



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



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.

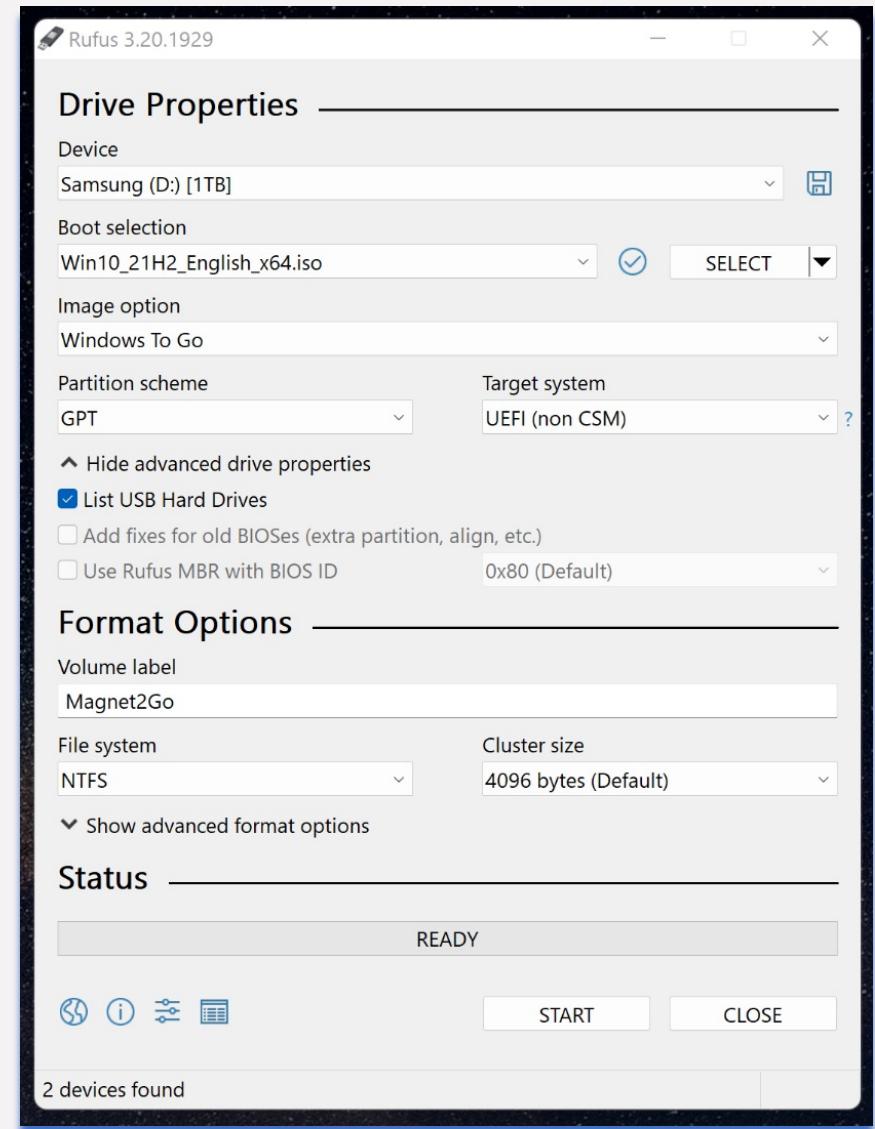
- **Device** The USB drive you want to use for Magnet2Go
- **Boot selection** Browse to and select the Window .iso file
- **Image option** Select **Windows to Go**

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**

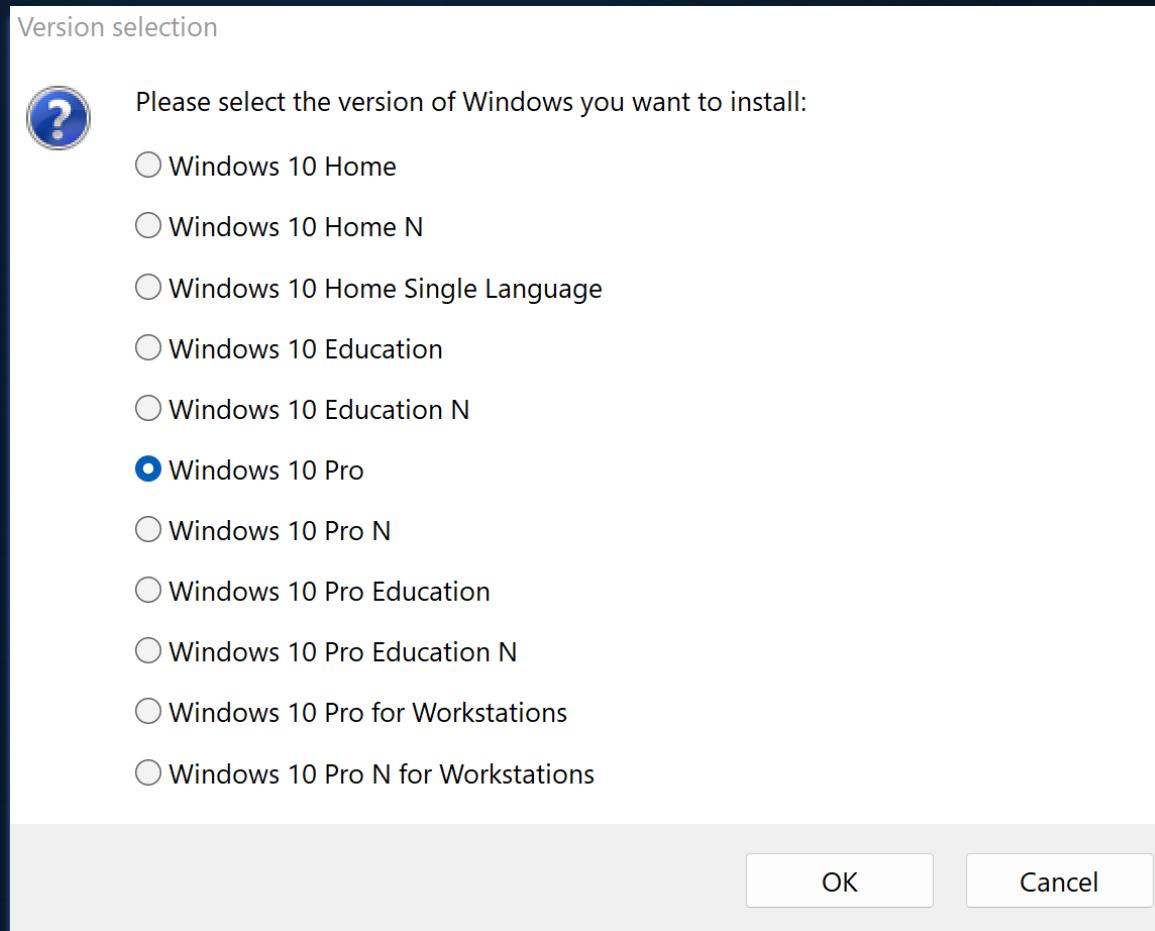
Triple check your settings and then press Start.

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



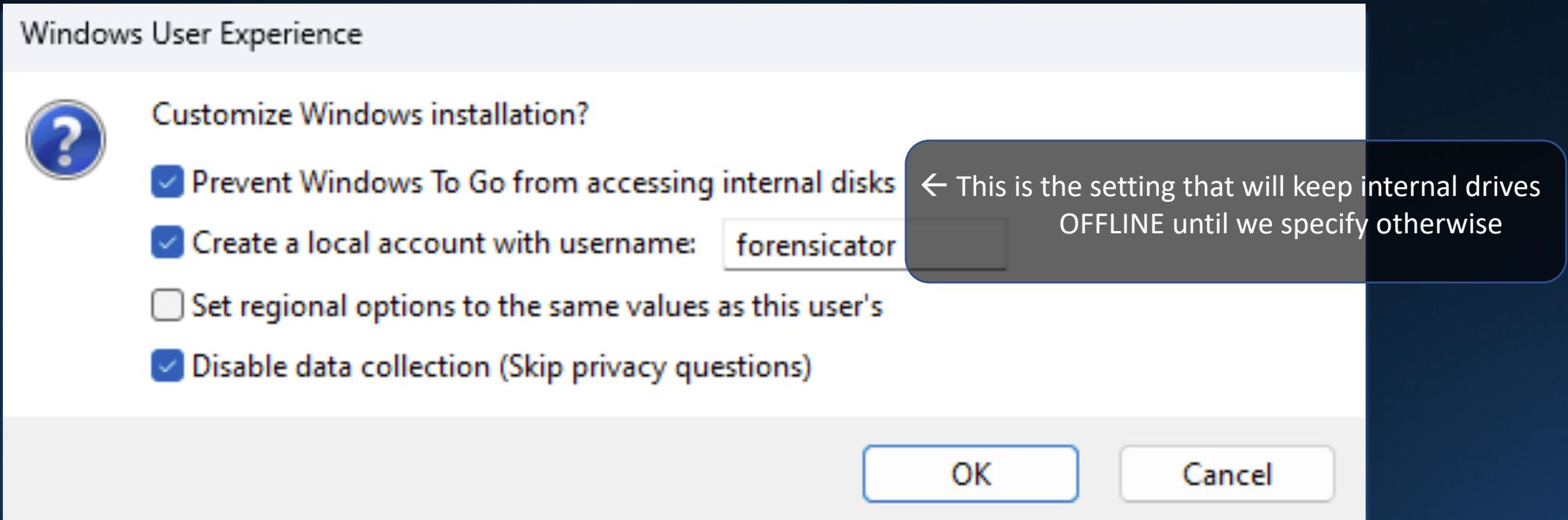


Windows Version



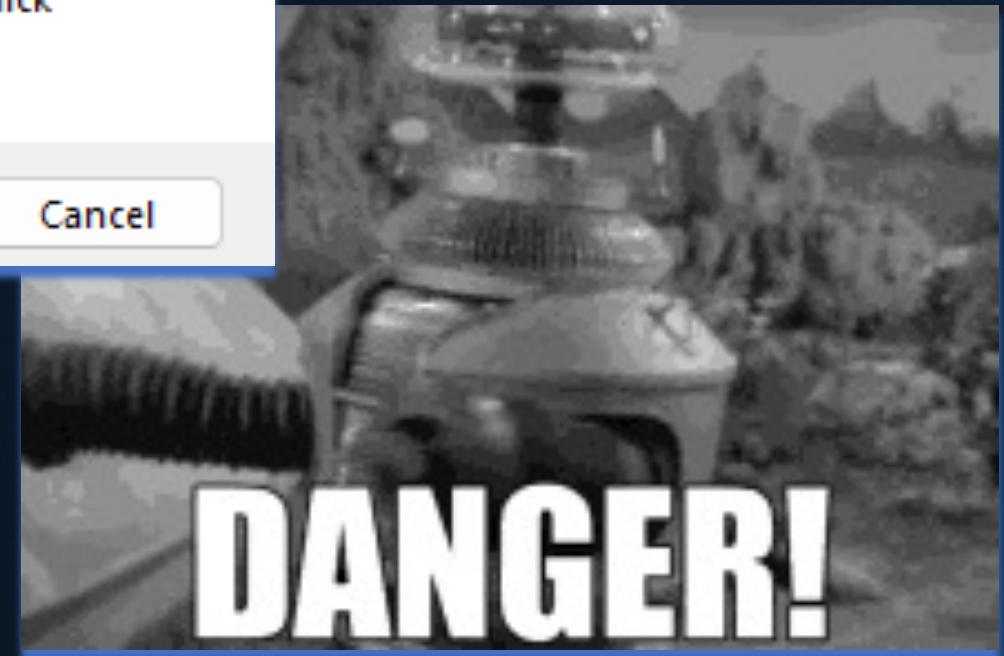
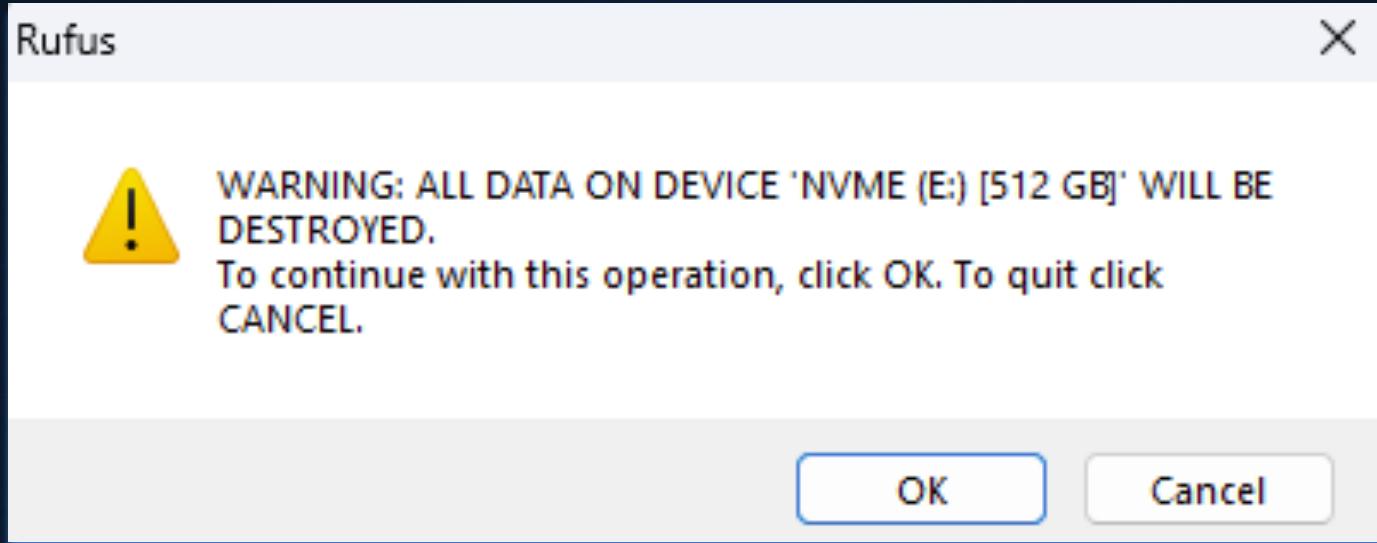


W U X





Danger, Will Robinson

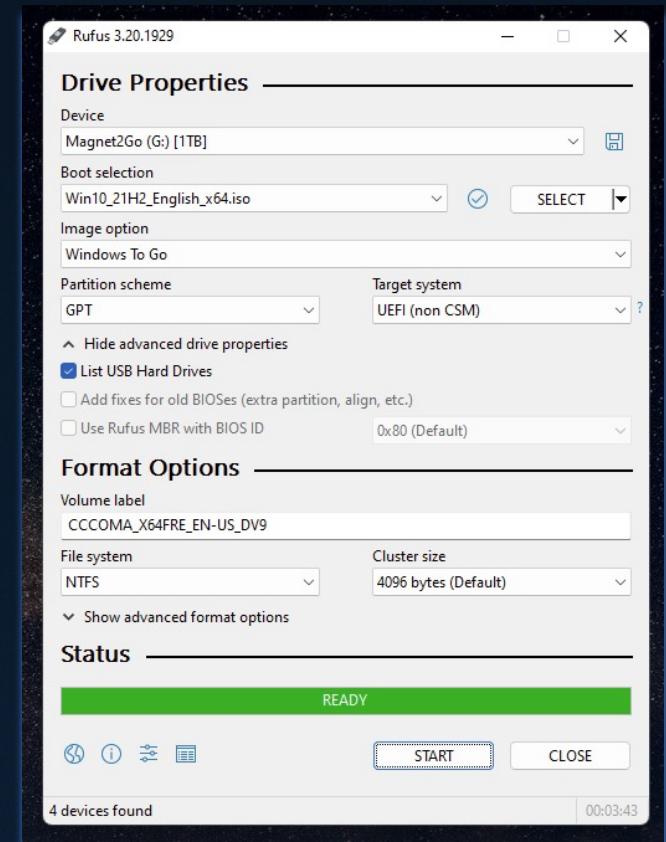
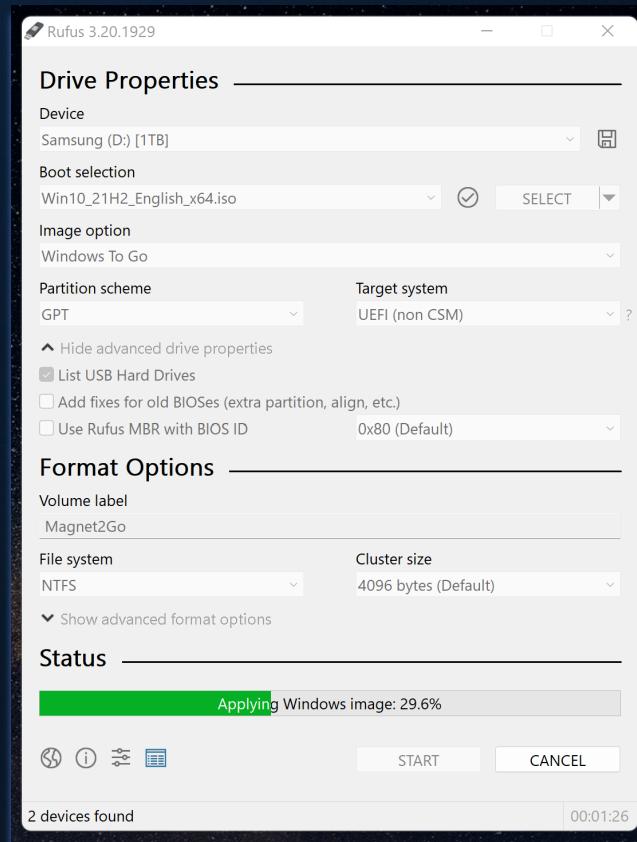
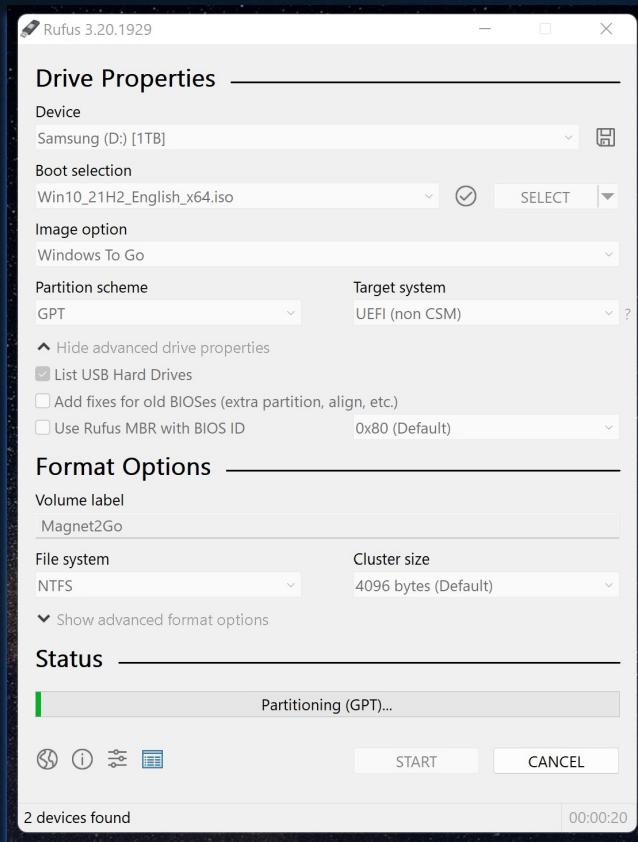




Partitioning...

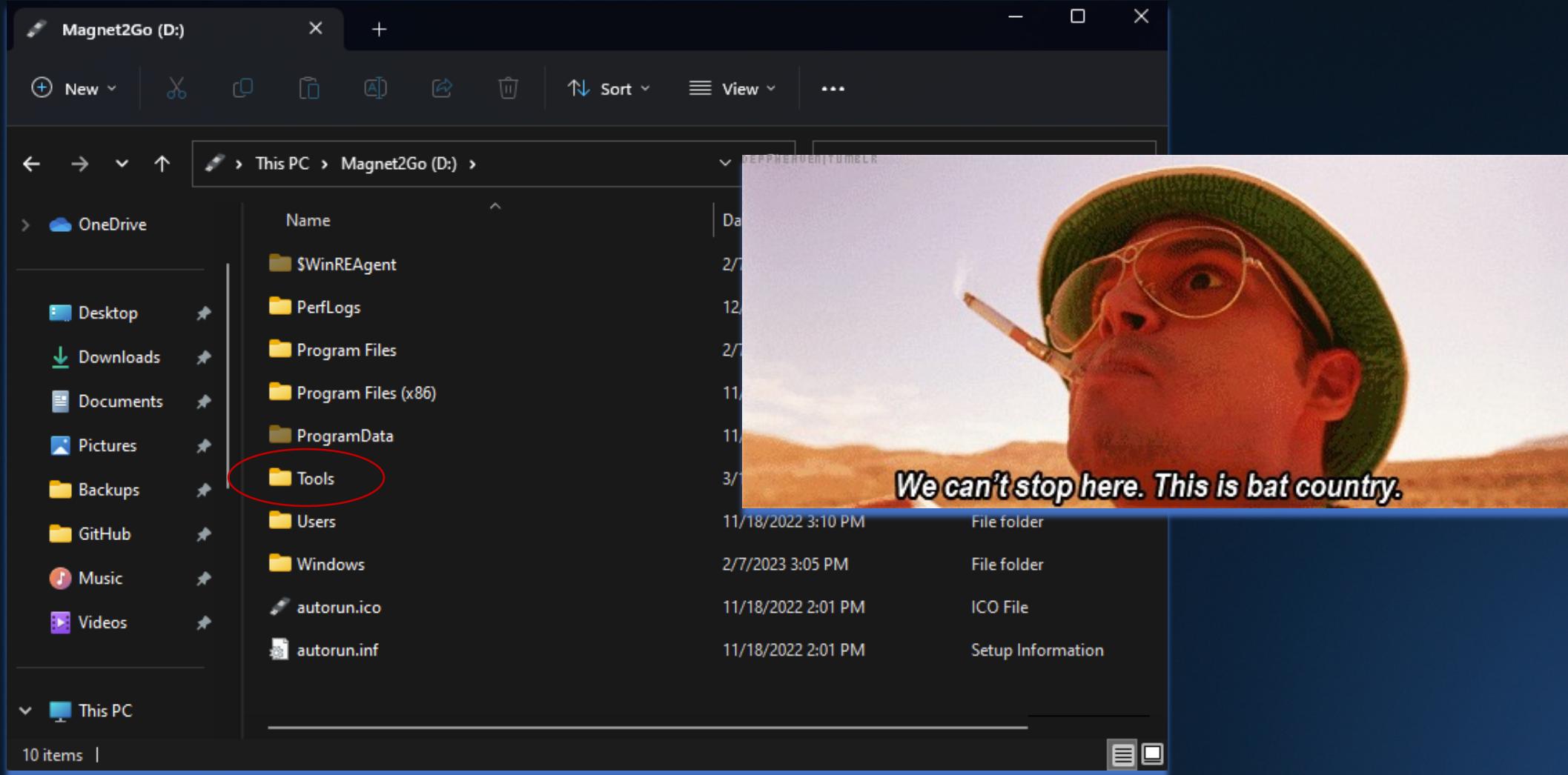
Applying Image...

Complete.





Before You Go On...





Tools Directory

The screenshot shows a Windows File Explorer window titled 'Tools'. The path in the address bar is 'This PC > Magnet2Go (D:) > Tools >'. The left sidebar shows standard folder icons for OneDrive, Desktop, Downloads, Documents, Pictures, Backups, GitHub, Music, and Videos. The main pane displays a list of files and folders:

Name	Date modified	Type	Size
.Help	2/7/2023 2:54 PM	File folder	
7zip	1/25/2023 12:41 PM	File folder	
Arsenal-Image-Mounter	11/18/2022 2:03 PM	File folder	
Customization	3/13/2023 10:04 AM	File folder	
Keywords	11/18/2022 2:03 PM	File folder	
Live-Response	3/13/2023 10:21 AM	File folder	
Magnet ACQUIRE	11/18/2022 3:49 PM	File folder	
Magnet OUTRIDER	3/13/2023 3:55 PM	File folder	
Magnet2Go Build Instructions.docx	10/24/2022 9:07 AM	Microsoft Word D...	1,592 KB
VC_redist.x64.exe	10/10/2022 5:26 PM	Application	24,636 KB



Live Response Tools

The screenshot shows a file explorer window titled "Live-Response". The path in the address bar is "Magnet2Go (D:) > Tools > Live-Response". The left sidebar shows a navigation tree with OneDrive, Desktop, Downloads, Documents, Pictures, Backups, GitHub, Music, and Videos. The main pane displays a list of files and folders:

Name	Date modified	Type	Size
KAPE	2/7/2023 3:29 PM	File folder	
Magnet_Dumpl	11/29/2022 1:05 PM	File folder	
Magnet_EDD	11/18/2022 2:03 PM	File folder	
Magnet_PROCESS_Capture	11/18/2022 2:03 PM	File folder	
Magnet_RAM_Capture	1/25/2023 12:41 PM	File folder	
Magnet_RESPONSE	3/13/2023 9:55 AM	File folder	
Magnet_WebPageSaver	11/18/2022 2:03 PM	File folder	
Mal-Hash	3/13/2023 10:18 AM	File folder	
Sysinternals	11/18/2022 2:03 PM	File folder	
CyberPipe.ps1	1/23/2023 7:02 AM	Windows PowerS...	8 KB

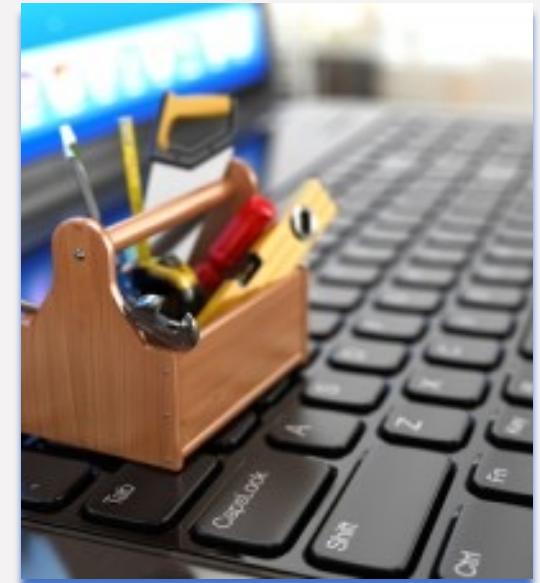


Suggested Tools

- 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 of 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

PhoenixBIOS Setup Utility

Main Advanced Security Boot Exit

CD-ROM Drive
+Removable Devices
+Hard Drive
Network boot from Intel E1000e

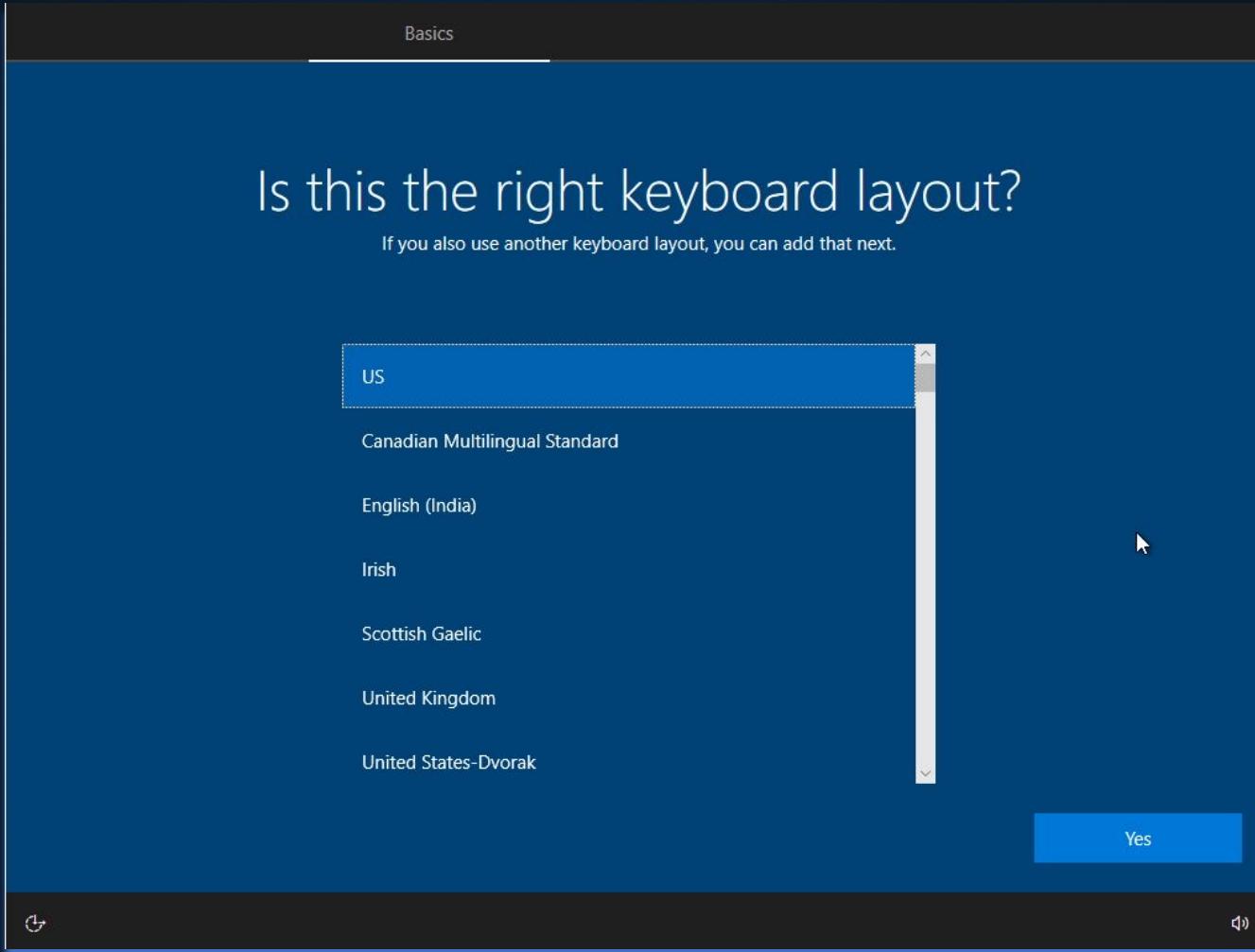
Item Specific Help

Keys used to view or configure devices:
<Enter> expands or collapses devices with a + or -
<Ctrl+Enter> expands all
<+> and <-> moves the device up or down.
<n> May move removable device between Hard Disk or Removable Disk
<d> Remove a device that is not installed.

F1 Help ↑ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit ↔ Select Menu Enter Select ▶ Sub-Menu F10 Save and Exit



First Boot (Setup)





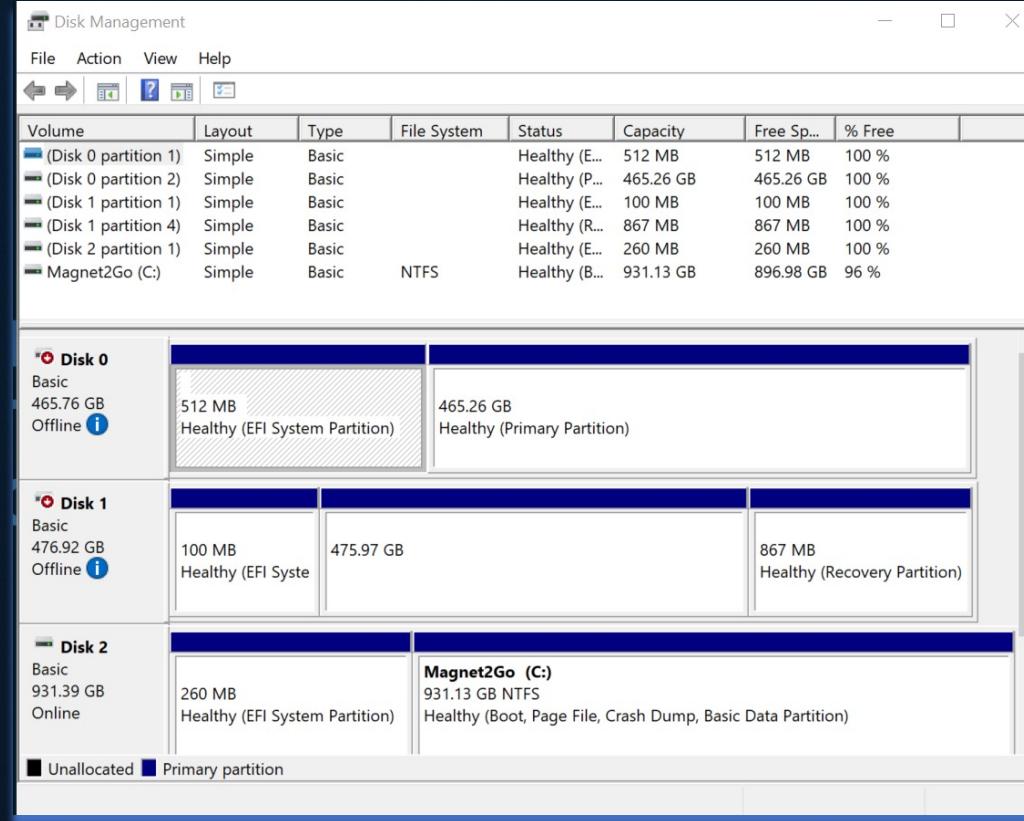
First Boot (Windows Configuration)

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.

```
C:\Windows\system32\diskpart.exe
Microsoft DiskPart version 10.0.19041.964

Copyright (C) Microsoft Corporation.
On computer: DESKTOP-FT734FO

DISKPART> list disk

Disk ### Status Size Free Dyn Gpt
----- -----
Disk 0 Offline 465 GB 1024 KB *
Disk 1 Offline 476 GB 3072 KB *
Disk 2 Online 931 GB 0 B *

DISKPART> select disk 1

Disk 1 is now the selected disk.

DISKPART> attributes disk set readonly

Disk attributes set successfully.

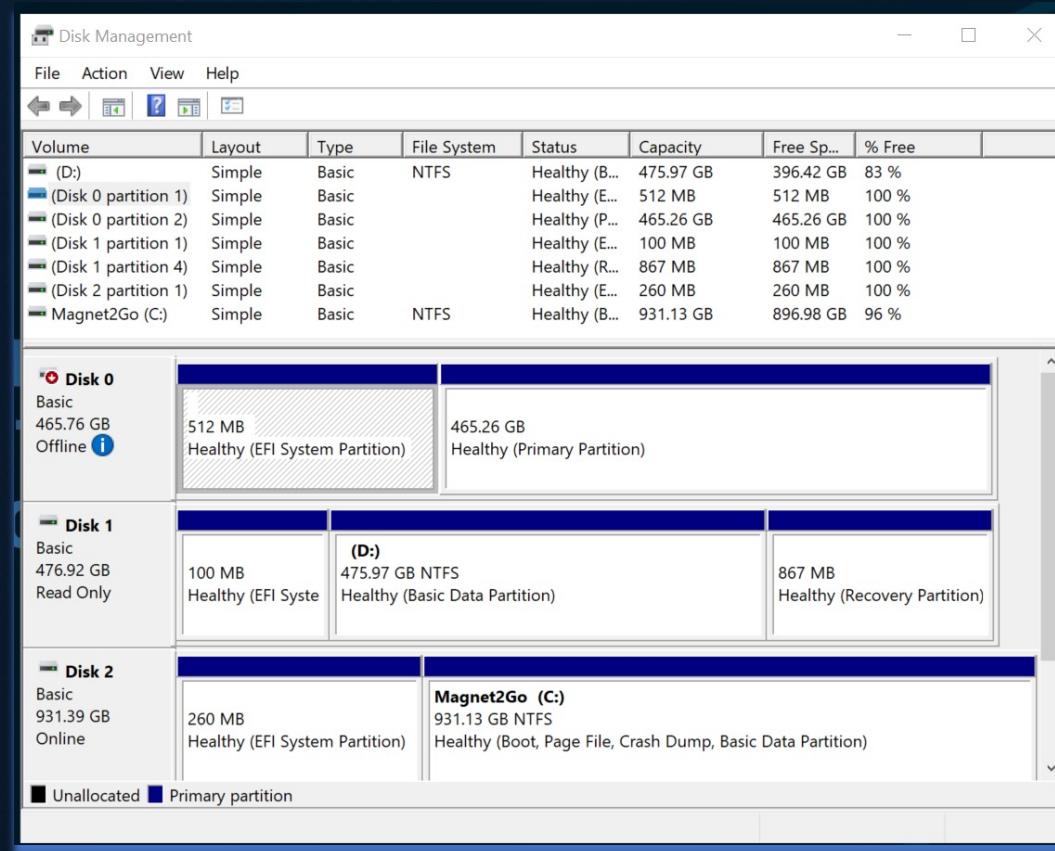
DISKPART> online disk

DiskPart successfully onlined the selected disk.

DISKPART>
```



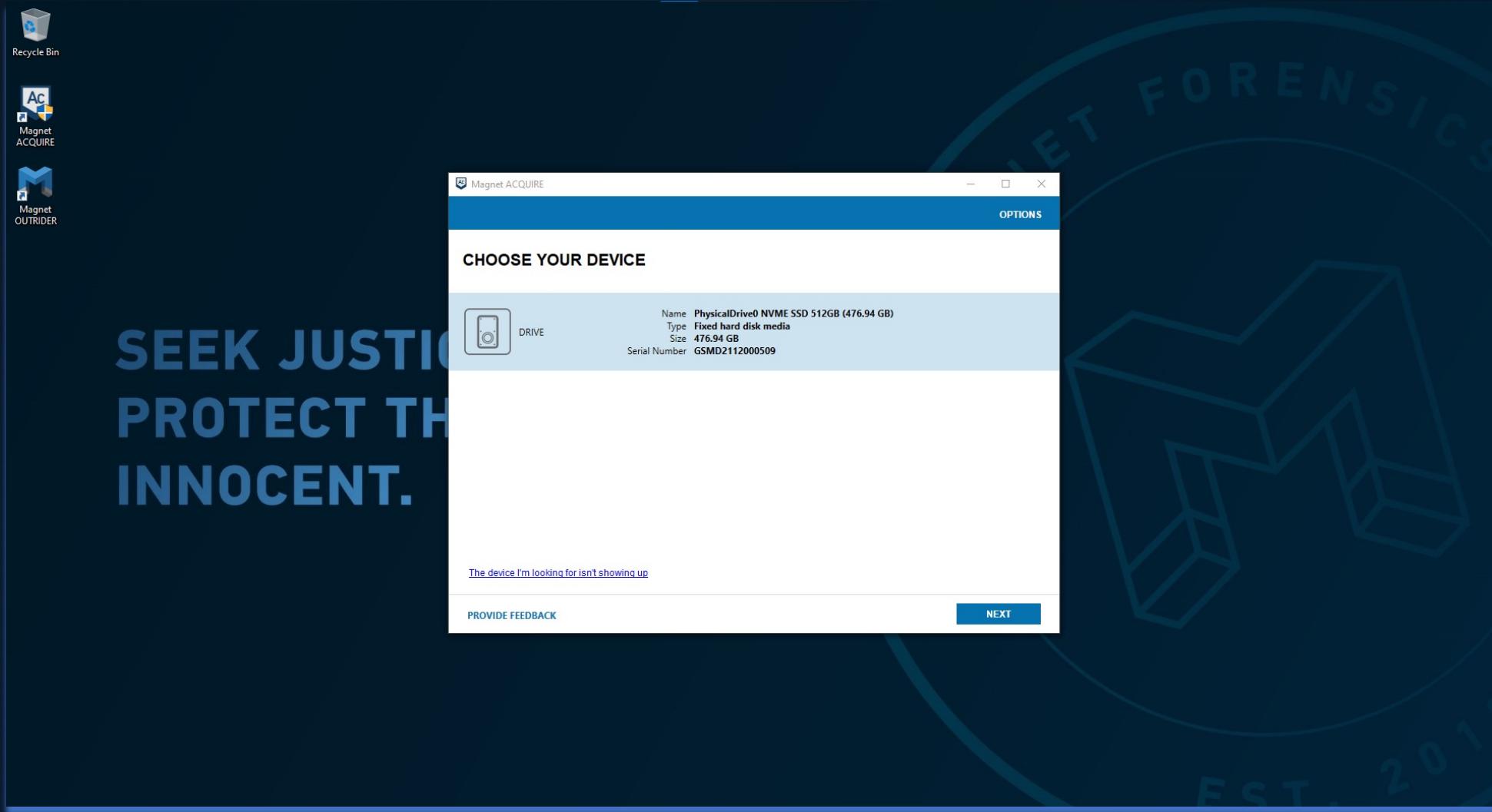
Verify READ-ONLY



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.

The screenshot shows the Magnet OUTRIDER v3.3.0 software interface. The main window title is "MAGNET OUTRIDER". The top navigation bar includes "MANAGE" and "ABOUT" buttons. On the left, a sidebar menu has "Scan progress" selected. Under "Scan progress", there's a "Critical hits" section with a red exclamation mark icon. Below it is a "Scan summary" section. A "LOCATED APPLICATIONS" section is expanded, showing the following table:

Critical Hits	Count
Anti-Forensic Files	2
Cloud Files	1
Collect Files	0
Cryptocurrency Files	0
Dark Web Files	1
Encryption Files	0
Gaming Files	0
Messaging Files	5
P2P Files	0
VM Files	0

At the bottom of the sidebar, the elapsed time is listed as "Elapsed time: 00:00:25". To the right of the sidebar, a large blue circle contains the text "Scan complete", "HITS FOUND!", and "Click on the category names to view hits.". At the bottom right of the main area is a blue button labeled "OPEN REPORT".



Live Response

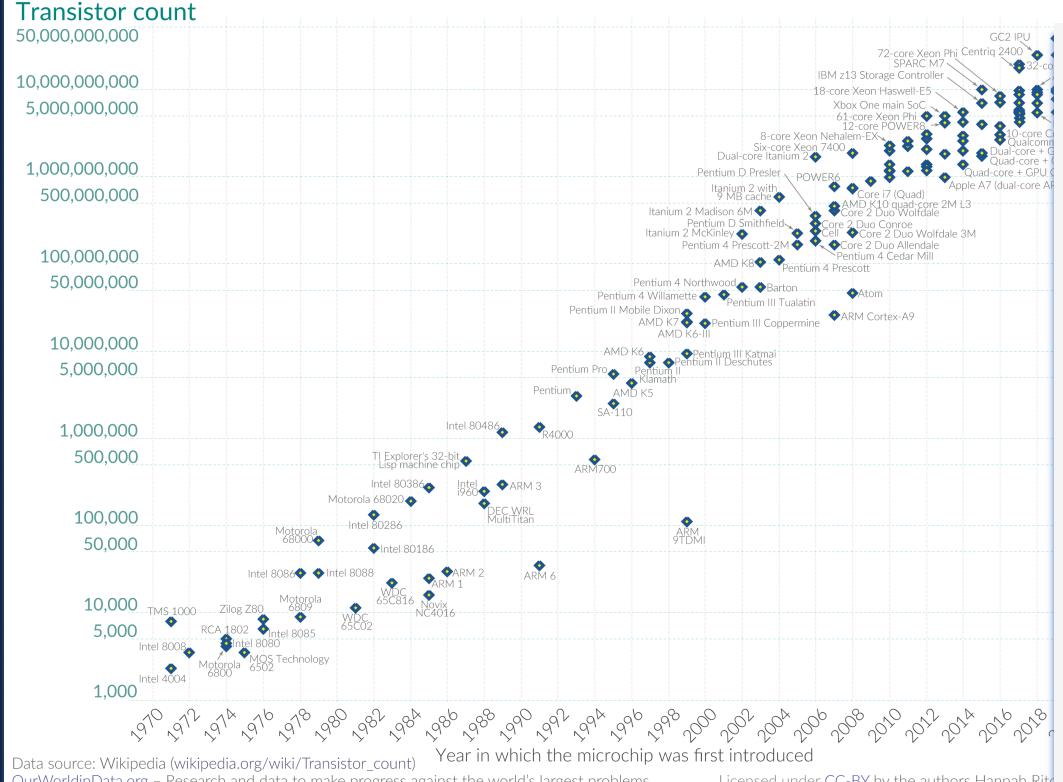
Triage collections for On and Off Network



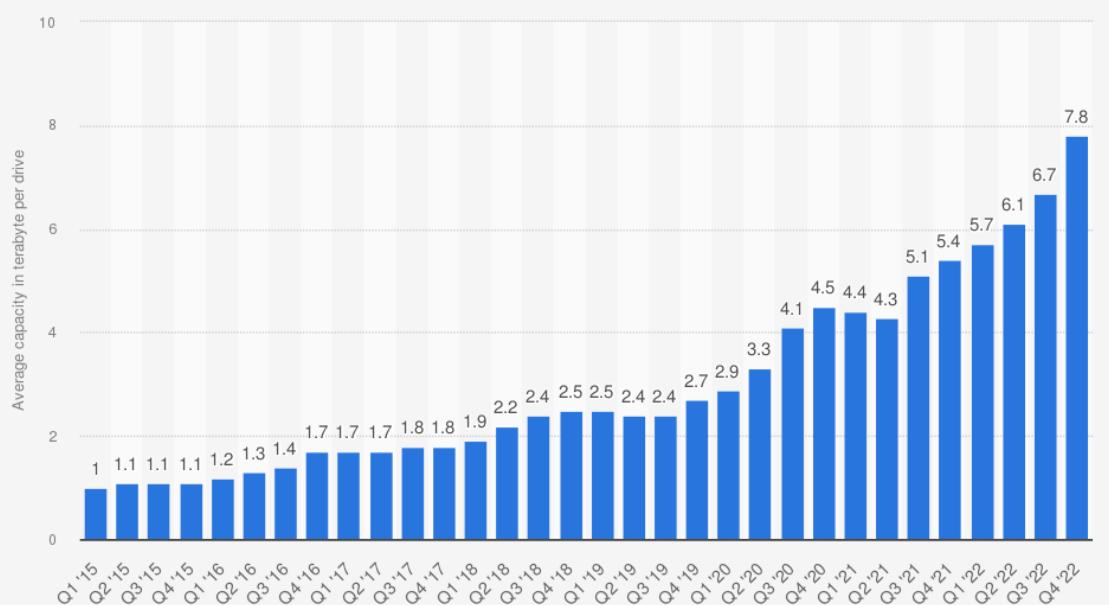
Magnitudes of Data

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:

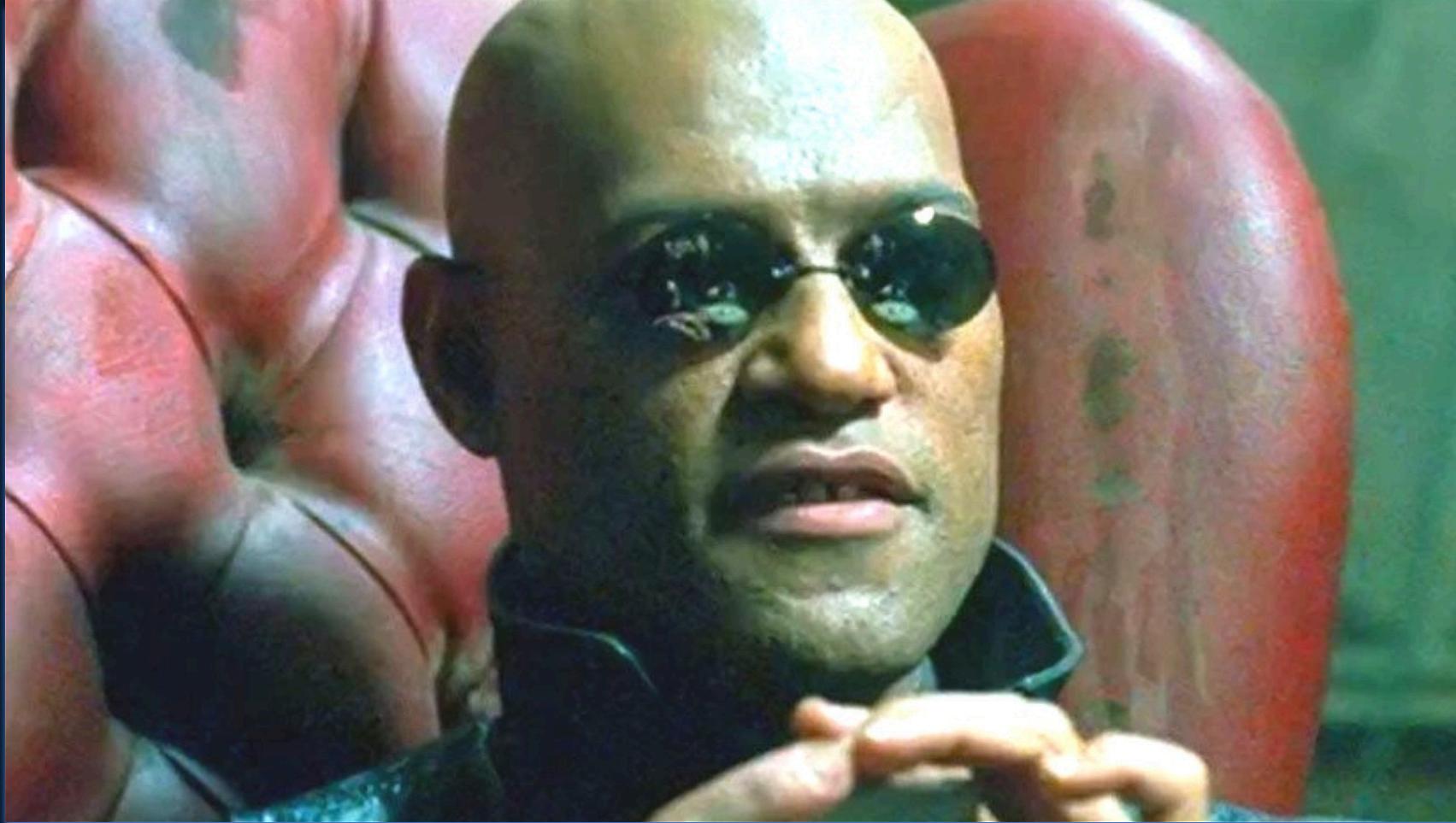
https://en.wikipedia.org/wiki/Moore%27s_law#/

<https://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



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



Online Triage Acquisition

- Magnet IGNITE
- Magnet AXIOM Cyber
- Magnet AUTOMATE Enterprise

SEEK JUSTICE. PROTECT THE INNOCENT.



MAGNET
FORENSICS®

The screenshot shows the Magnet IGNITE software interface. At the top, there's a navigation bar with 'MAGNET IGNITE' and 'CASE LIST'. Below it, the case name 'The Adventure of the Creeping...' and the collector name 'MORIARTY' are displayed. A search bar and an 'ADVANCED' button are also present. On the left, a sidebar titled 'COLLECTION INFORMATION' lists 'FILE ACTIVITY (2025)', 'FILE LOG (256391)', 'INCIDENT RESPONSE (816236)', 'INDICATORS OF COMPROMISE (204)', 'YARA RULES (204)' (which is currently selected), and 'REFINED RESULTS (98)'. The main panel is titled 'Yara Rules' and shows '204 Hits'. It lists numerous file paths, such as C:\Toolz\BloodHound-win32-x64\resources\app\node_modules\package-lock.json and C:\Users\jmorarity\Desktop\CyberPipe\KAPE\Modules\bin\RECmd\RegistryExplore\BatchExamples\RECmdBatch.guide. Navigation buttons at the bottom indicate pages 1 through 3.



Magnet Free Tools

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

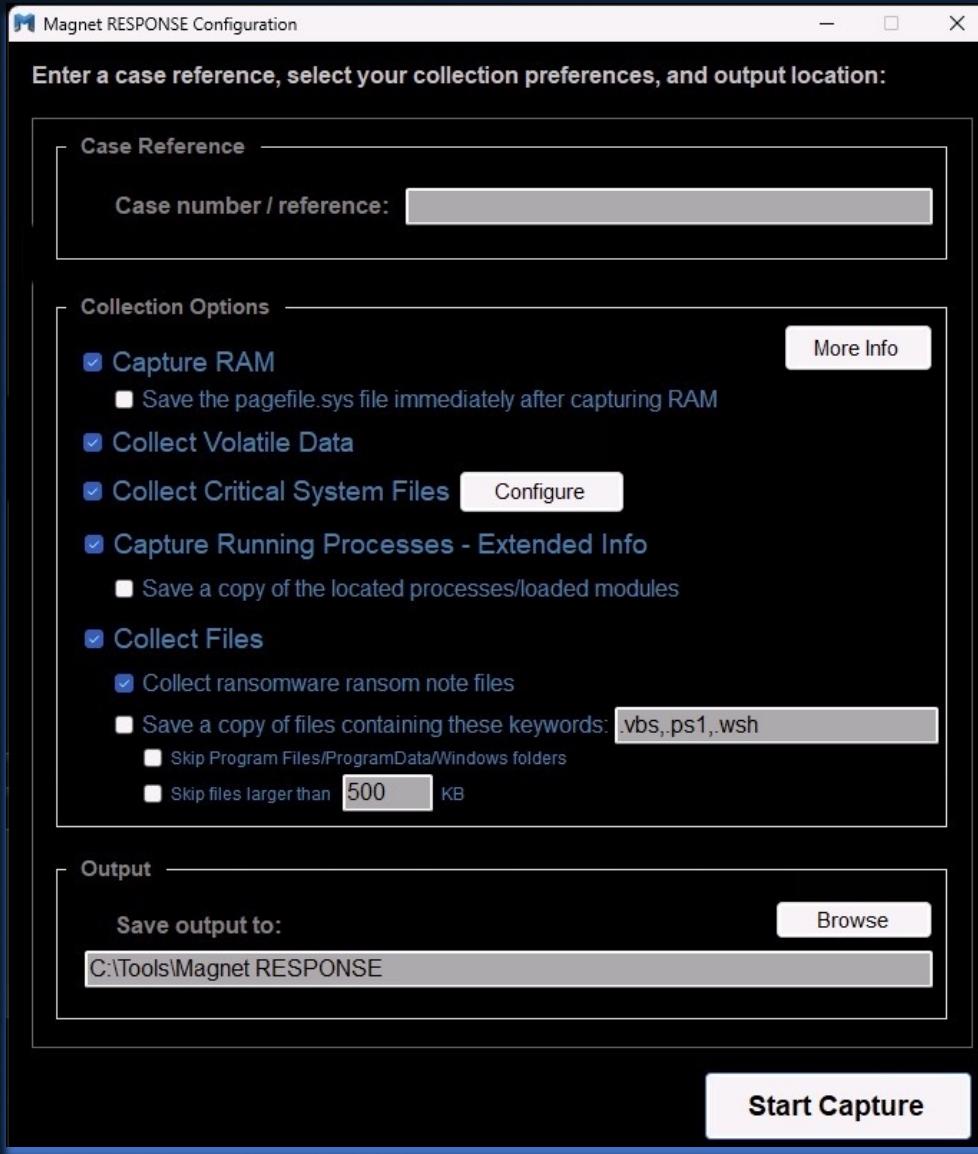


<https://www.magnetforensics.com/free-tools/>

The screenshot shows a web browser displaying the URL <https://support.magnetforensics.com/s/free-tools>. The page features the Magnet Forensics logo at the top left. A navigation bar with links to HOME, KNOWLEDGE BASE, TECH SUPPORT, ARTIFACT EXCHANGE, and More is visible. The main content area is titled "FREE TOOLS" and includes a sub-section for "MAGNET ACQUIRE". It lists the version as 2.47.0.28714 and the release date as 2022-01-25. A "DOWNLOAD" button is present, along with links for "RELEASE NOTES" and "System Requirements". Below this section is another for "MAGNET SHIELD", which is described as empowering frontline officers to collect and report on fleeting digital evidence. A "DOWNLOAD" button and a "LEARN MORE" link are provided. At the bottom of the page is a section for "MAGNET CHROMEBOOK ACQUISITION ASSISTANT", listing version 1.06 and release date 2021-11-21, with a note about acquiring logical images from Chromebooks. To the right of the main content, there is a sidebar titled "TOP ARTICLES" under the heading "FREE TOOLS", featuring links to various articles like "Generate wordlists with the AXIOM Wordlist Generator", "Acquire Memory with MAGNET RAM Capture", and "System requirements: Magnet ACQUIRE". A "View All (20+)" link is also present.



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/>

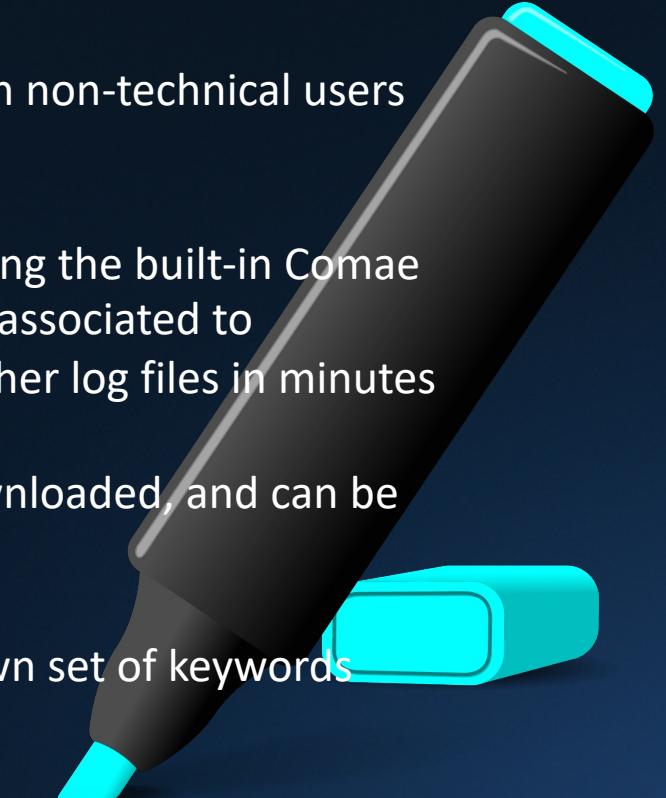
magnetforensics.com



Magnet RESPONSE

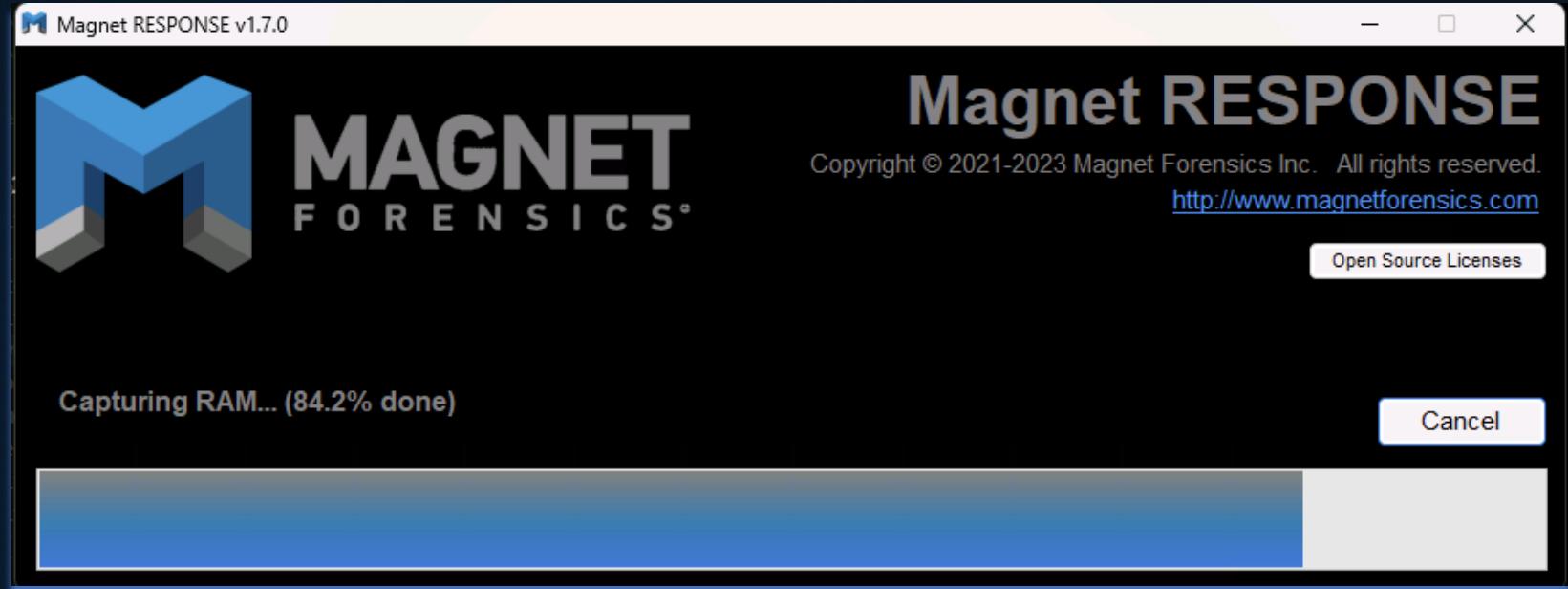
Highlights:

- 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 Dumpl) 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 comprised 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.

magnetforensics.com



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.

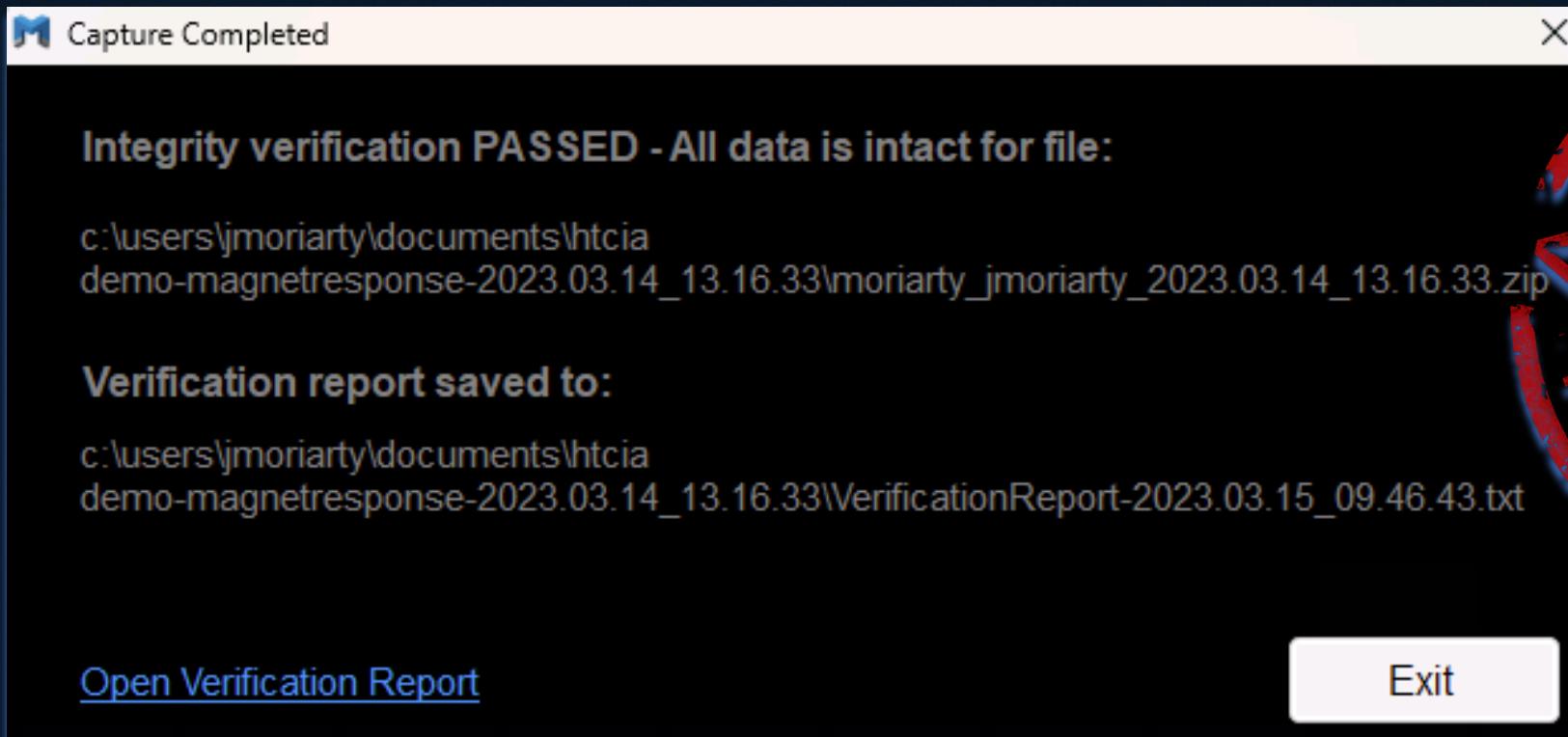
- Option 1 - Capture Everything Rename the executable to have the text "AutoCapture" (no quotes) anywhere in the filename. All options will be enabled, and the capture will commence without prompting for any configuration from the user. The captured data will be saved to the folder the executable runs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

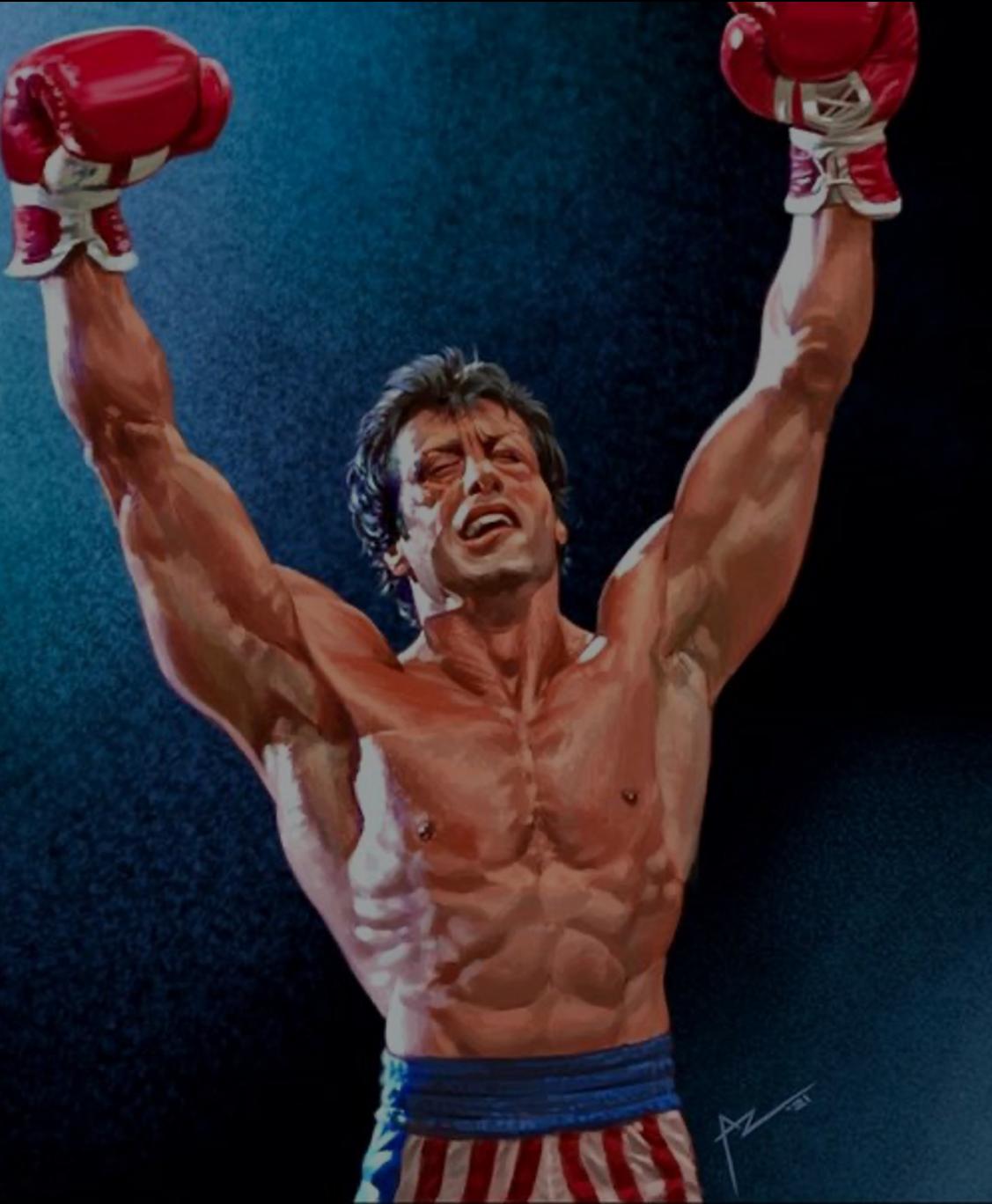


Magnet RESPONSE

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.





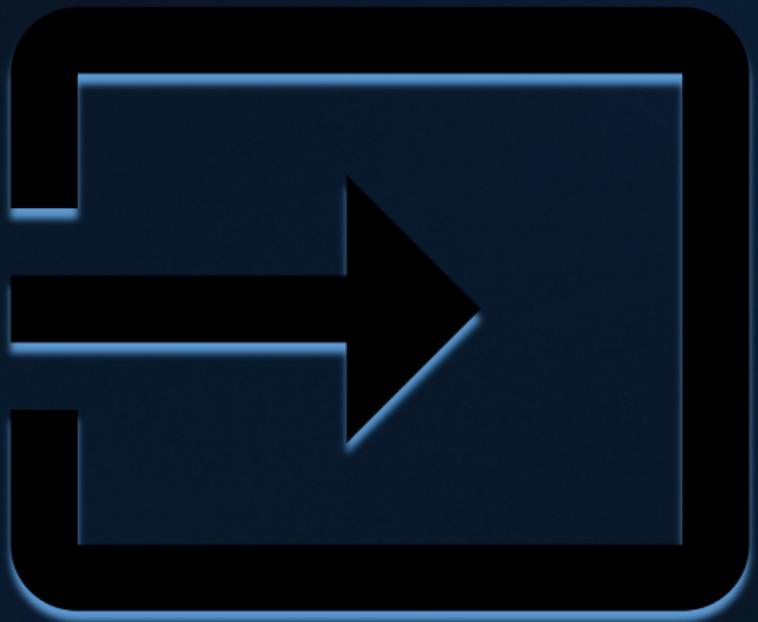
HARDWARE CHOICES

- Samsung T5 or T7





Magnet RESPONSE Output



HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33			
Name	Date modified	Type	Size
7z MORIARTY_jmoriarty_2023.03.14_13.16.33...	3/14/2023 1:21 PM	ZIP File	909,893 KB
DMP RAMDump-MORIARTY-20230314-131633...	3/14/2023 1:17 PM	DMP File	16,382,988 ...

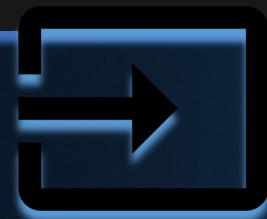
HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 > extracted >			
Name	Date modified	Type	
Logs	3/14/2023 1:37 PM	File folder	
Processes	3/14/2023 1:37 PM	File folder	
Saved_Files	3/14/2023 1:37 PM	File folder	
Volatile_Data	3/14/2023 1:37 PM	File folder	



Magnet RESPONSE Output

SEEK JUSTICE. PROTECT THE INNOCENT.

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			



magnetforensics.com

Evidence Processing Tips





Memory Processing

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet AXIOM Process 5.2.0.25407

File Tools Help

EVIDENCE SOURCES

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

WINDOWS SELECT EVIDENCE SOURCE

DRIVE IMAGE FILES & FOLDERS VOLUME SHADOW COPY MEMORY

Magnet AXIOM Process 7.1.0.35864

File Tools Help

EVIDENCE SOURCES

CASE DETAILS

EVIDENCE SOURCES

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption
- Add keywords to search
- Extract text from files (OCR)
- Calculate hashes and find matches On
- Analyze chats with MagnetAI
- Analyze pictures with MagnetAI
- Add CPS data to search
- Search with YARA rules
- Find more artifacts

ARTIFACT DETAILS 0

- Mobile artifacts
- Cloud artifacts
- Computer artifacts
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

WINDOWS SELECT MEMORY PLUG-IN

Based on the evidence source, you can use the memory plug-ins below. Using different memory plug-ins may return different results. For more information, review the [Selecting memory plug-in with AXIOM Cyber](#) article.

COMAE VOLATILITY

BACK NEXT



Image Processing

Computer > Windows > Load Evidence > IMAGE

The screenshot displays two windows of the Magnet AXIOM Process software.

Top Window: SELECT EVIDENCE SOURCE

- CASE DETAILS:** EVIDENCE SOURCES (1)
- PROCESSING DETAILS:** Search archives and mobile backups (On), Decode file-based encryption, Add keywords to search, Extract text from files (OCR), Calculate hashes and find matches (On), Analyze chats with Magnet.AI, Analyze pictures with Magnet.AI, Add CPS data to search, Search with YARA rules, Find more artifacts.
- ARTIFACT DETAILS:** 221 artifacts (Mobile artifacts, Cloud artifacts, Computer artifacts 221 of 271, Vehicle artifacts, Parse and carve artifacts, Privileged content, Date range filter).
- ANALYZE EVIDENCE:**

Bottom Window: ADD FILES AND FOLDERS

- CASE DETAILS:** EVIDENCE SOURCES (1)
- PROCESSING DETAILS:** Search archives and mobile backups (On), Decode file-based encryption, Add keywords to search, Extract text from files (OCR), Calculate hashes and find matches (On), Analyze chats with Magnet.AI, Analyze pictures with Magnet.AI, Add CPS data to search, Search with YARA rules, Find more artifacts.
- ARTIFACT DETAILS:** 221 artifacts (Mobile artifacts, Cloud artifacts, Computer artifacts 221 of 271, Vehicle artifacts, Parse and carve artifacts, Privileged content, Date range filter).
- EVIDENCE SOURCES:** FILES & FOLDERS (selected), VOLUME SHADOW COPY, MEMORY.
- File List:** MORTIARY_jmortiary_2023.06.02_16.05.03.zip (checked), Logs (checked), Saved_Files (checked), Volatile_Data (checked).

Buttons at the bottom: BACK, NEXT



YARA

Magnet AXIOM Process 7.1.0.35864

File Tools Help

SEARCH WITH YARA RULES

CASE DETAILS

EVIDENCE SOURCES 2

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption
- Add keywords to search
- Extract text from files (OCR)
- Calculate hashes and find matches On
- Analyze chats with Magnet.AI
- Analyze pictures with Magnet.AI
- Add CPS data to search
- Search with YARA rules** On
- Find more artifacts

ARTIFACT DETAILS 221

- Mobile artifacts
- Cloud artifacts
- Computer artifacts 221 of 271
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

YARA RULE SETS

Use YARA rules to identify matching files. You can import YARA rule sets from a folder containing .yar or .yara files, or you can manually add YARA rule sets.

NOTE: Running several YARA rule sets at once might increase scan times.

Reading YARA rule sets from 1 synced folders. [EDIT](#)

X Q

SELECT ALL	ADD NEW RULE SET	REFRESH	Rules selected: 4
Enabled	Rule set name	Source path	Date created
<input checked="" type="checkbox"/>	ADApps.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:26:41 PM
<input checked="" type="checkbox"/>	kiwi_passwords.yar	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:26:54 PM
<input checked="" type="checkbox"/>	remote_access_apps.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:25:24 PM
<input checked="" type="checkbox"/>	SharpHound.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA	6/2/2023 4:26:32 PM
<input type="checkbox"/>	Linux.Virus.Vit.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Awfull.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Cmay.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.DeadCode.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Elerad.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Greenp.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Mocket.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Negt.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Trojan.CaddyWiper.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Trojan.Dridex.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM

BACK
GO TO FIND MORE ARTIFACTS



Keywords

Magnet AXIOM Process 7.1.0.35864

File Tools Help

ADD KEYWORDS TO SEARCH

CASE DETAILS

EVIDENCE SOURCES 2

PROCESSING DETAILS

- Search archives and mobile backups On
- Decode file-based encryption
- Add keywords to search On
- Extract text from files (OCR)
- Calculate hashes and find matches On
- Analyze chats with Magnet.AI
- Analyze pictures with Magnet.AI
- Add CPS data to search
- Search with YARA rules On
- Find more artifacts

ARTIFACT DETAILS 221

- Mobile artifacts
- Cloud artifacts
- Computer artifacts 221 of 271
- Vehicle artifacts
- Parse and carve artifacts
- Privileged content
- Date range filter

ANALYZE EVIDENCE

KEYWORD LISTS

ADD KEYWORD LIST

Keyword lists added: 1

Enabled	File source	Date loaded	Number of records
<input type="checkbox"/>	F\RansomCare\keywords.txt	5/26/2023 3:46:50 PM	53
<input checked="" type="checkbox"/>	C\Users\dmetz\OneDrive - Magnet Forensics Inc\YARA\Indicators-of-Compromise\References\triage-keywords.txt	6/2/2023 4:29:39 PM	53

KEYWORDS

ADD KEYWORD

Keywords added: 53

Keyword	Regex / GREP
psexesvc	<input type="checkbox"/>
rar.exe	<input type="checkbox"/>
rclone	<input type="checkbox"/>
recycle	<input type="checkbox"/>
Reflection	<input type="checkbox"/>
Remove-Module	<input type="checkbox"/>
rundll32	<input type="checkbox"/>
scrcons	<input type="checkbox"/>
Set-PSReadLineOption	<input type="checkbox"/>
silver	<input type="checkbox"/>
Start-Process	<input type="checkbox"/>

BACK GO TO EXTRACT TEXT FROM FILES (OCR)



Artifacts from RESPONSE Triage

SEEK JUSTICE. PROTECT THE INNOCENT.

Magnet AXIOM Examine v7.1.0.35864 - Magnet RESPONSE Demo

File Tools Process Help

Case dashboard

CASE OVERVIEW

EVIDENCE SOURCES 3

- RAMDump-MORIARTY-20230602-160503...
- RAMDump-MORIARTY-20230602-160503...
- MORIARTY_jmoriarty_2023.06.02_16.05.03.zip

INSIGHTS

Potential Cloud Evidence Leads 0

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 Magnet RESPONSE Demo

SCAN 1

Scanned by Doug Metz
Scan date/time - local time 6/2/2023 4:31:55 PM
Scan description

[VIEW SCAN SUMMARY](#)

PROJECT REVIEW ONLINE

You can integrate Magnet AXIOM with the Project REVIEW Online beta, a SaaS platform that allows users to review and collaborate with important stakeholders. [SHOW MORE](#)

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](#)

The AXIOMExamine.log file contains information about any errors encountered, jobs that were run, and general debugging information.

[OPEN LOG FILE](#)

EVIDENCE OVERVIEW

[ADD NEW EVIDENCE](#)

RAMDump-MORIARTY-20230602-160503-W... (26,857)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.dmp

Description

Location RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.dmp

Platform Computer

Process method Parsing and carving

[CHANGE PICTURE](#)

RAMDump-MORIARTY-20230602-160503-W... (141,106)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.json.zip

Description

Location RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.json.zip

Platform Computer

Process method Parsing and carving

[CHANGE PICTURE](#)

MORIARTY_jmoriarty_2023.06.02_16.05.03... (2,562,195)

[VIEW EVIDENCE FOR THIS SOURCE ONLY](#)

Evidence number MORIARTY_jmoriarty_2023.06.02_16.05.03.zip

Description

PLACES TO START

ARTIFACT CATEGORIES

[VIEW ALL ARTIFACT CATEGORIES](#)

Evidence source All

Number of artifacts 2,730,158

Operating System	Count	Total
Memory	140,821	2,508,197
Web Related	64,513	
Media	9,379	
Refined Results	3,928	
Custom	1,583	
...	...	

TAGS AND COMMENTS

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](#)

CPS DATA MATCHES

MAGNET.AI CATEGORIZATION

KEYWORD MATCHES (2,028,489)

[VIEW ALL KEYWORD MATCHES](#)

KEYWORD MATCHES

[MATCHES](#)



THANK YOU



<https://github.com/dwmetz>



<https://bakerstreetforensics.com>



doug.metz@magnetforensics.com



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



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



@dwmetz

