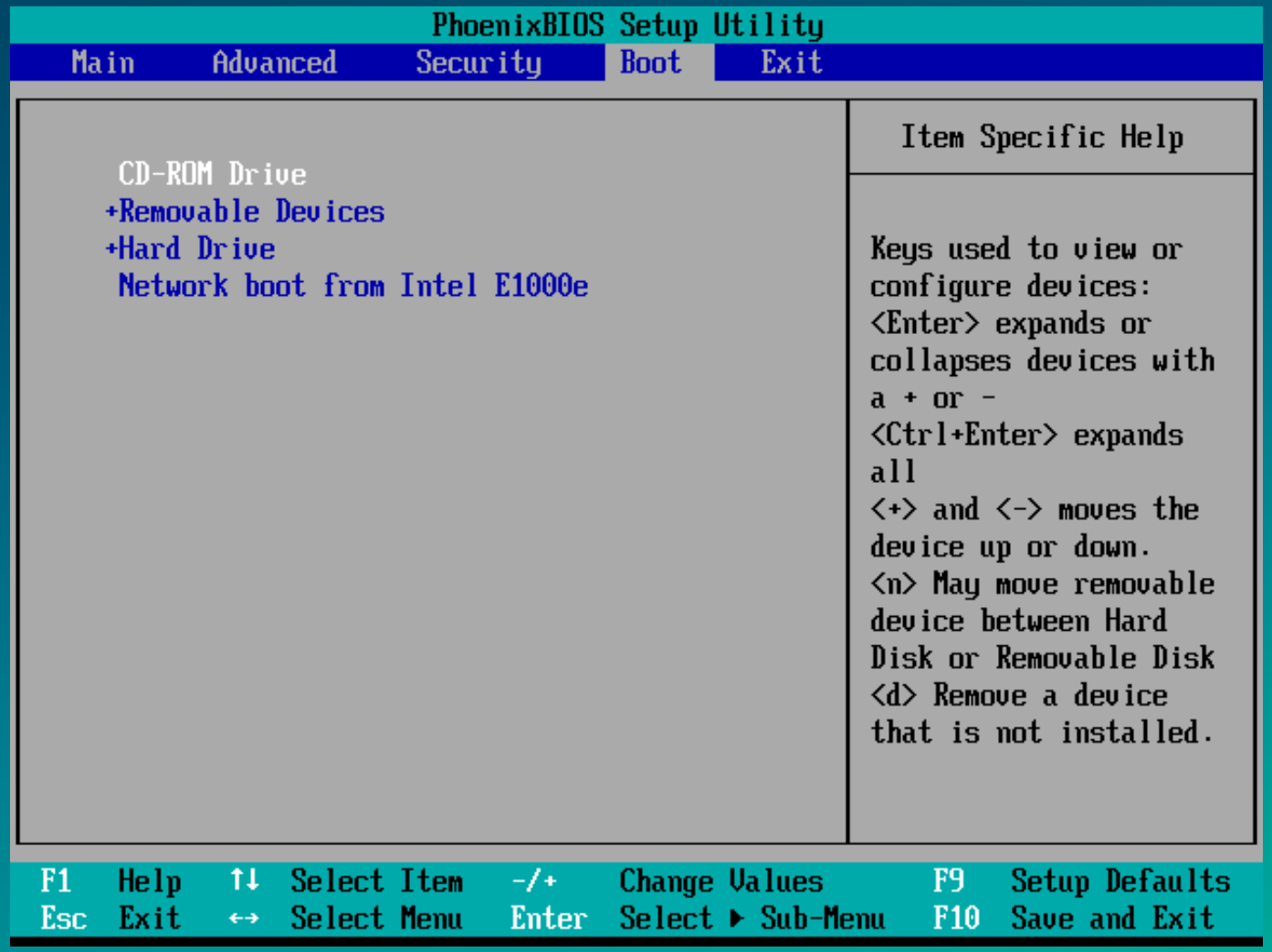
  This is a dependency for a number or the Magnet Forensics tools.
- Arsenal Image Mounter – (copied from existing installation); https://arsenalrecon.com/downloads/

Live Response

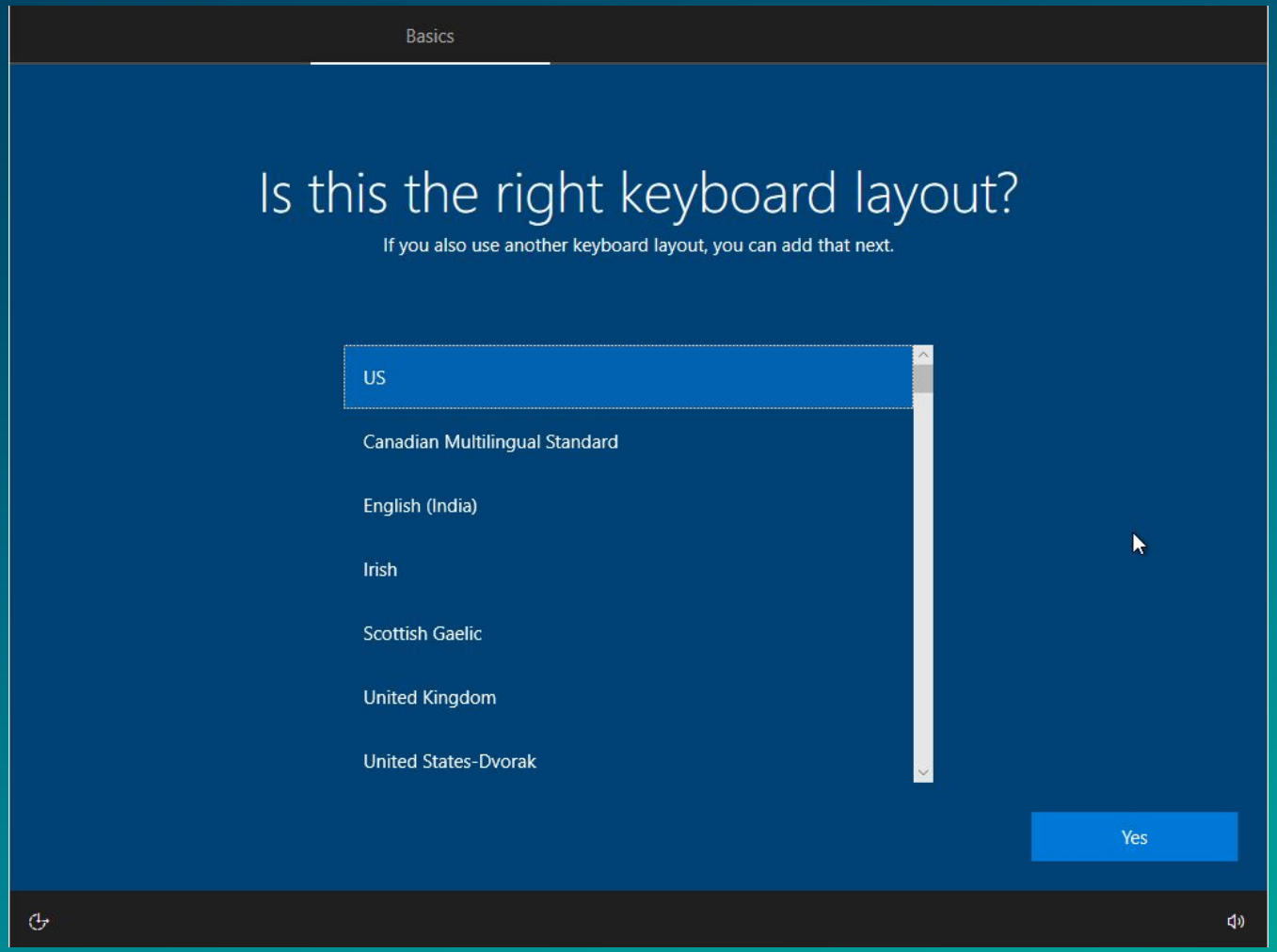
- Magnet RAM Capture - https://support.magnetforensics.com/s/free-tools
- Magnet DumpIt for Windows - https://www.magnetforensics.com/blog/how-to-get-started-with-comae/
- Magnet Encrypted Disk Detector - https://support.magnetforensics.com/s/free-tools
- Magnet Process Capture - https://support.magnetforensics.com/s/free-tools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



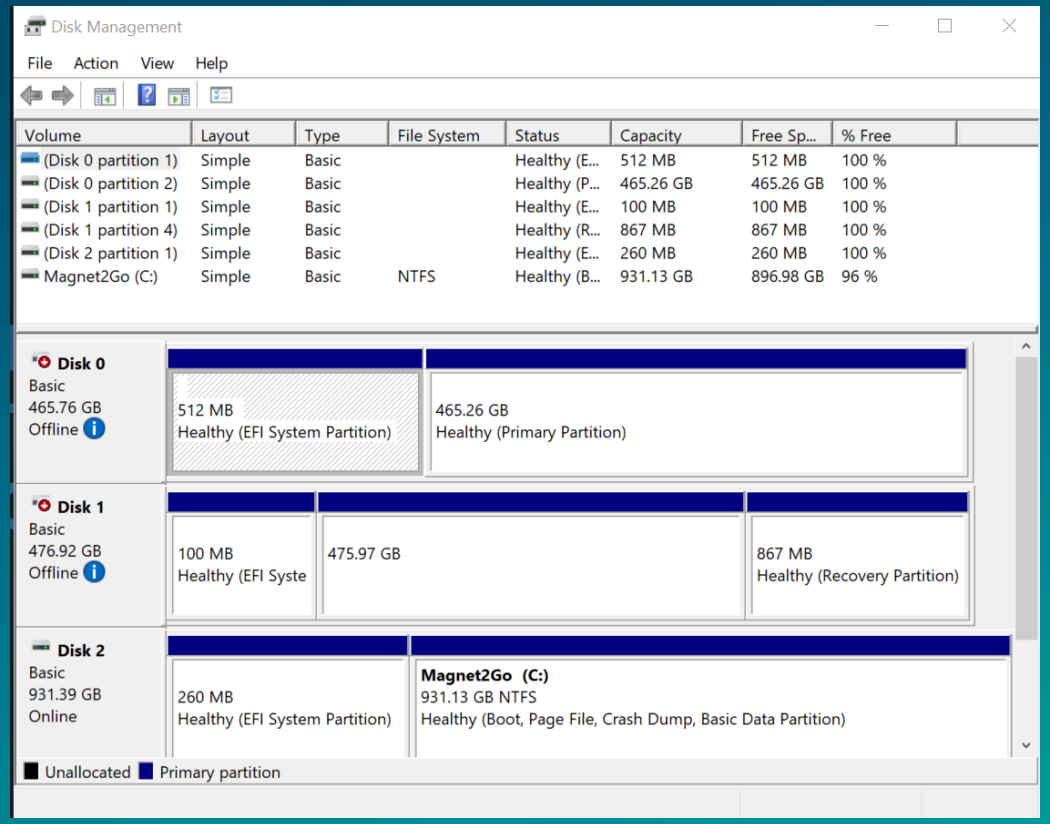
First Boot (Setup)



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.

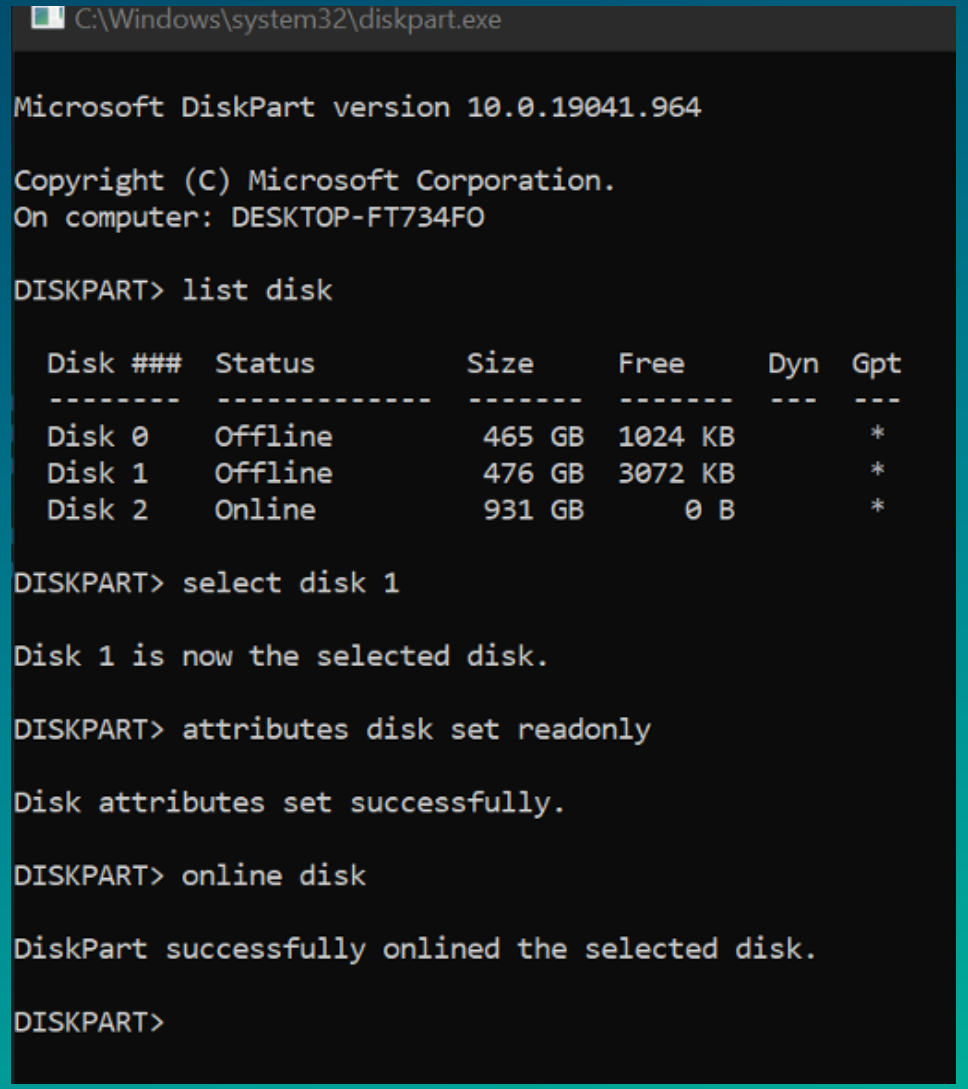
Diskpart Syntax

- **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.

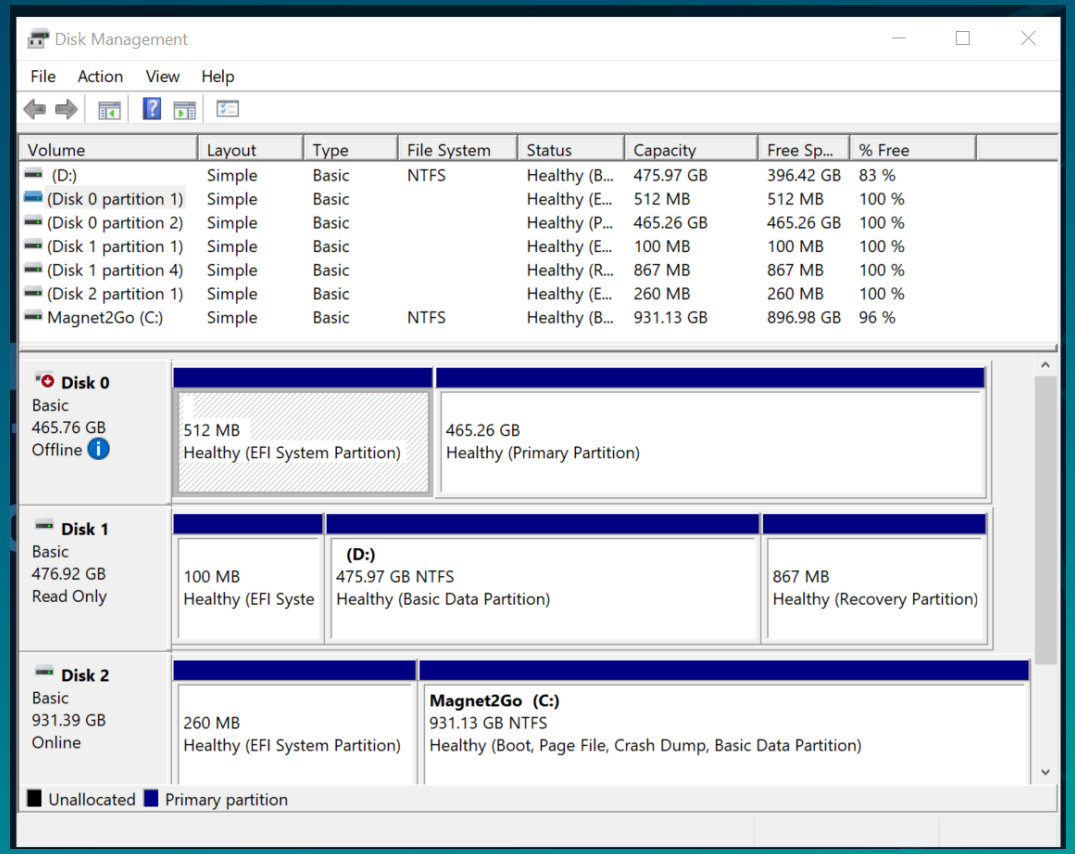
- **Select disk 1** will select the specified disk number.

- 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.

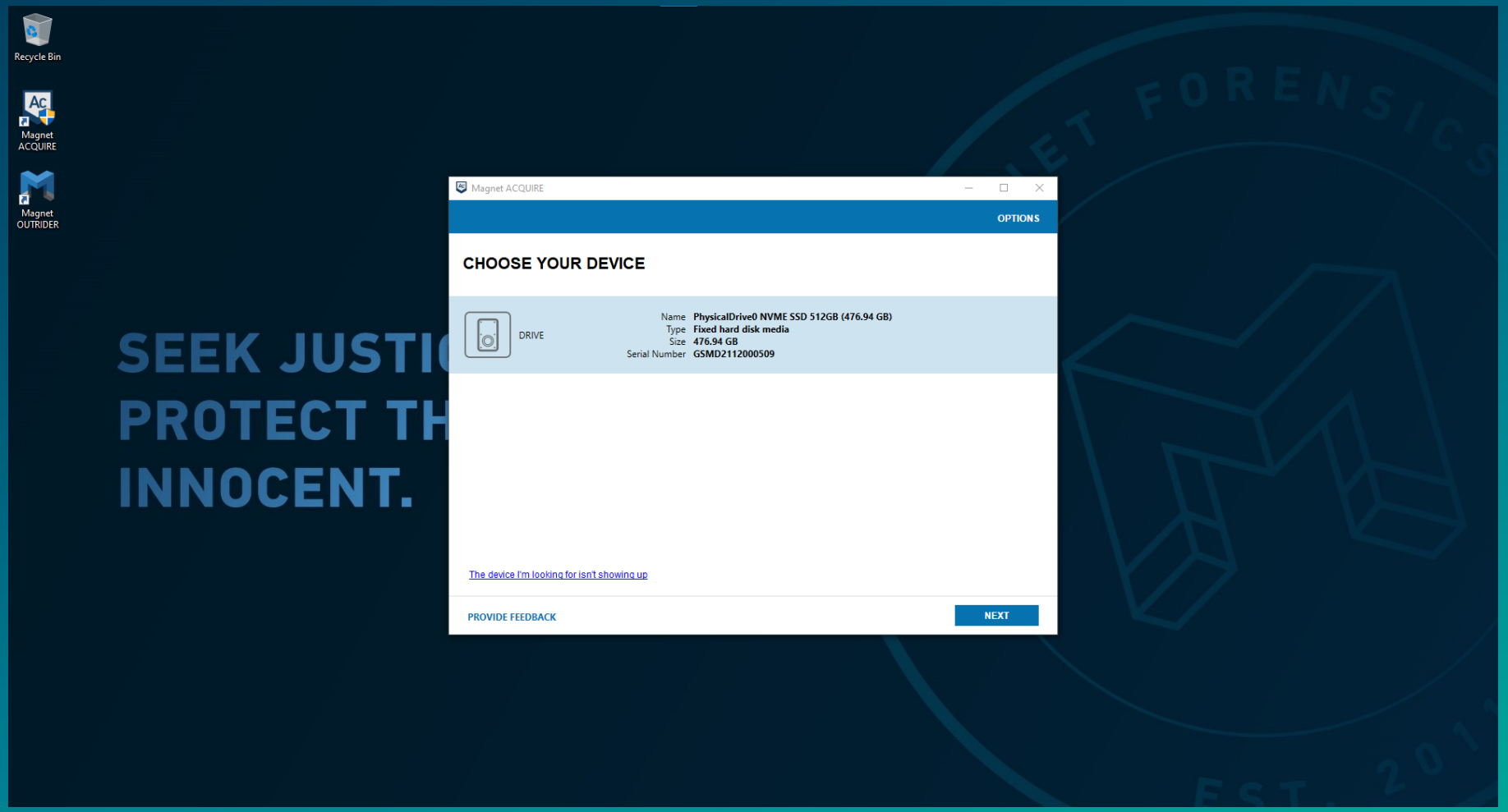


Verify READ-ONLY



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

Disk Acquisition – Magnet ACQUIRE

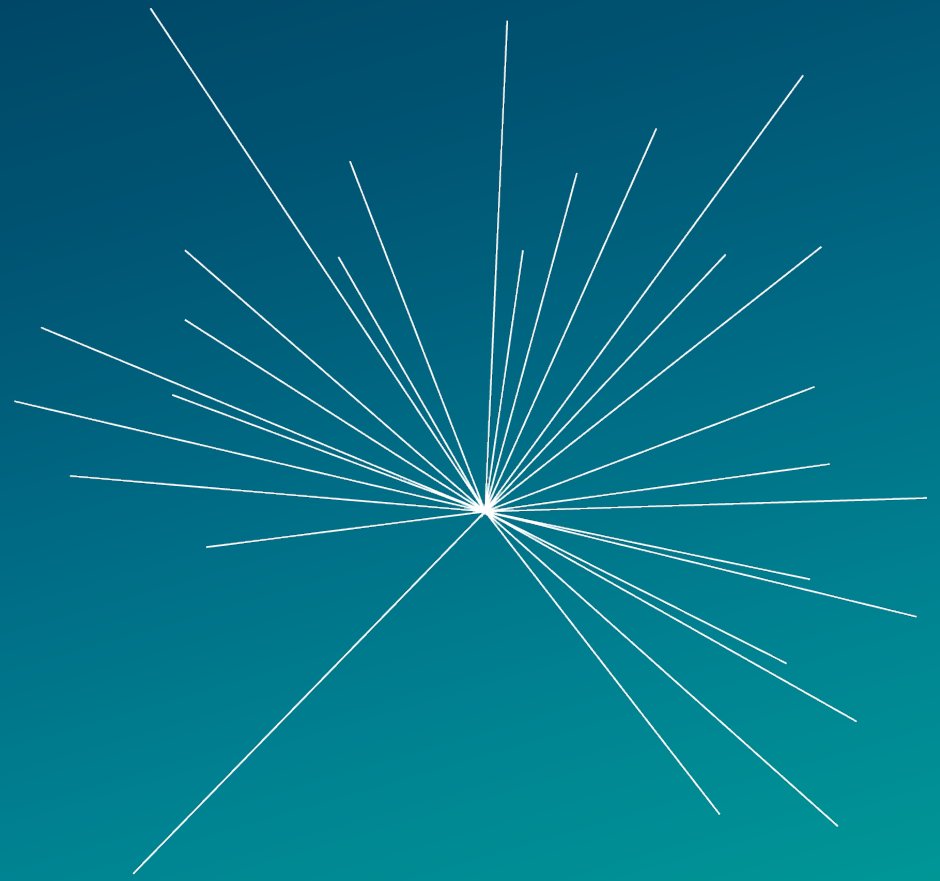


Triage for Illicit Content – Magnet OUTRIDER

MAGNET USER SUMMIT 2023

Live Response

Triage collections for On and Off Network



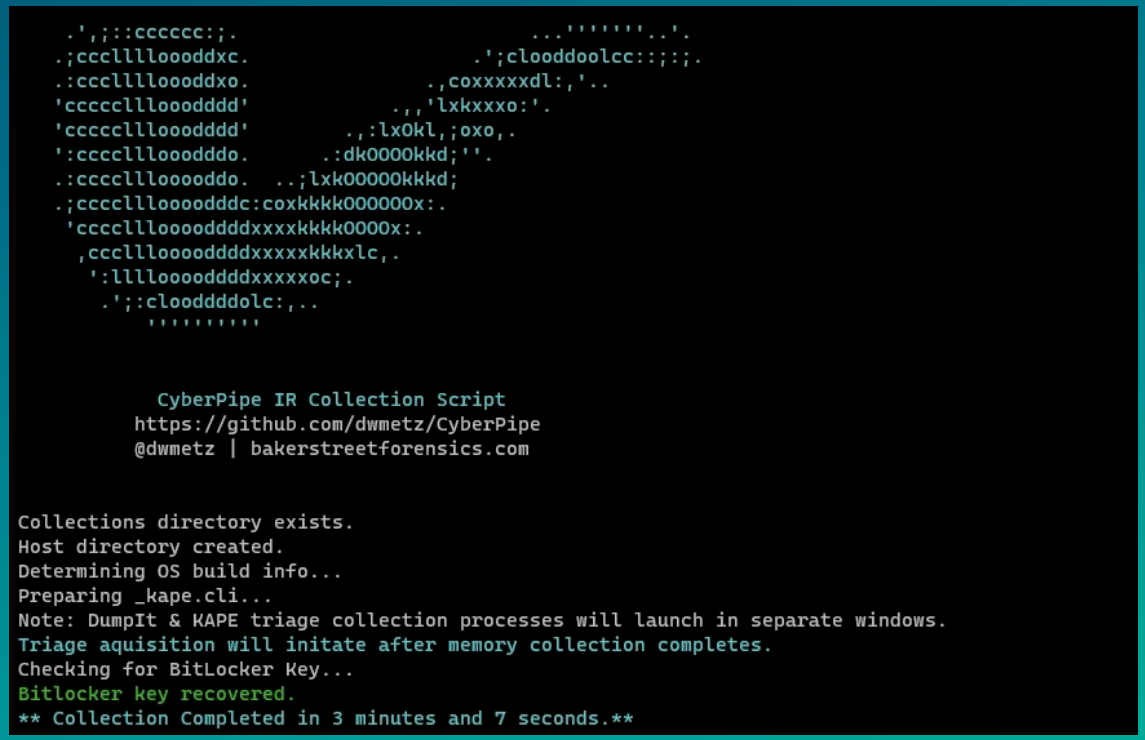
CyberPipe

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.



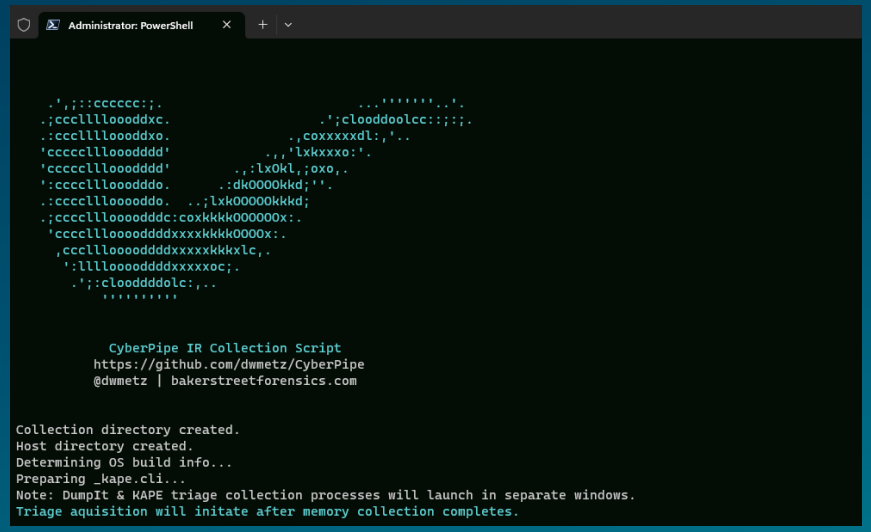
CyberPipe

v4.0 Features: "One Script to Rule them All"

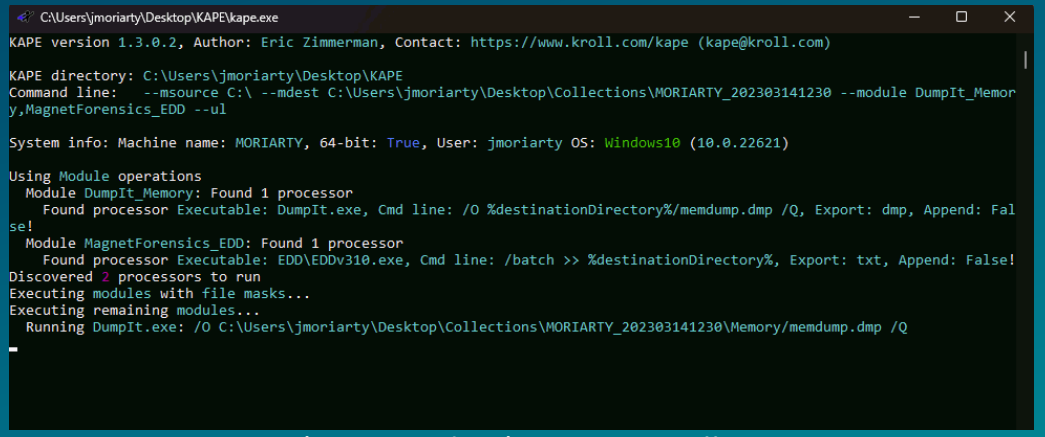
- Admin permissions check before execution.
- Memory acquisition will use Magnet DumpIt for Windows (previously used Magnet RAM Capture).
- Support for x64, ARM64 and x86 architectures.
- Both memory acquisition and triage collection now facilitated via KAPE batch mode with _kape.cli dynamically built 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.

```
    ':lllloooodddxxxxxoc;.
     .';::cloodddolc:,..
         ''''''''''
"
Write-Host -Fore Cyan "           CyberPipe IR Collection Script"
Write-Host -Fore Gray "         https://github.com/dwmetz/CyberPipe"
Write-Host -Fore Gray "         @dwmetz | bakerstreetforensics.com"
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 {
```

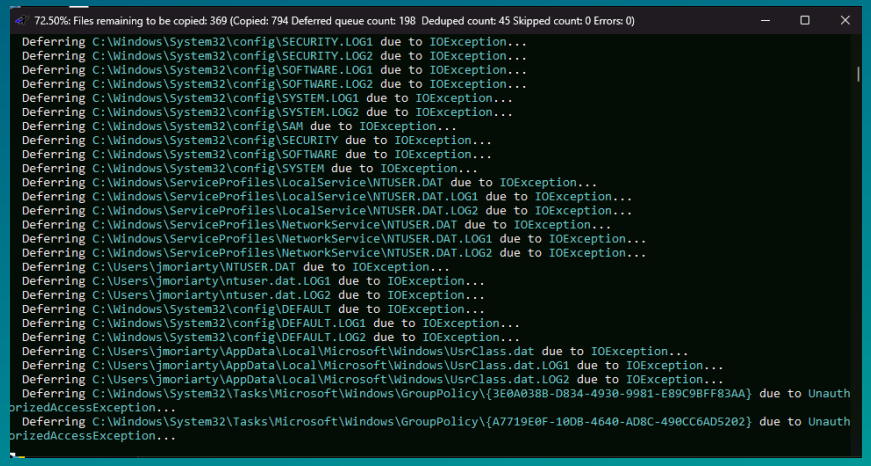
CyberPipe Operations



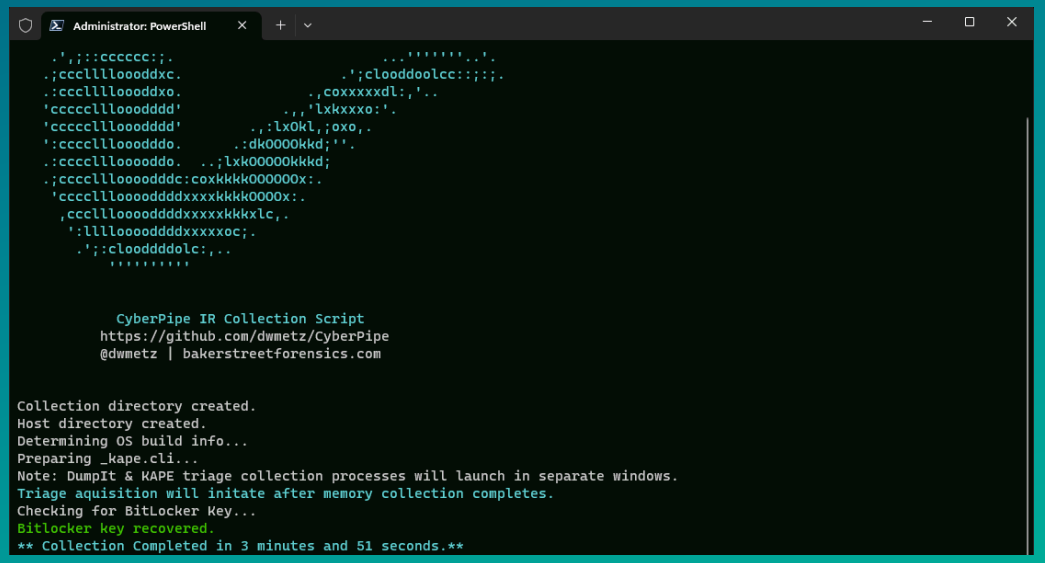
1. Script launch



2. (new window) Memory Collection

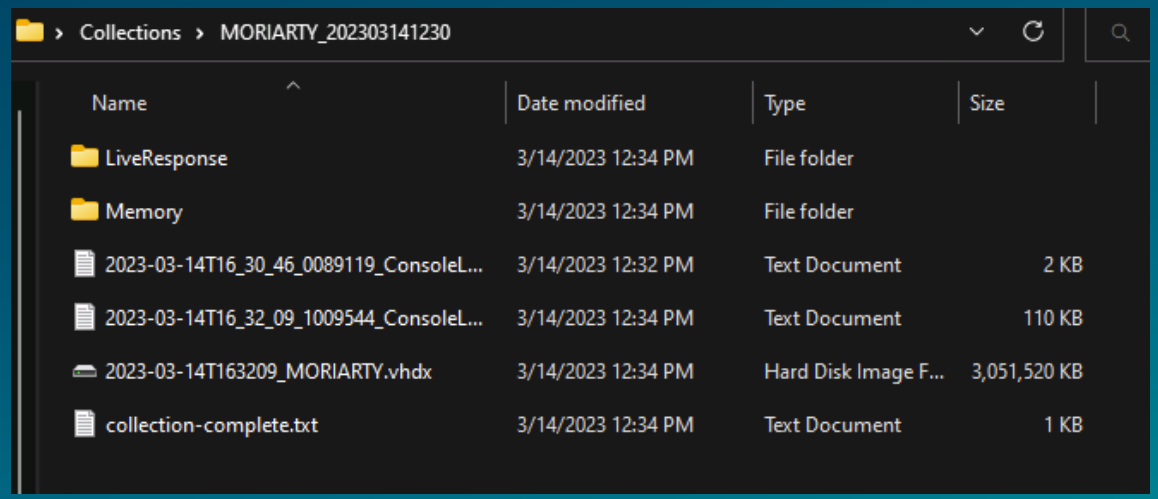


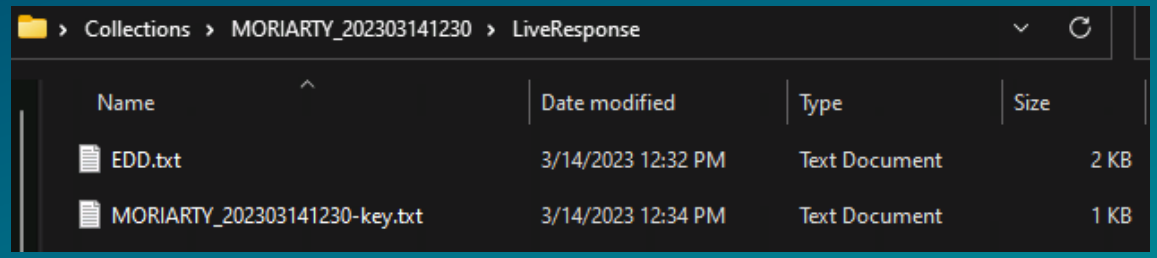
3. (2nd new window) Triage Collection

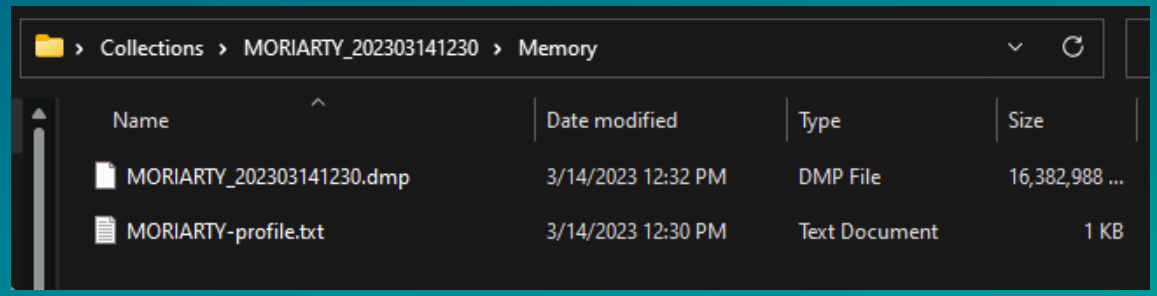


4. Clean-up and Complete

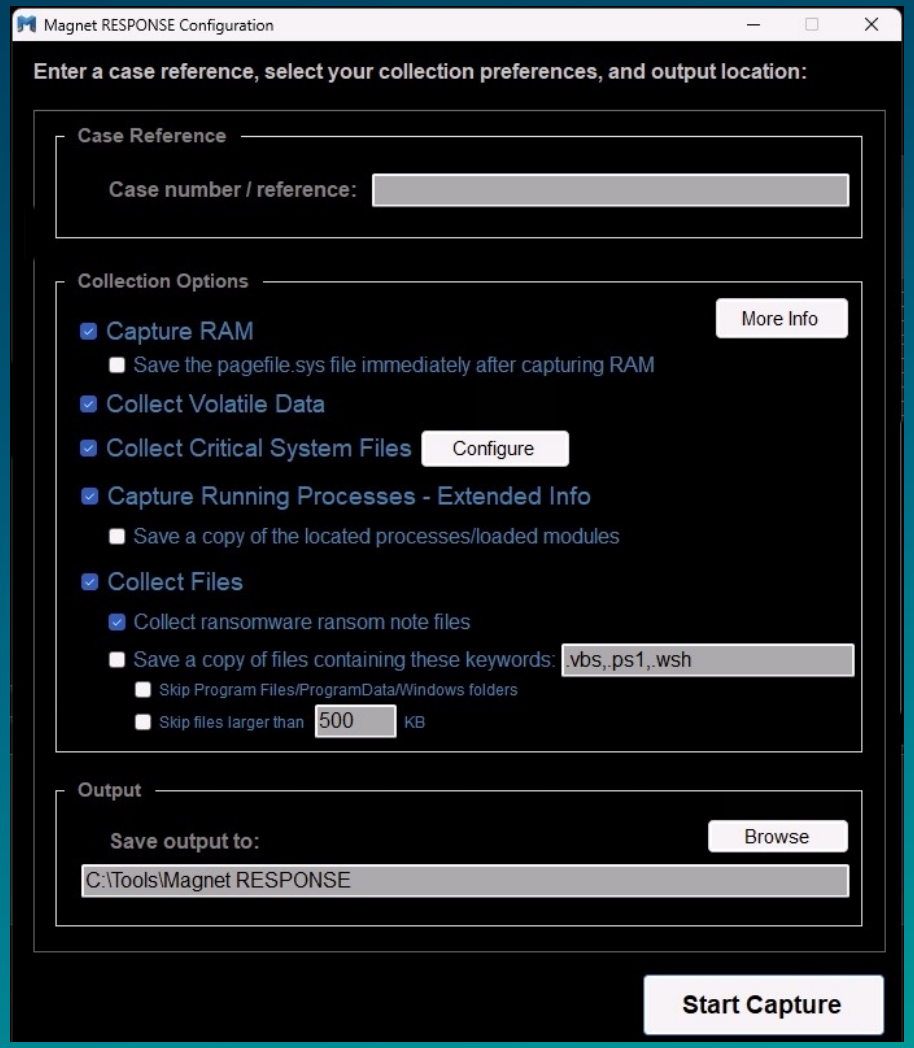
CyberPipe Output







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/

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 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 – no need for multiple tools to get the IR data you need

•Portable: It is compromised 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.

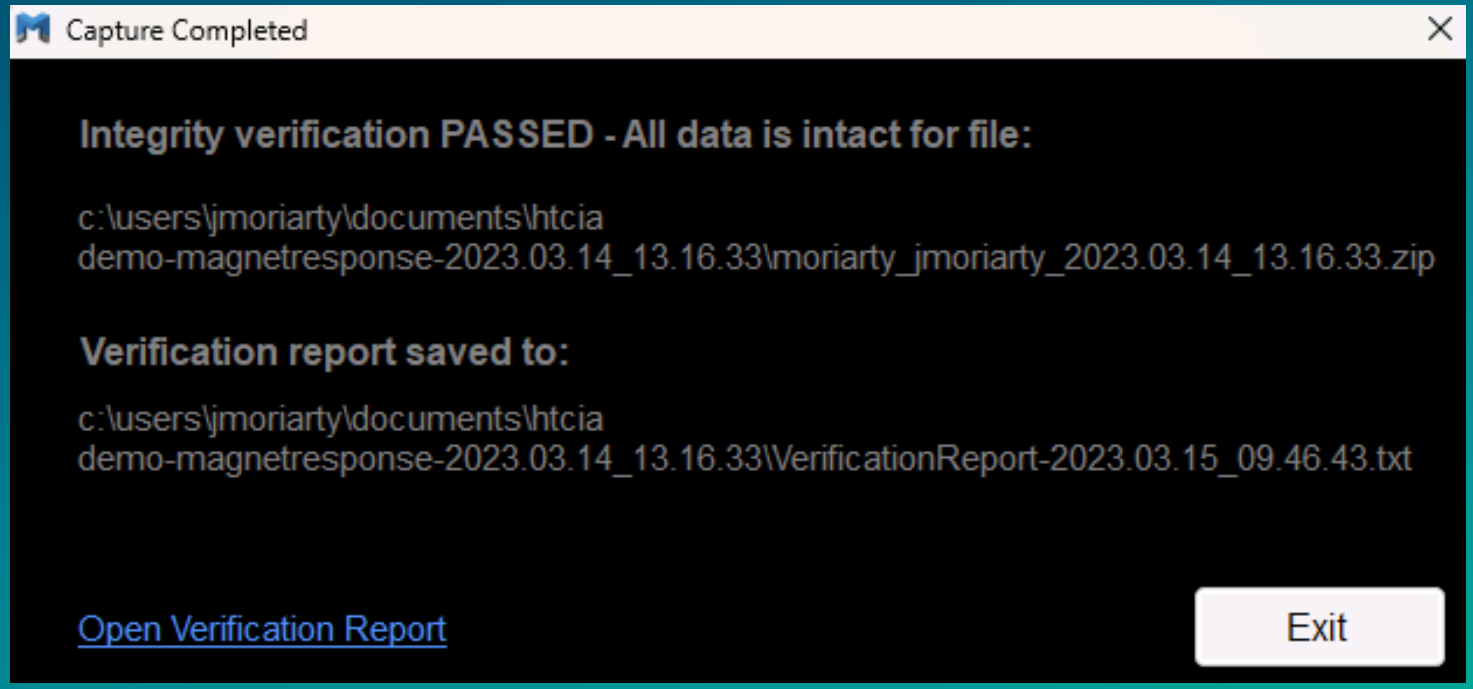
•Option 1 - Capture Everything Rename the executable to have the text "AutoCapture" (no quotes) anywhere in the filename. All options will be enabled, and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs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

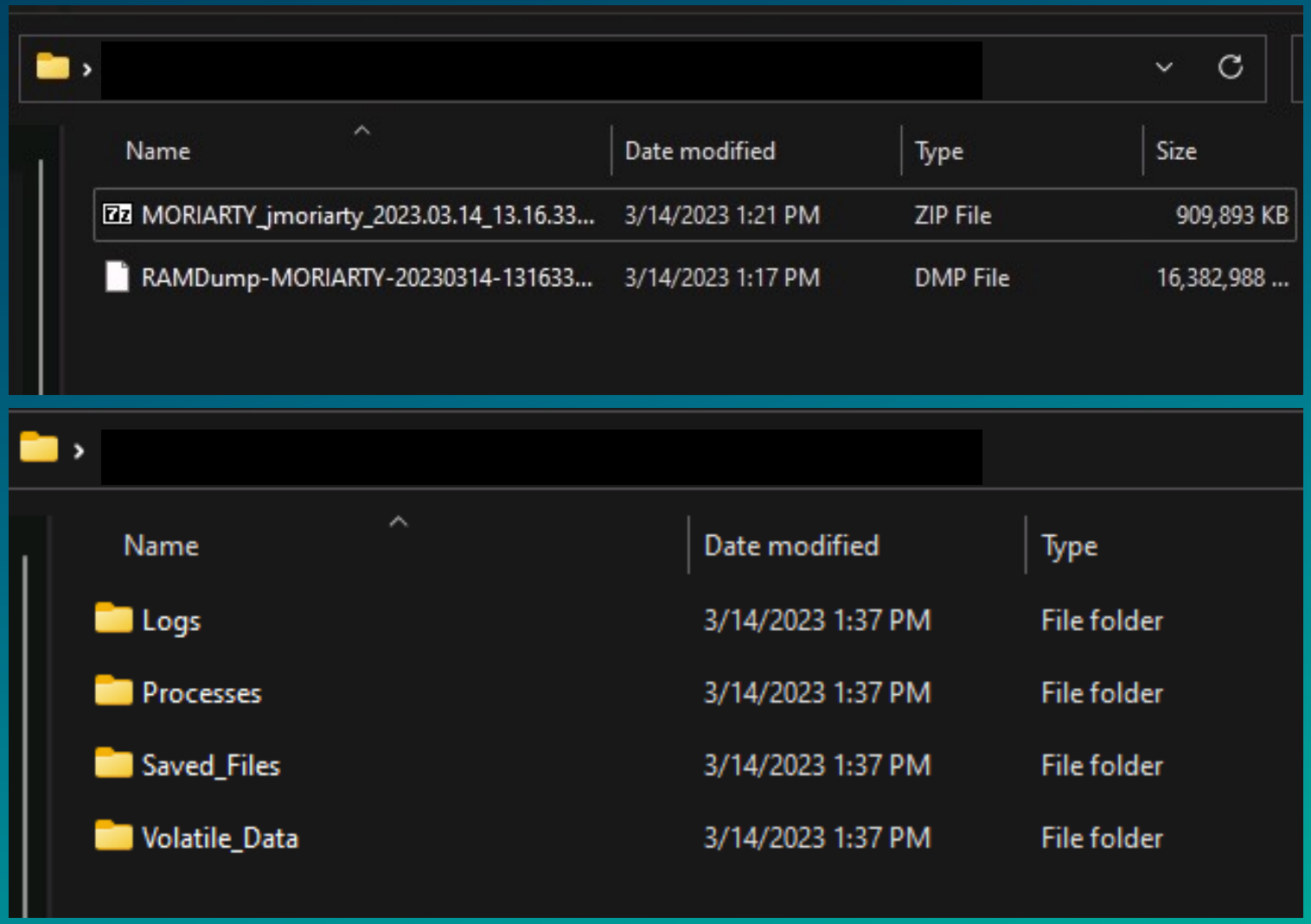
Magnet RESPONSE

Verifying a Capture Package

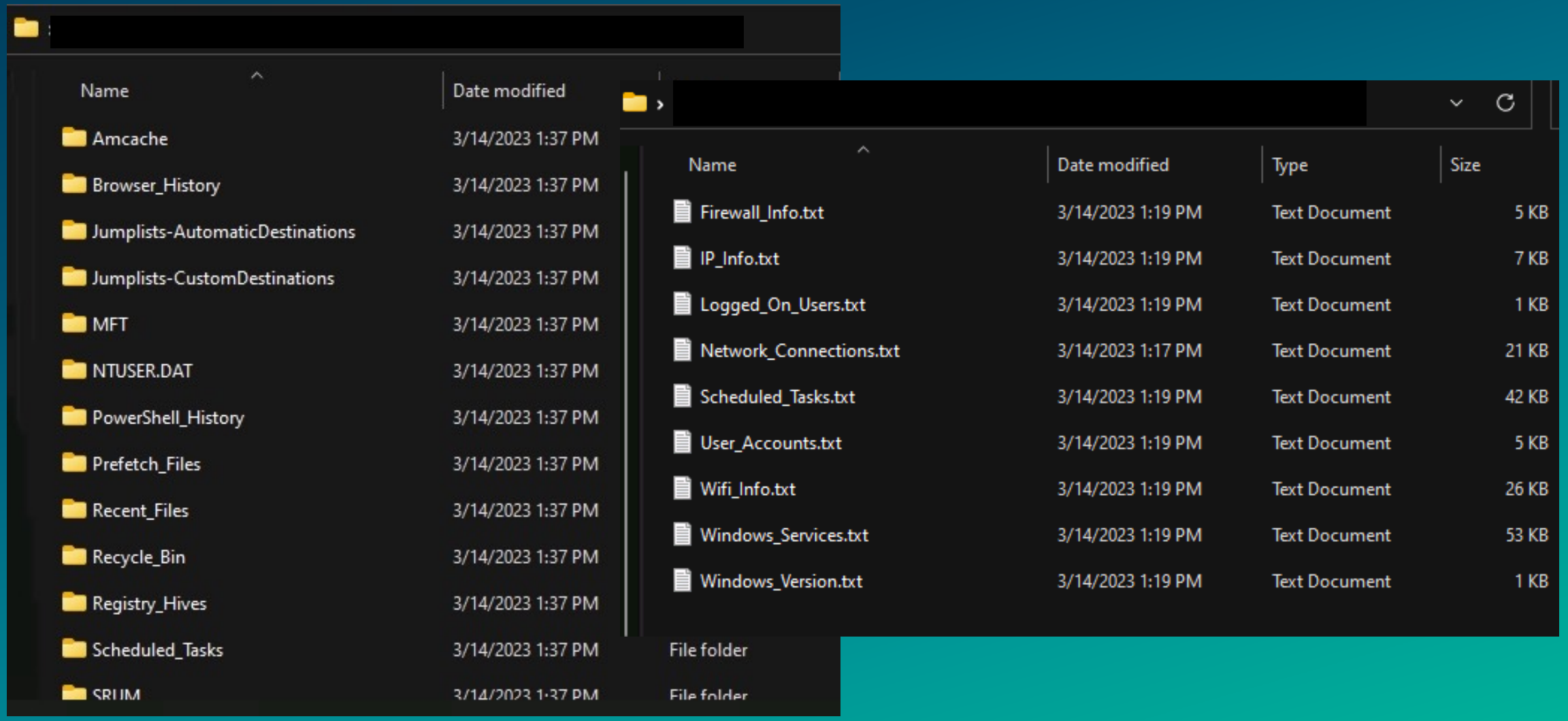
To verify the ZIP, simply drag and drop it on to the RESPONSE executable. RESPONSE will launch as normal and go directly into a verification process, providing a message at the end indicating if the verification was successful. A text file containing details of the verification is saved to the same folder.



Magnet RESPONSE Output



Magnet RESPONSE Output



Name	Date modified	Type	Size
Amcache	3/14/2023 1:37 PM		
Browser_History	3/14/2023 1:37 PM		
Jumplists-AutomaticDestinations	3/14/2023 1:37 PM		
Jumplists-CustomDestinations	3/14/2023 1:37 PM		
MFT	3/14/2023 1:37 PM		
NTUSER.DAT	3/14/2023 1:37 PM		
PowerShell_History	3/14/2023 1:37 PM		
Prefetch_Files	3/14/2023 1:37 PM		
Recent_Files	3/14/2023 1:37 PM		
Recycle_Bin	3/14/2023 1:37 PM		
Registry_Hives	3/14/2023 1:37 PM		
Scheduled_Tasks	3/14/2023 1:37 PM	File folder	
SRUM	3/14/2023 1:37 PM	File folder	

Name	Date modified	Type	Size
Firewall_Info.txt	3/14/2023 1:19 PM	Text Document	5 KB
IP_Info.txt	3/14/2023 1:19 PM	Text Document	7 KB
Logged_On_Users.txt	3/14/2023 1:19 PM	Text Document	1 KB
Network_Connections.txt	3/14/2023 1:17 PM	Text Document	21 KB
Scheduled_Tasks.txt	3/14/2023 1:19 PM	Text Document	42 KB
User_Accounts.txt	3/14/2023 1:19 PM	Text Document	5 KB
Wifi_Info.txt	3/14/2023 1:19 PM	Text Document	26 KB
Windows_Services.txt	3/14/2023 1:19 PM	Text Document	53 KB
Windows_Version.txt	3/14/2023 1:19 PM	Text Document	1 KB

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.

THANK YOU

MAGNET FORENSICS

https://github.com/dwmetz

https://bakerstreetforensics.com

doug.metz@magnetforensics.com

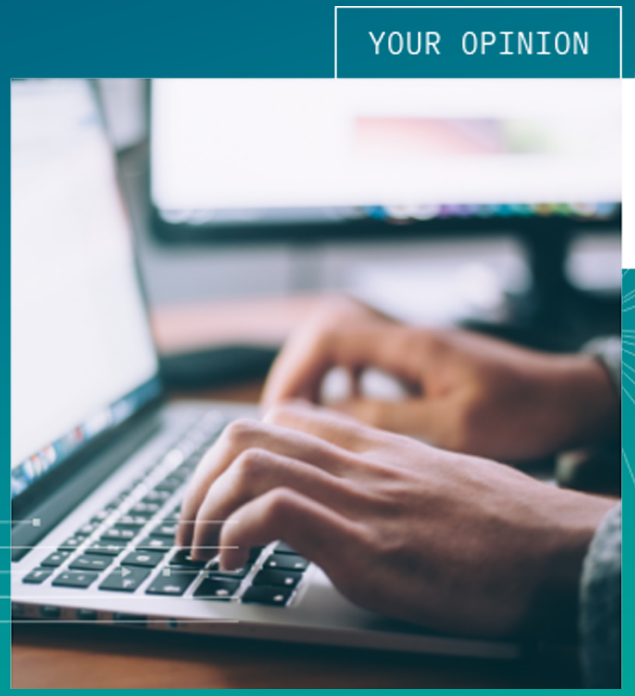
https://www.linkedin.com/in/dwmetz/

https://infosec.exchange/@dwmetz

@dwmetz

SURVEY REMINDER

We want your feedback! Please log in to your Event Portal and complete a survey for this session, located on the SURVEYS page.



MAGNET USER SUMMIT 2023

NASHVILLE | MAGNETUSERSUMMIT.COM | #MUS2023