MAGNET VIRTUAL SUMMIT 2024

Investigating Malware with Free Tools & Magnet AXIOM Cyber

Doug Metz, Senior Security Forensics Specialist

Magnet Forensics

About Me

MAGNET FORENSICS

The **Aux**tera Project

BAKER STREET FORENSICS

D . F . I . R .

HTCIA

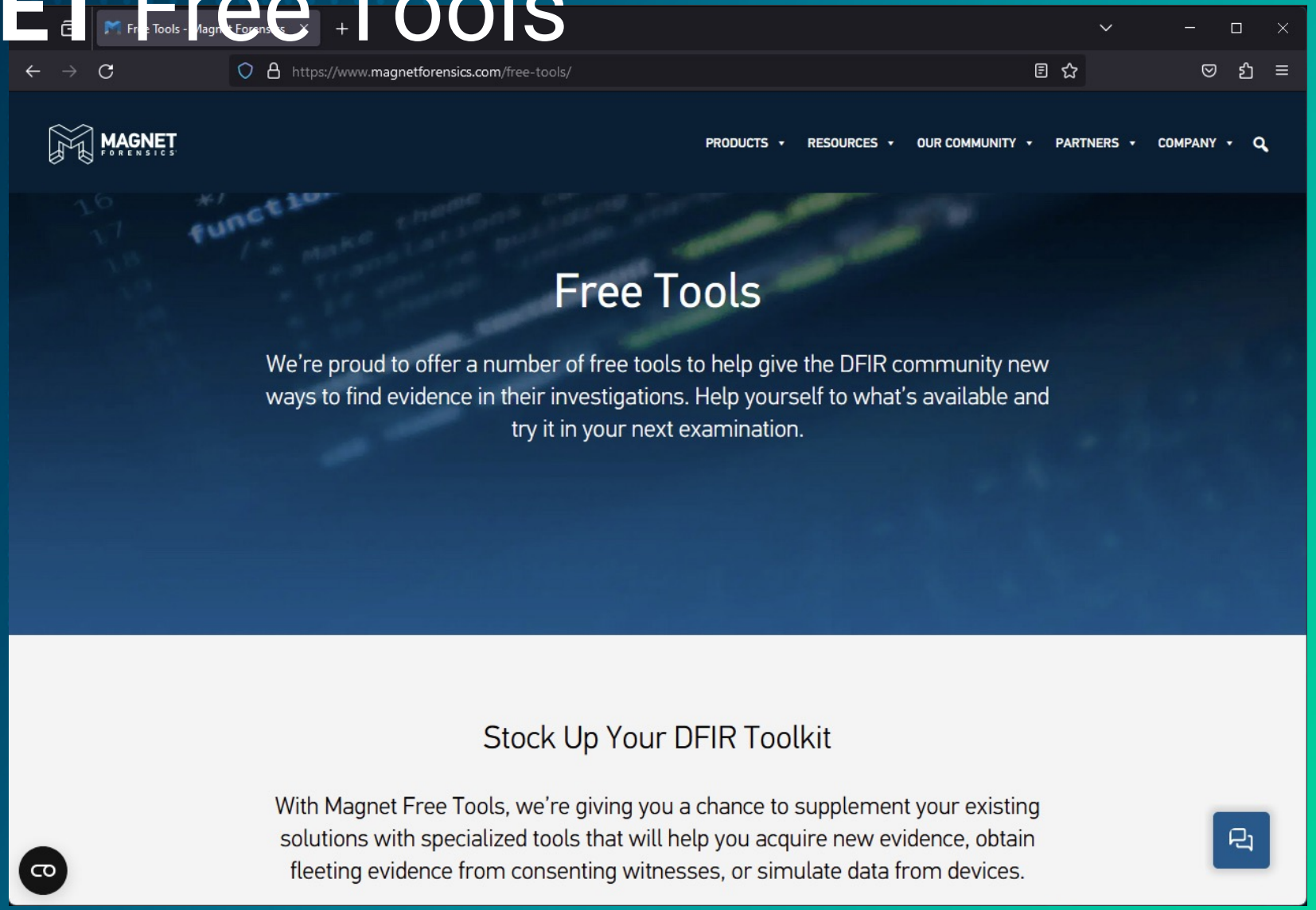
Delaware Valley - Philadelphia

Investigating Malware with Free Tools & Magnet AXIOM Cyber

How to use free tools as part of a malware investigation workflow.

Learn how to supplement your digital forensics toolkit with several of our top free tools including **Magnet RESPONSE, MAGNET DumpIt (for Windows and Linux), MAGNET Hash Sets Manager, and Magnet ACQUIRE**. Plus, see how Magnet AXIOM Cyber works with each to enhance your investigation workflow.

MAGNET Free Tools



MAGNET Free Tools

MAGNET RESPONSE

Magnet RESPONSE is a free and easy-to-use solution to quickly collect and preserve data from local endpoints before it is potentially

MAGNET HASH SETS MANAGER

MAGNET Hash Sets Manager offers you a central database that allows you to automatically manage hash set distribution to

MAGNET ACQUIRE

Magnet ACQUIRE lets digital forensic examiners quickly and easily acquire forensic images of any iOS or Android device...

MAGNET DUMPIT FOR WINDOWS

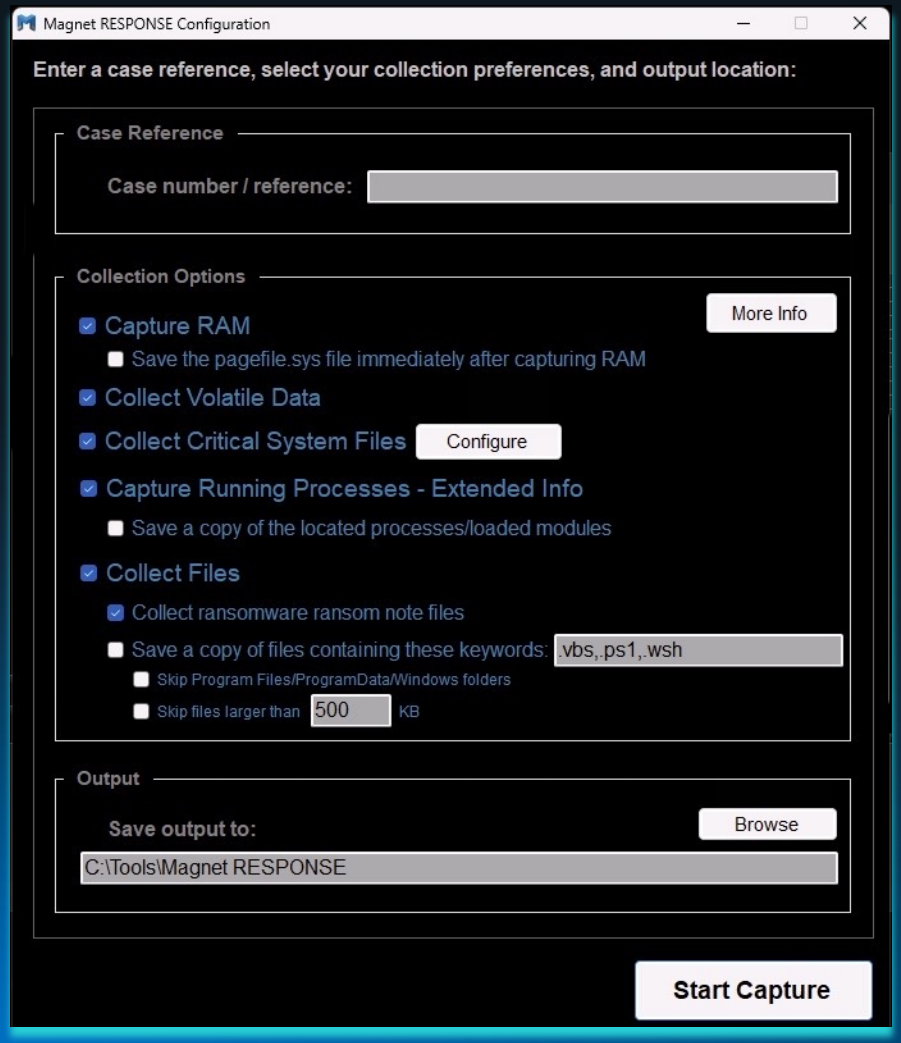
MAGNET DumpIt for Windows is a fast memory acquisition tool for Windows (x86, x64, ARM64). Generate full memory crash dumps of Windows

MAGNET DUMPIT FOR LINUX

MAGNET DumpIt for Linux is a fast memory acquisition open source tool for Linux written in Rust on GitHub. Generate full memory crash

MAGNET RESPONSE

MAGNET RESPONSE



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

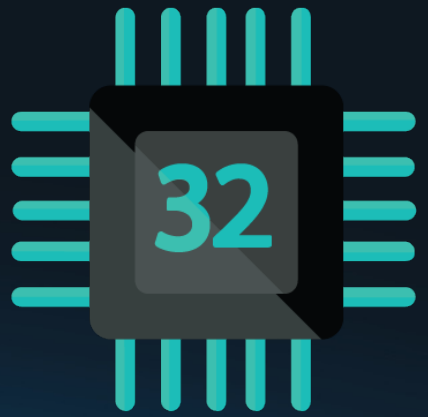
Minimal to no training is required—it's as simple as entering a case name, selecting the collection options and then "start capture."

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/

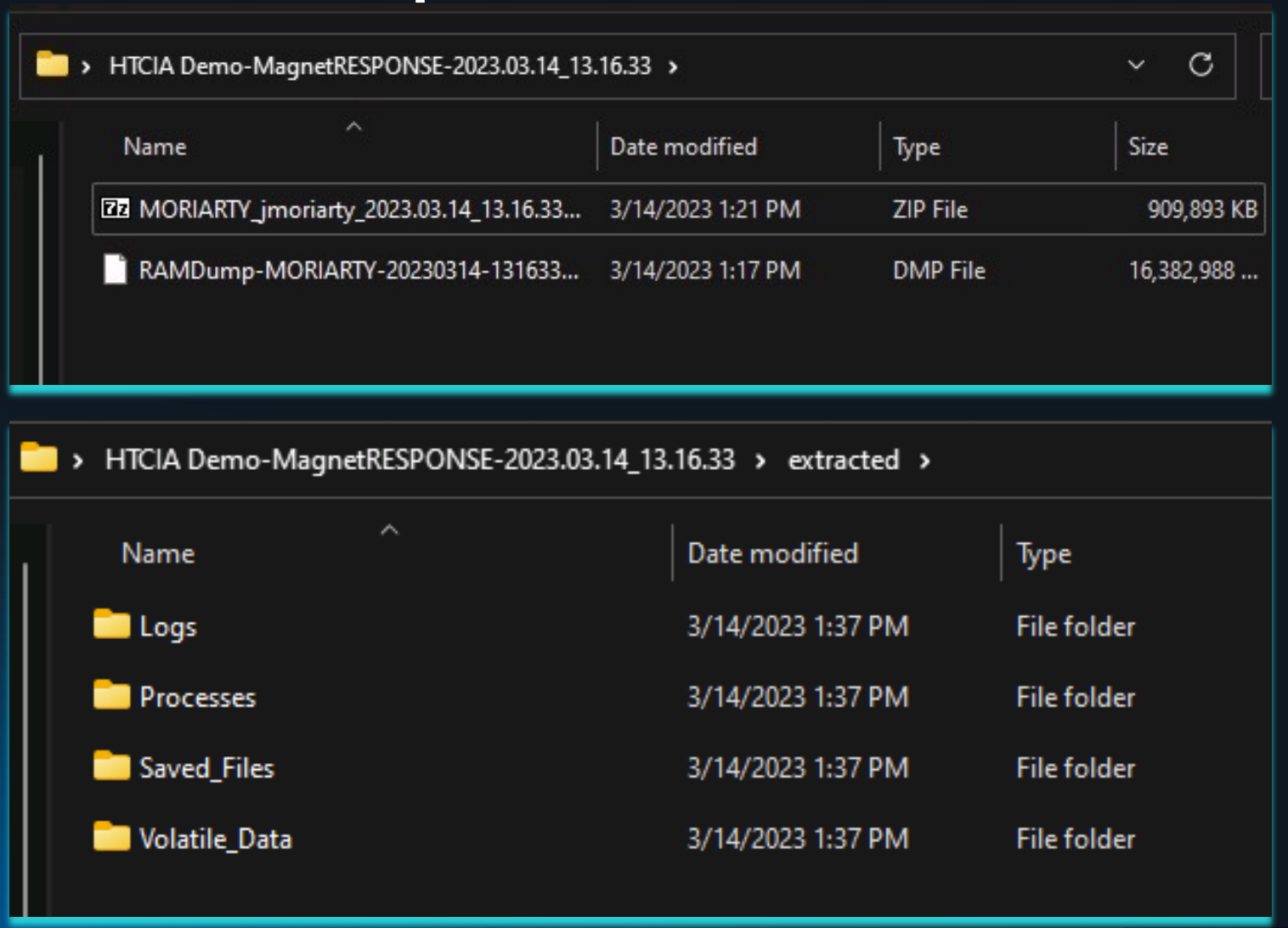
MAGNET RESPONSE - RAM

Memory collection made easy

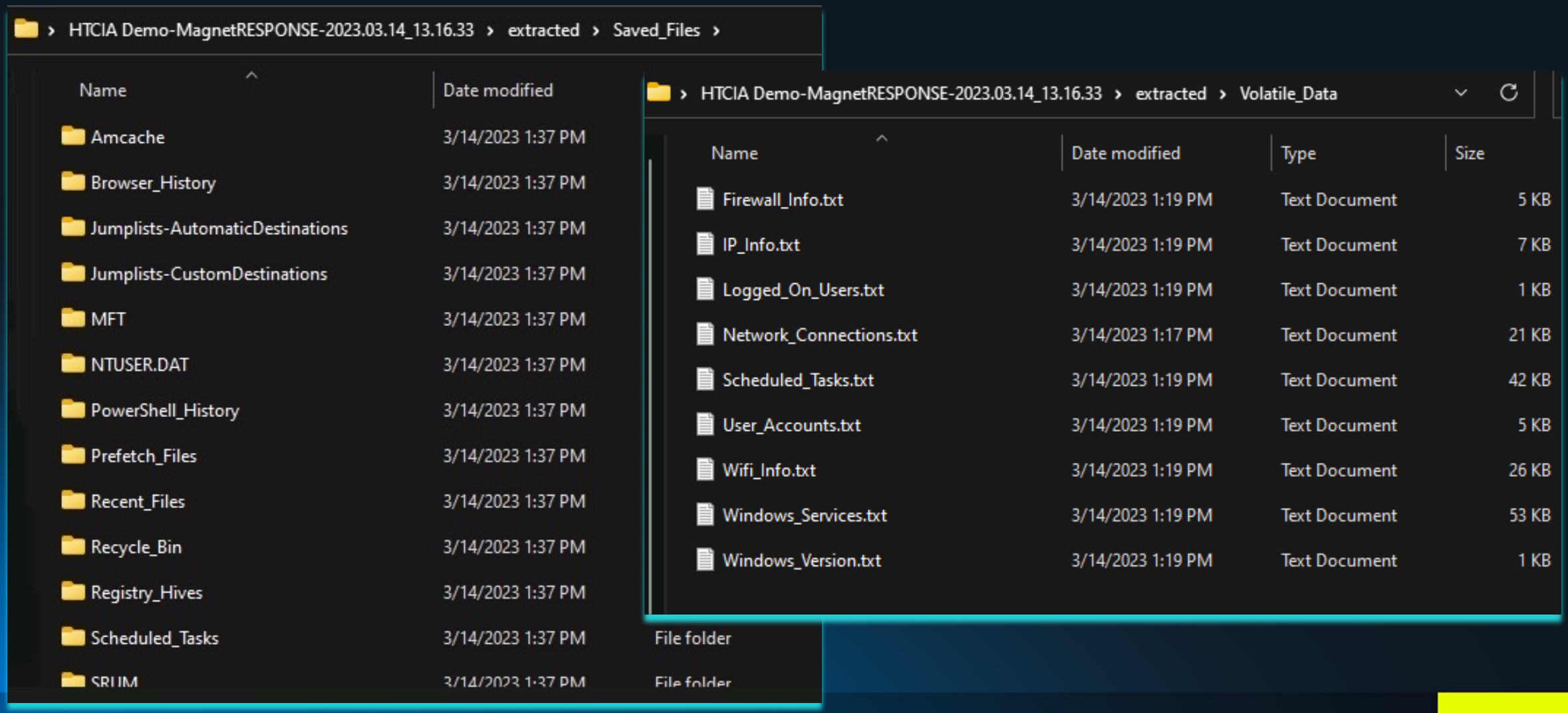


VS

MAGNET RESPONSE Output



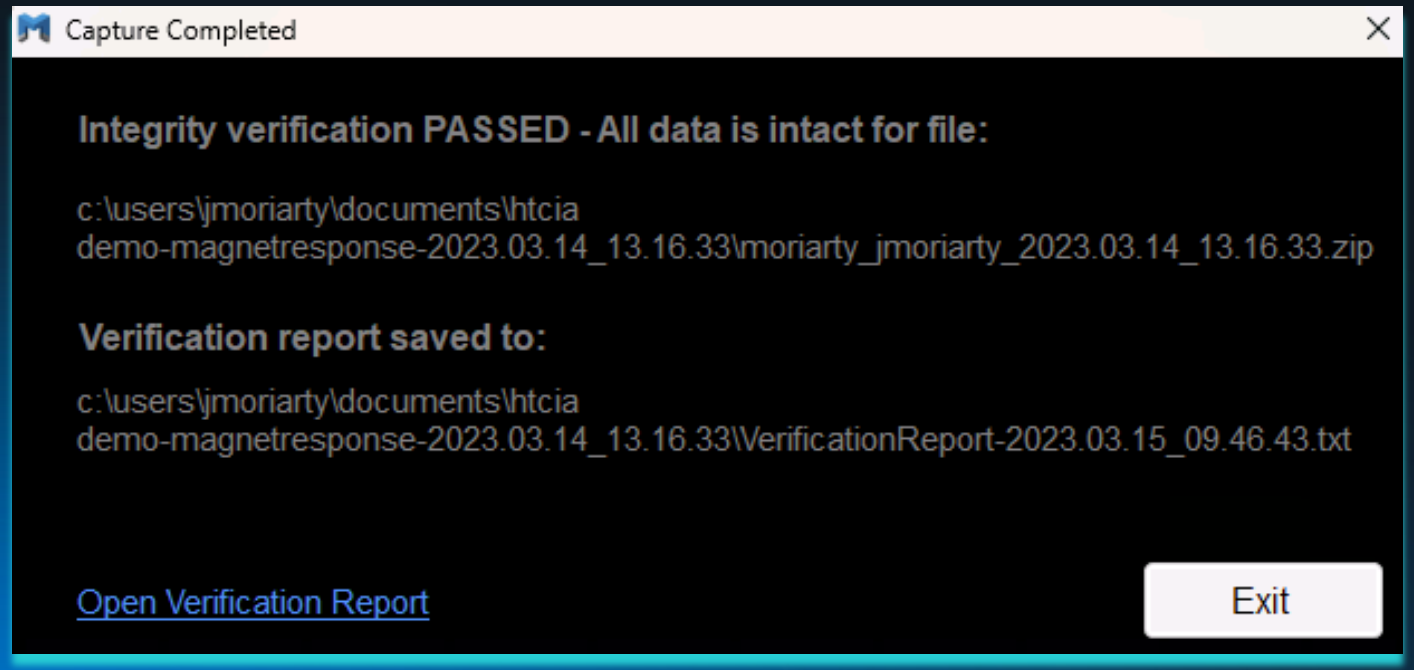
MAGNET RESPONSE Output



MAGNET RESPONSE Verification

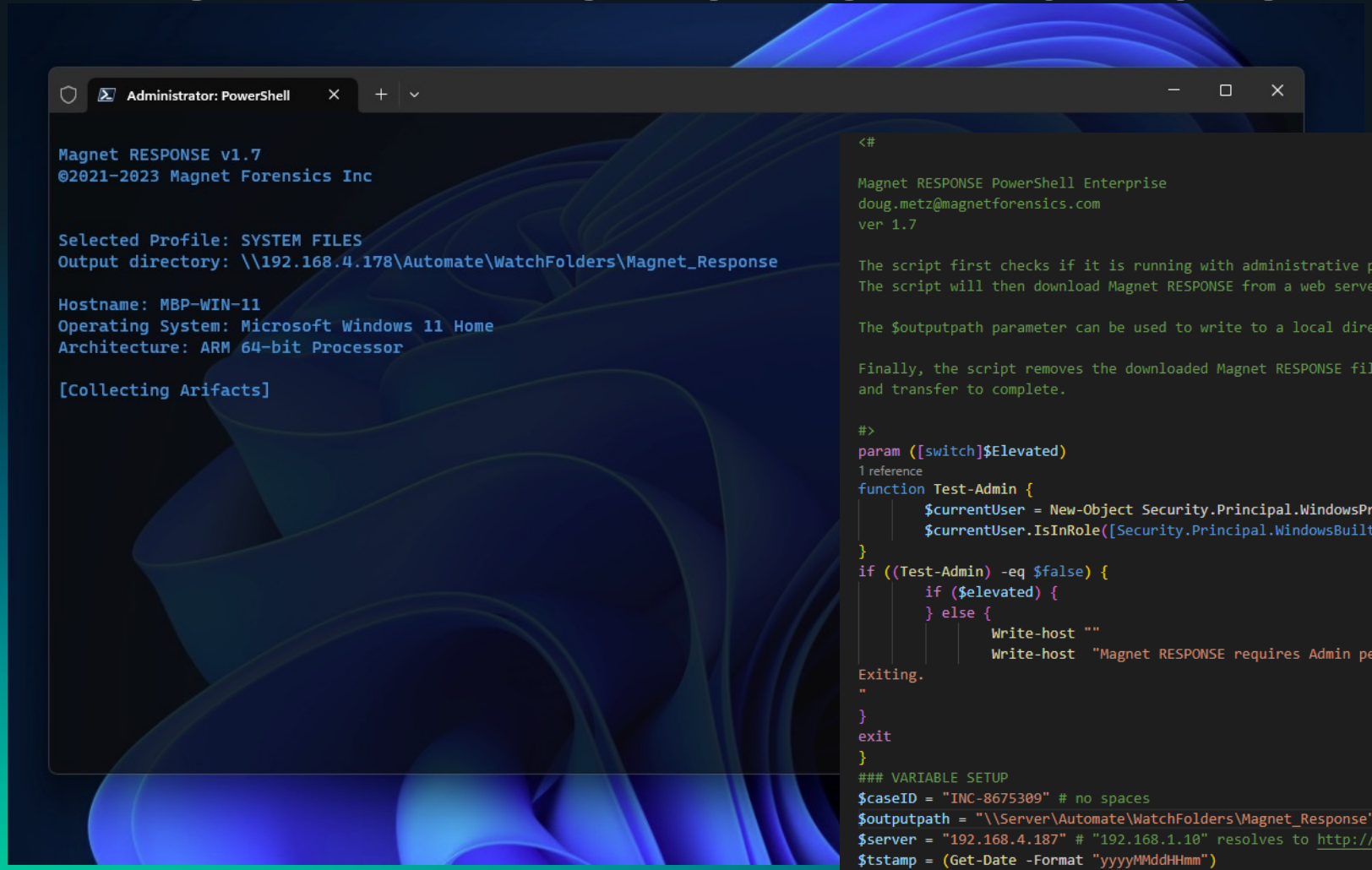
Verifying a Capture Package

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 POWERSHELL

MAGNET RESPONSE PowerShell




```powershell
<#

Magnet RESPONSE PowerShell Enterprise
doug.metz@magnetforensics.com
ver 1.7

The script first checks if it is running with administrative permissions and exits if not.
The script will then download Magnet RESPONSE from a web server, extract it, and run with the specified options.

The $outputpath parameter can be used to write to a local directory `C:Temp`, `D:\Output` or network `\\Server\Share`.

Finally, the script removes the downloaded Magnet RESPONSE files and prints the time taken for the collection
and transfer to complete.

#>
param ([switch]$Elevated)
1 reference
function Test-Admin {
        $currentUser = New-Object Security.Principal.WindowsPrincipal $([Security.Principal.WindowsIdentity]::GetCurrent())
        $currentUser.IsInRole([Security.Principal.WindowsBuiltinRole]::Administrator)
}
if ((Test-Admin) -eq $false) {
        if ($elevated) {
        } else {
                Write-host ""
                Write-host  "Magnet RESPONSE requires Admin permissions.
Exiting.
"
}
exit
}
### VARIABLE SETUP
$caseID = "INC-8675309" # no spaces
$outputpath = "\\Server\Automate\WatchFolders\Magnet_Response" # Update to reflect output destination. C:\Temp R:\Output \\Server\Share
$server = "192.168.4.187" # "192.168.1.10" resolves to http://192.168.1.10/MagnetRESPONSE.zip
$tstamp = (Get-Date -Format "yyyyMMddHHmm")
#######
```

RESPONSE CLI Capture Options

/captureram	- Enables RAM capture
/capturepagefile	- Enables capture of pagefile.sys file
/capturevolatile	- Enables volatile data capture
/capturesystemfiles	- Enables critical system file collection
/captureextendedprocessinfo	- Enables extended info capture for running processes/loaded modules
/saveprocfiles	- Enables saving copies of running processes/loaded modules. Must be used with /captureextendedprocessinfo switch
/capturefiles:<keyword.csv>	- Enables scanning for files with filenames containing specified keywords e.g. /capturefiles:secret,badfile,.vbs,confidential
/skipsystemfolders	- Indicates that the Program Files/ProgramData/Windows folders should be skipped when searching for files based on filename keywords. Must be used with /capturefiles
/maxsize:<file size in KB>	- Indicates the maximum file size to collect from hits found using /capturefiles – any files above this size are skipped e.g. /maxsize:500
/captureransomnotes	- Enables the ransomware ransom note collection

Case Variables

```
### VARIABLE SETUP
$caseID = "demo-161" # no spaces
$outputpath = ”\\server\share" # Update to reflect output destination.
$server = "192.168.4.187" # "192.168.1.10" resolves to
http://192.168.1.10/MagnetRESPONSE.zip
```

$caseID – Name of your case or incident. (no spaces)

$outputpath – Where the collection output is sent

$server – Address for web server hosting MagnetRESPONSE.zip

Collection Profiles

```
#### Extended Process Capture
<#
$profileName = "EXTENDED PROCESS CAPTURE"
$arguments = "/capturevolatile /captureextendedprocessinfo /saveprocfiles"
#>
#### Systen Files

$profileName = "SYSTEM FILES"
$arguments = "/capturesystemfiles"
#>
#### Just RAM
<#
$profileName = "CAPTURE RAM"
$arguments = "/captureram"
#>
```

RESPONSE CLI Assembled

```
MagnetRESPONSE\MagnetRESPONSE.exe /accepteula /unattended
/output:$outputpath/$caseID-$env:ComputerName-$tstamp /caseref:$caseID $arguments
```

/accepteula /unattended – general CLI requirements

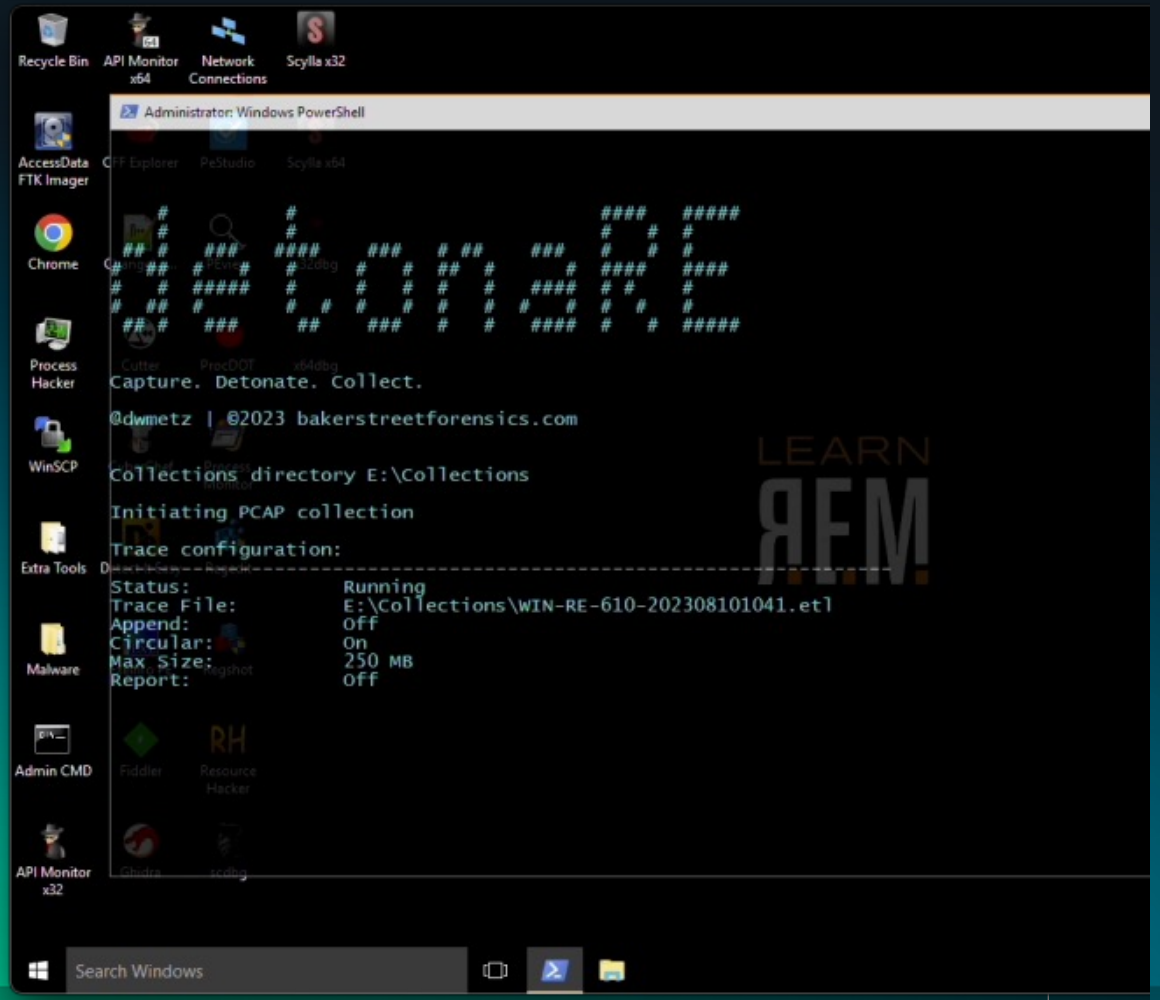
/output – server path\caseID-hostname-timestamp

/caseref:caseID – Case ID

$arguments – Specified in collection profile

Capturing Malware Evidence with detonaRE

detonaRE – *from Latin, to detonate*

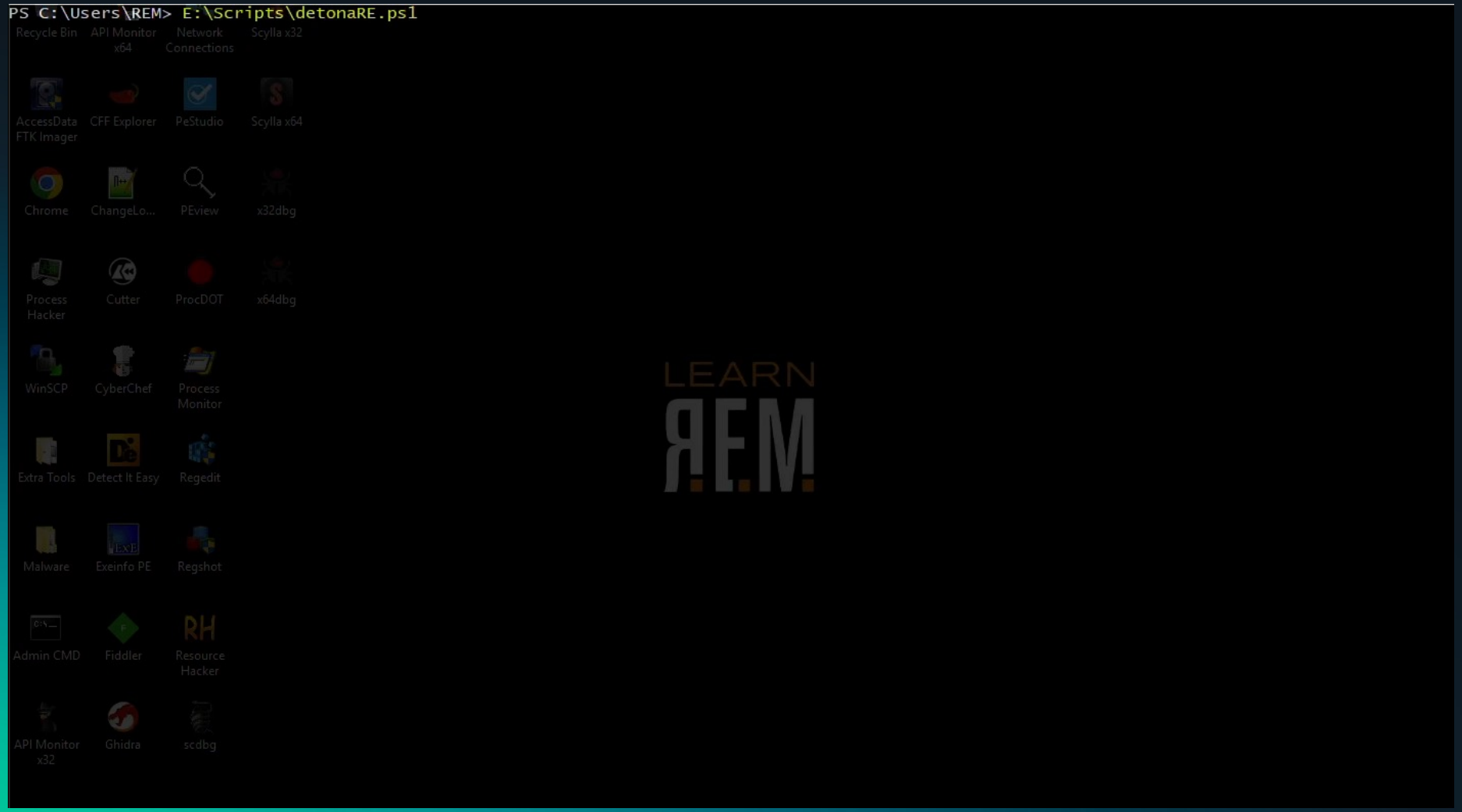


- initiates packet capture
- launches malware sample
- terminates packet capture after specified interval
- initiates evidence collection with Magnet RESPONSE (memory, process, and triage capture)
- converts collected .etl file (network capture) to .pcap with etl2pcapng.

variable configuration:

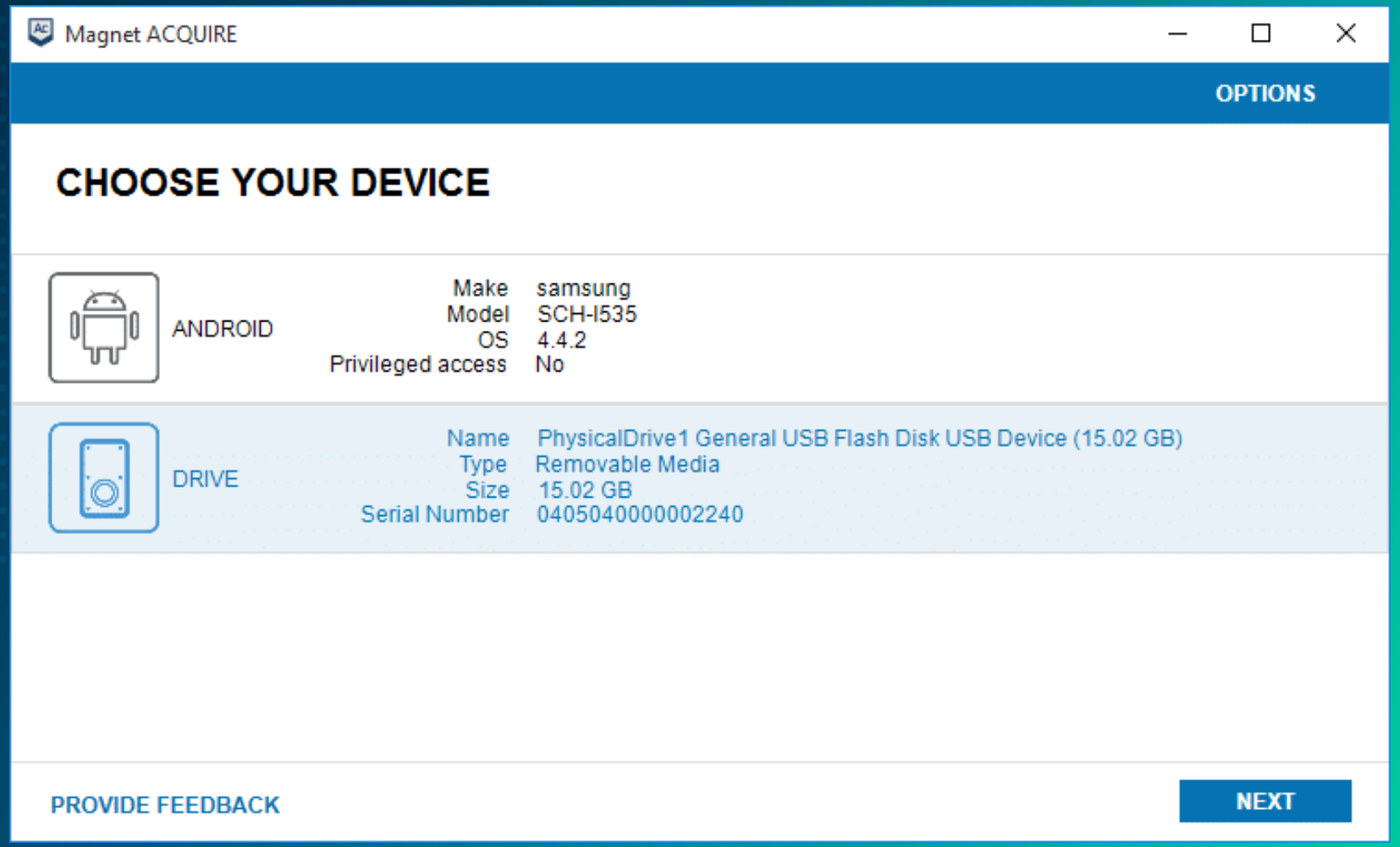
```
$malwspath = "E:" ## malware source path
$malwdpath = "C:\Users\REM\Desktop\Malware\"
## malware destination path
$malware = "redline-76ca4a.exe" ## malware
executable
$pcaptime = 180 ## duration in seconds for
pcap capture
$toolsdir = "E:\Tools" ## MagnetRESPONSE.exe
and etl2pcapng.exe
```

detonaRE – demo



MAGNET ACQUIRE

MAGNET ACQUIRE



Magnet ACQUIRE lets digital forensic examiners quickly and easily acquire forensic images of any iOS or Android device, hard drive, and removable media.

MAGNET ACQUIRE

The Power of One Acquisition Tool for Smartphones and Computers
Magnet ACQUIRE combines an intuitive user interface with reliable and fast extractions, giving you the data quickly and easily.

COMBINED COMPUTER AND MOBILE ACQUISITION
Acquire smartphones and tablets as well as image laptops, desktop computers, and removable media.

CUT THROUGH THE NOISE WITH TARGETED ACQUISITION
Get the areas of the hard drive most known for containing important evidence and eliminate unnecessary files that won't really support your case from the beginning.

When to use what collection tool?

MAGNET RESPONSE: Triage collections with or without Memory, online, offline and isolated assets; Windows only.

MAGNET ACQUIRE: Mobile collections (Android/iOS); Computer Collections (Full disk or targeted), external USB devices; dead disk forensics; Windows, Linux*

AXIOM CYBER REMOTE ACQUIRE: Online assets, triage or full disk collections; Windows, Linux, Mac

DUMPIT: Strictly memory collections; Windows or Linux

	MAGNET RESPONSE	MAGNET ACQUIRE	AXIOM CYBER REMOTE ACQUIRE	MAGNET DUMPIT
Windows	✅	✅	✅	✅
Linux		✅	✅	✅
Mac			✅	
Mobile		✅		

MAGNET AXIOM™ CYBER

Simplify your remote forensic investigations by focusing on the evidence that matters.

AXIOM Cyber is a digital forensics solution that allows organizations to perform remote acquisitions while collecting and analyzing evidence from cloud services, computers, and mobile devices.

Remote Acquisition

Acquire From The Cloud

Examine From All Sources

Easy Reporting

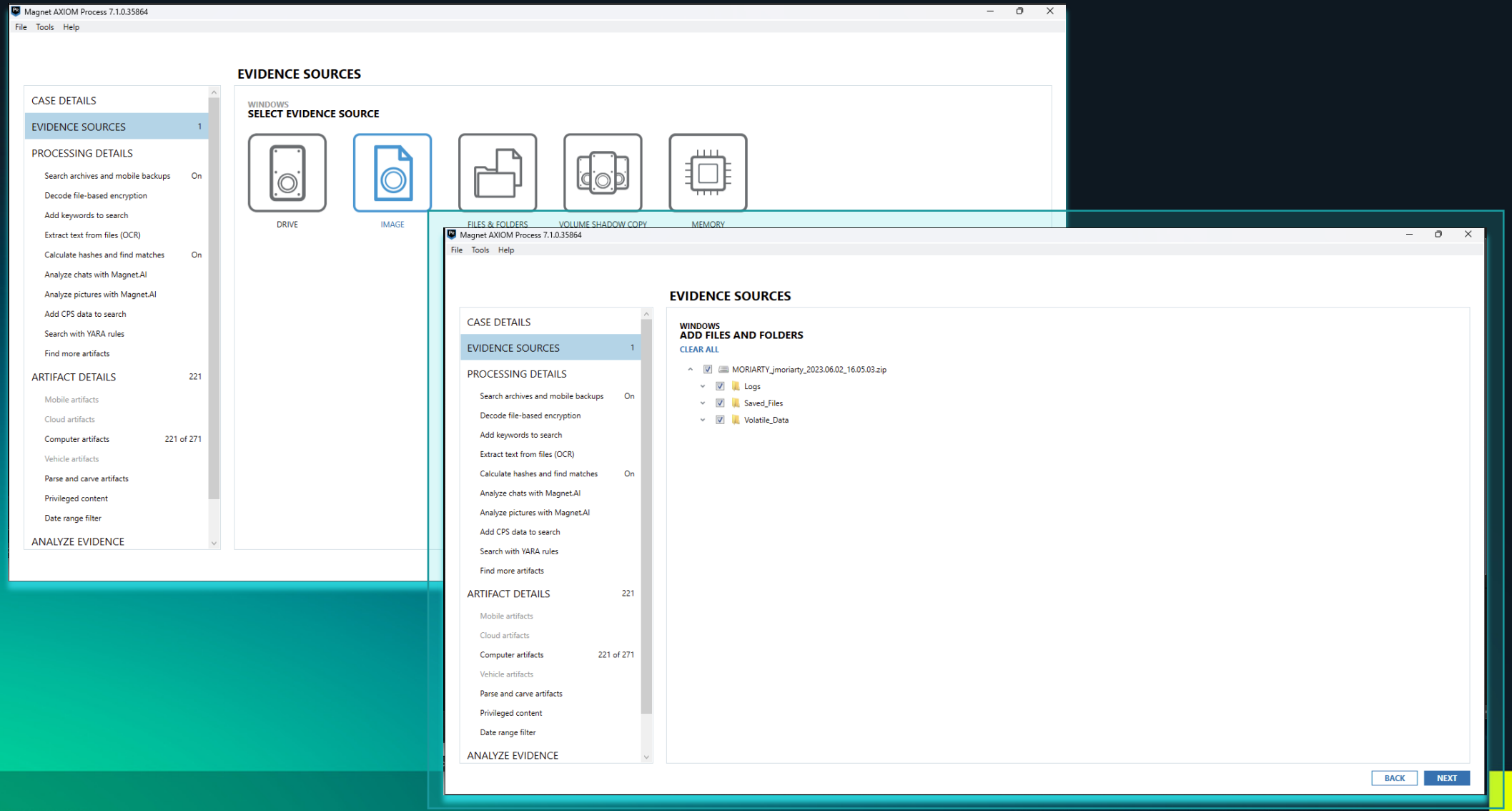
Quick Root Cause Analysis

Processing Malware Evidence with

MAGNET AXIOM™ CYBER

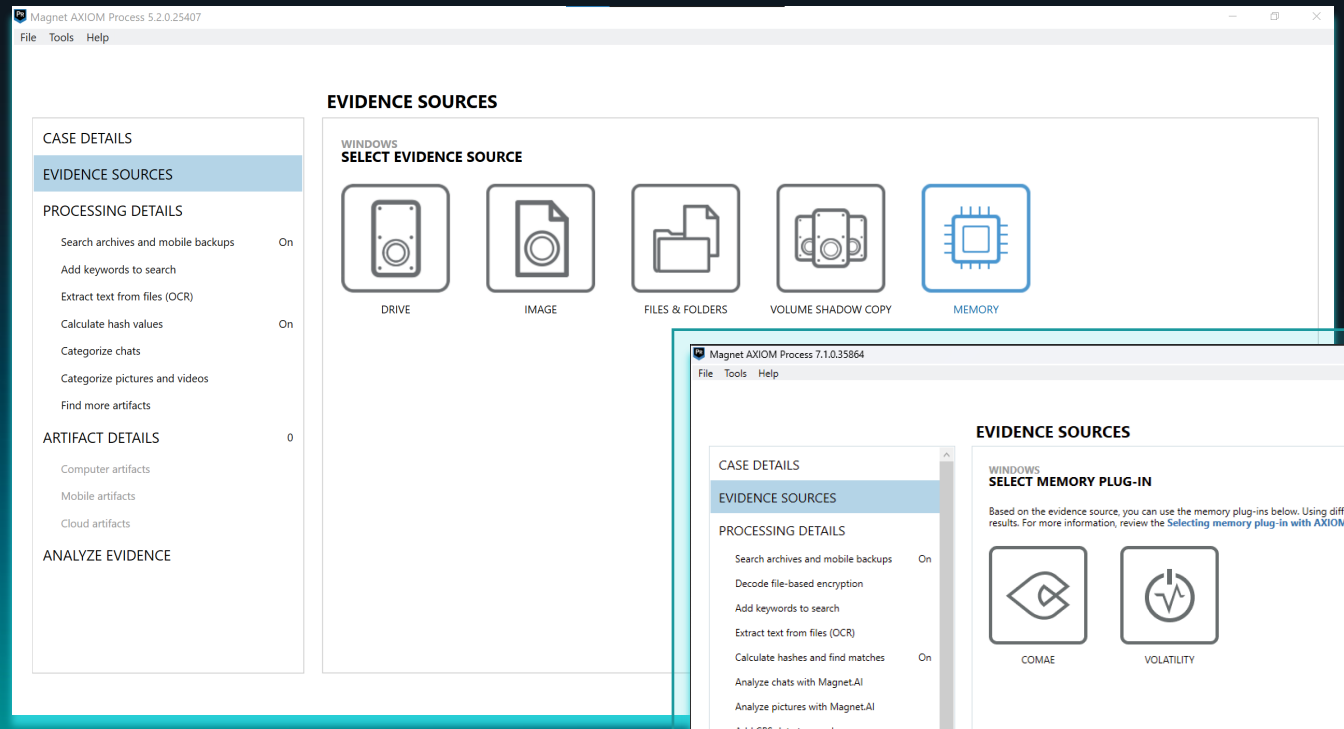
Triage Processing

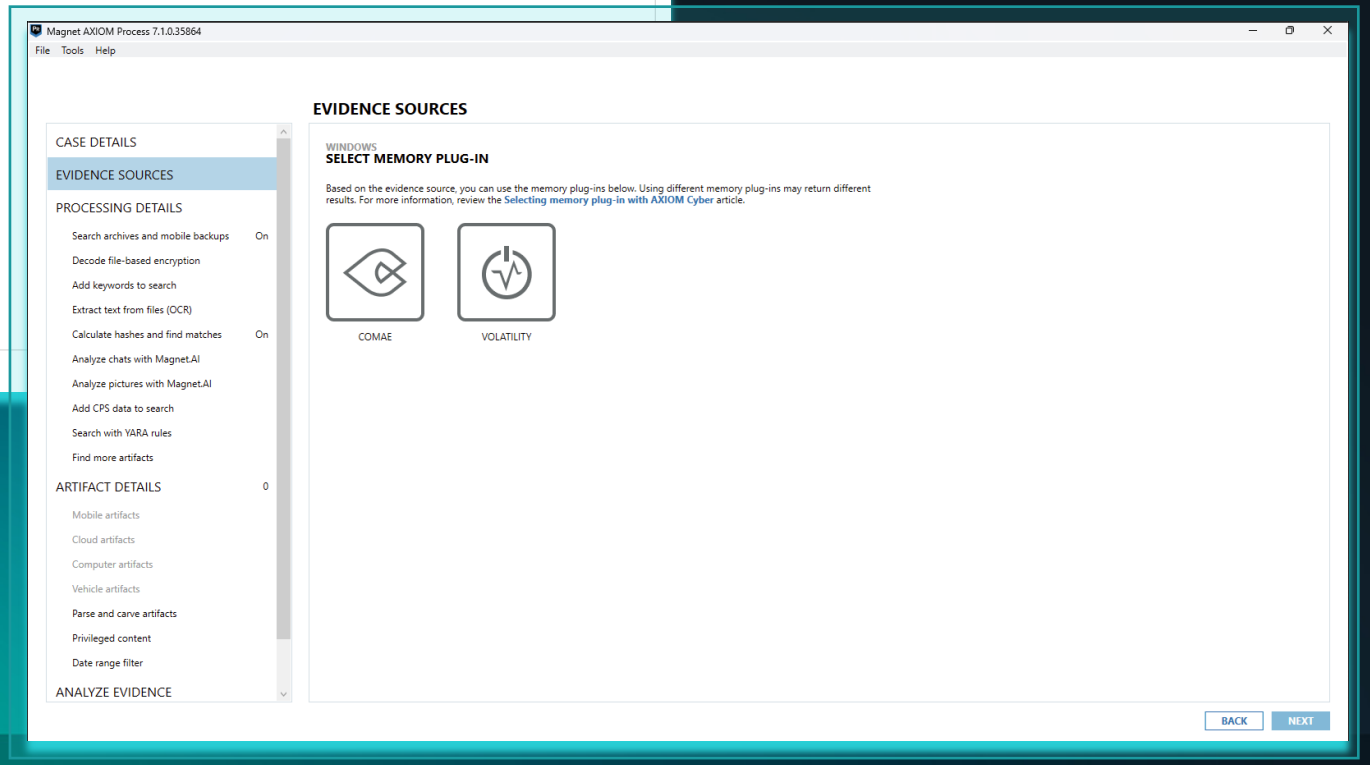
Computer > Windows > Load Evidence > IMAGE



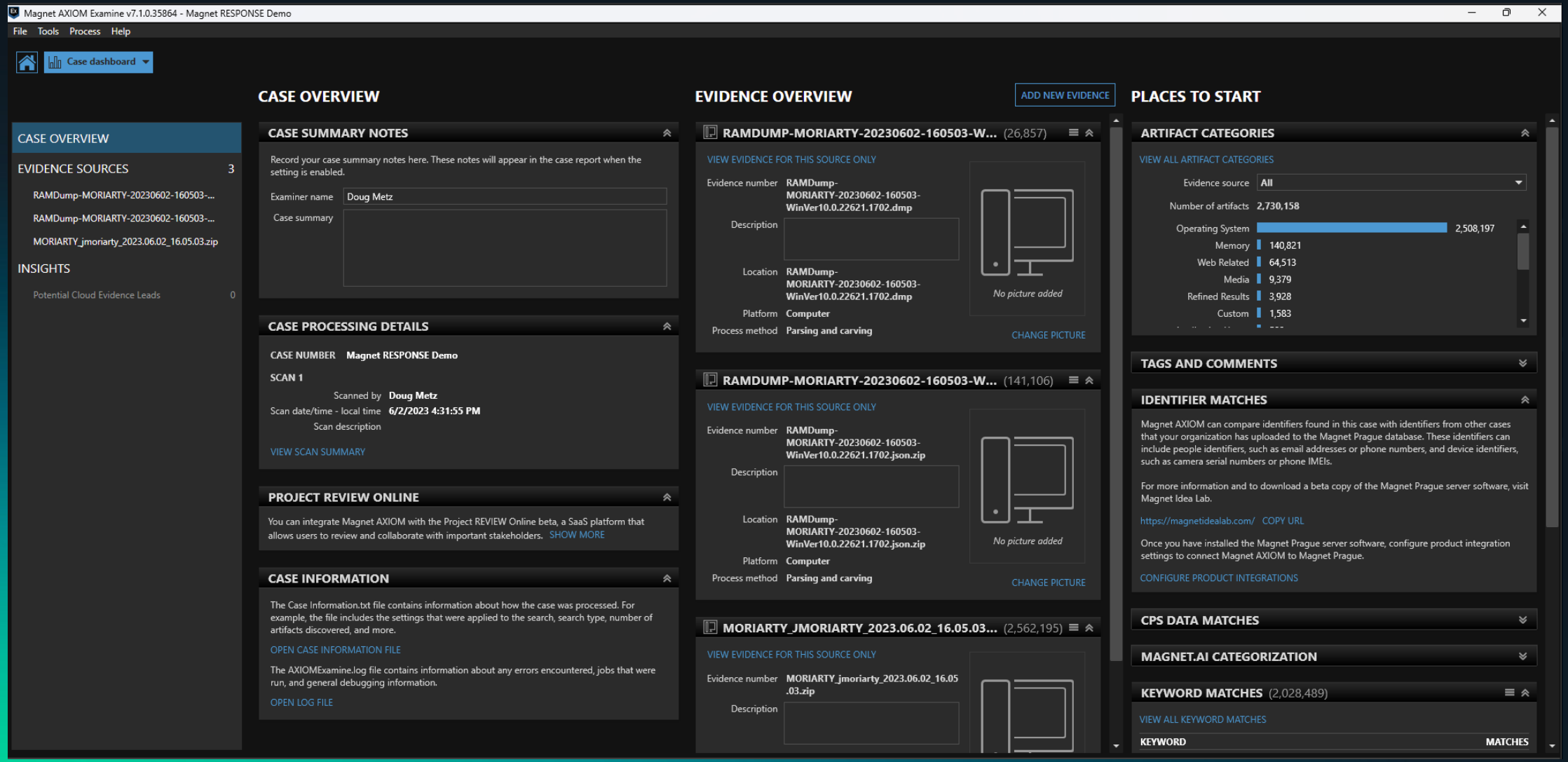
Comae Memory Processing

Computer > Windows > Load Evidence > MEMORY

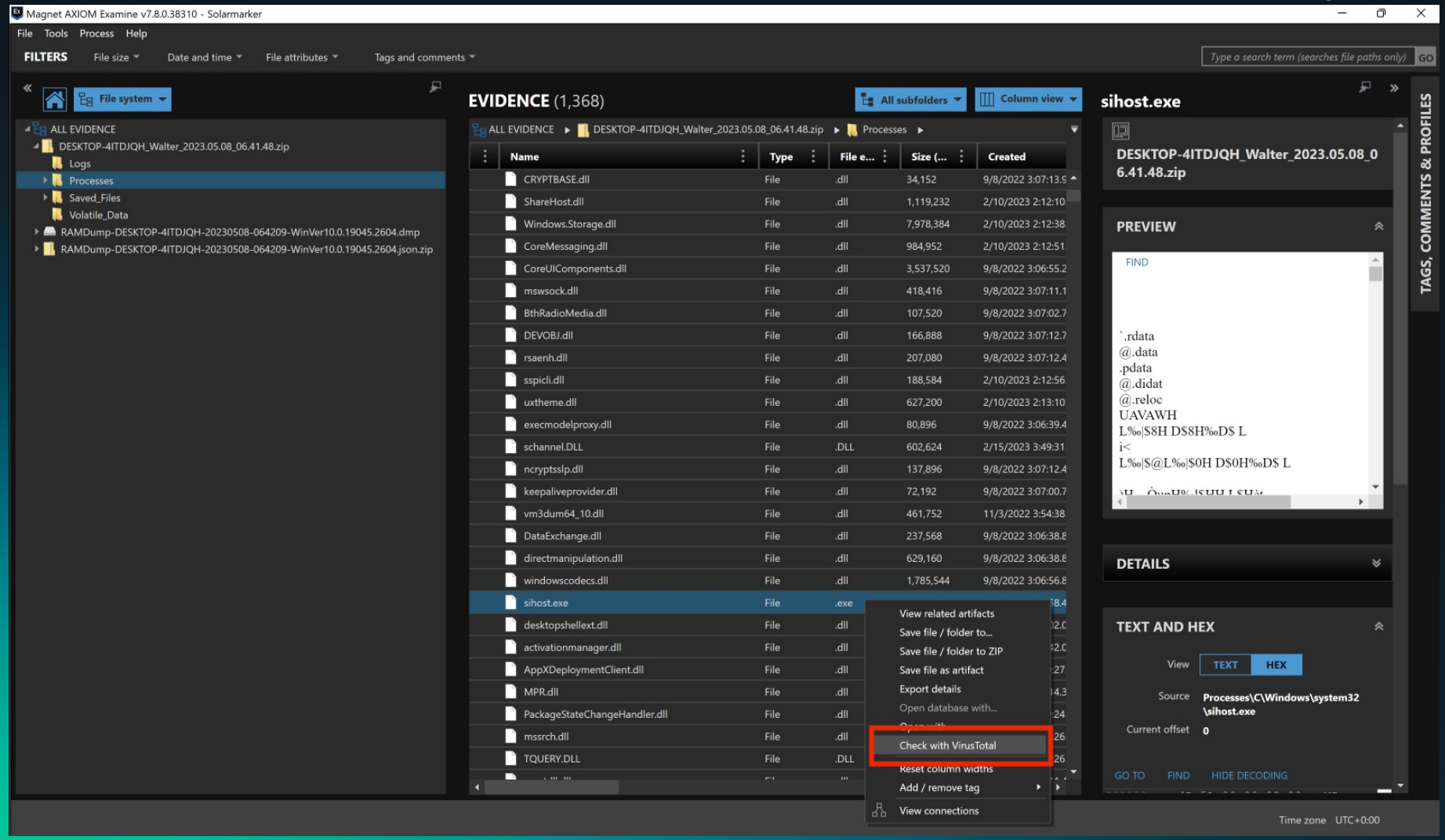




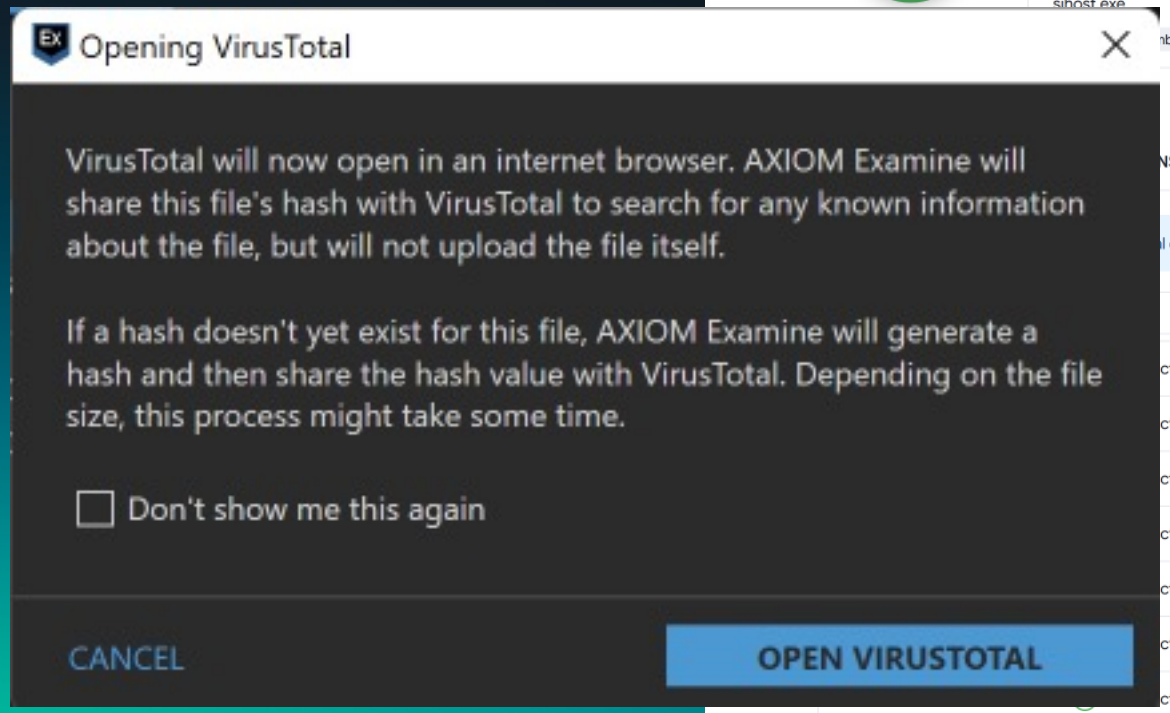
Artifacts from RESPONSE RAM & Triage

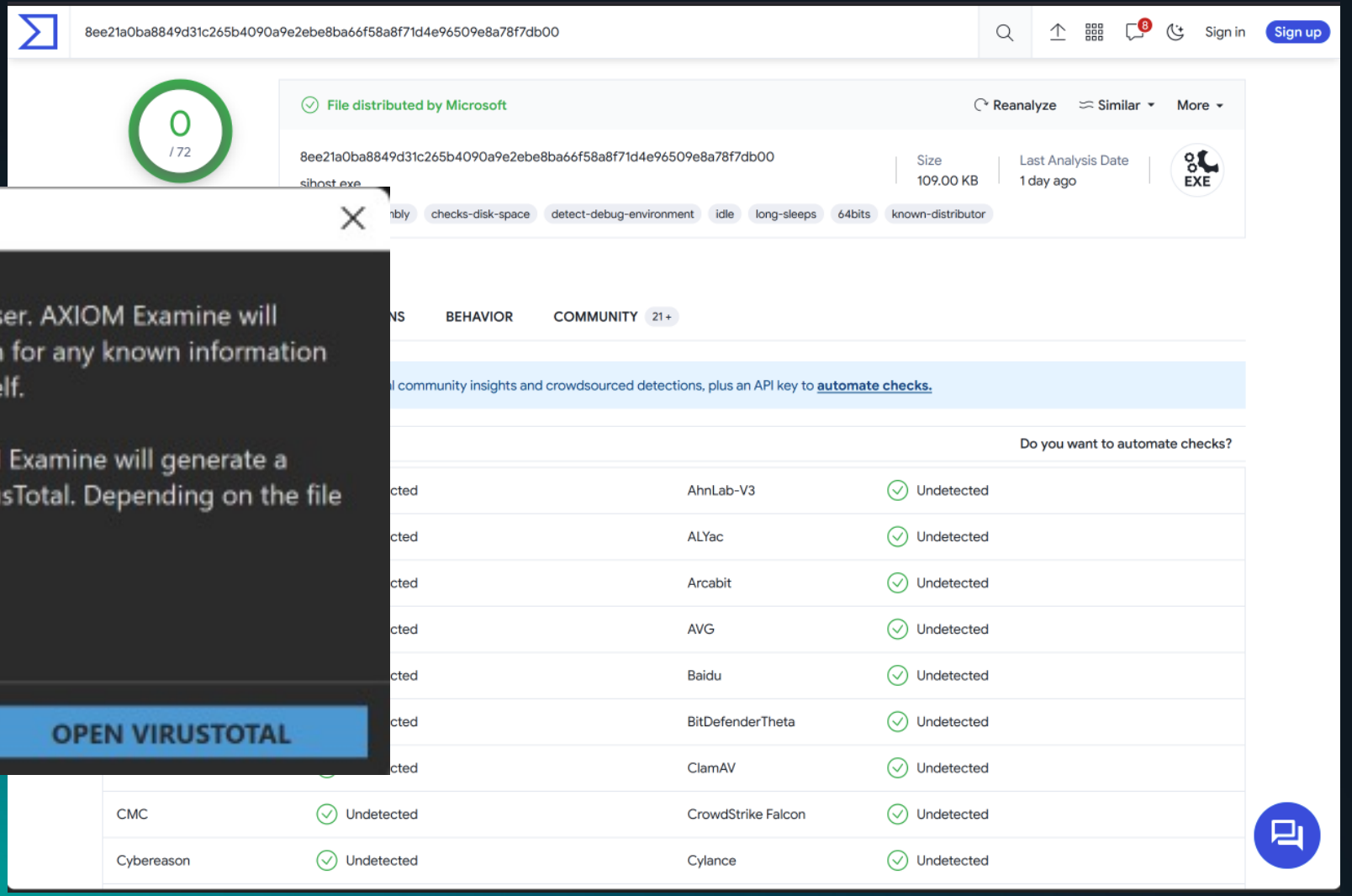


VirusTotal Lookups with AXIOM Cyber

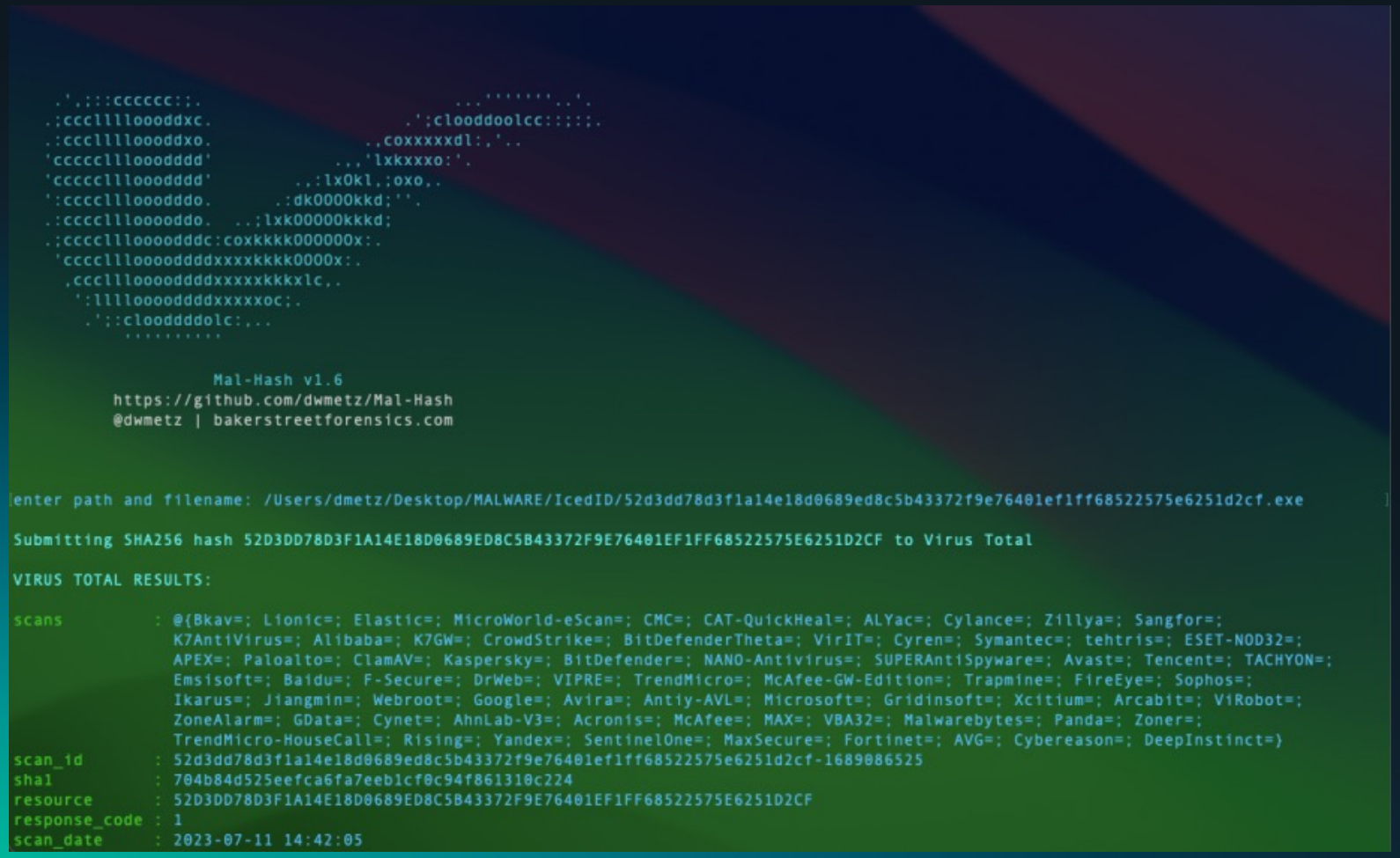


VirusTotal Lookups with AXIOM Cyber





VirusTotal Queries with PowerShell



VirusTotal Queries with PowerShell

VTHashSub.ps1

- The script takes a hash value as input and submits the hash to Virus Total* for analysis.
- The script will check Malware Bazaar to see if a sample matching the hash is available.
- The hashes, Virus Total and Malware Bazaar results are both displayed on screen and saved to a text report.
- Timestamp of the analysis is recorded in UTC.

Mal-Hash.ps1

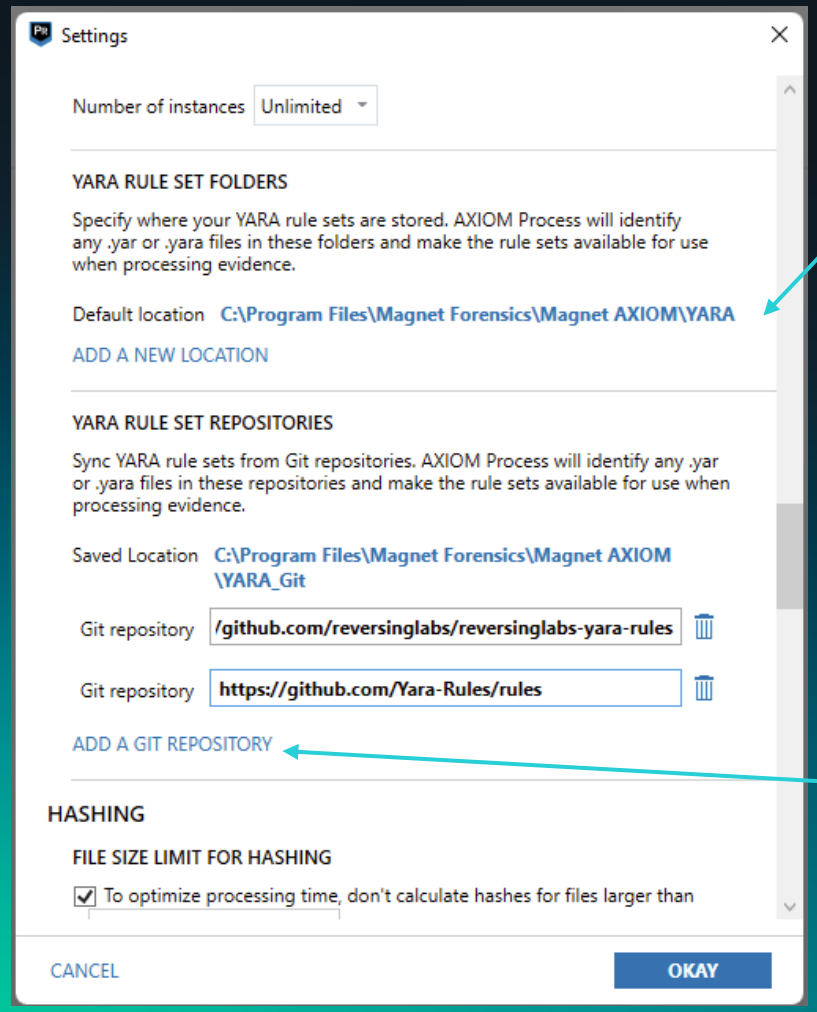
•The script takes the input of a file, calculates the hashes (MD5, SHA1, SHA256), and then submits the SHA256 hash to Virus Total* for analysis.
•The script will also run Strings against the sample.
•The script will check Malware Bazaar to see if a sample matching the hash is available.
•The hashes, strings, Virus Total and Malware Bazaar results are both displayed on screen and saved to a text report.
•Timestamp of the analysis is recorded in UTC.

Mal-Hash.ps1 and VTHashSub.ps1 will operate (via PowerShell) on Windows, Mac & Linux.

** Virus Total API key expected in vt-api.txt.*

MAGNET AXIOM CYBER & YARA

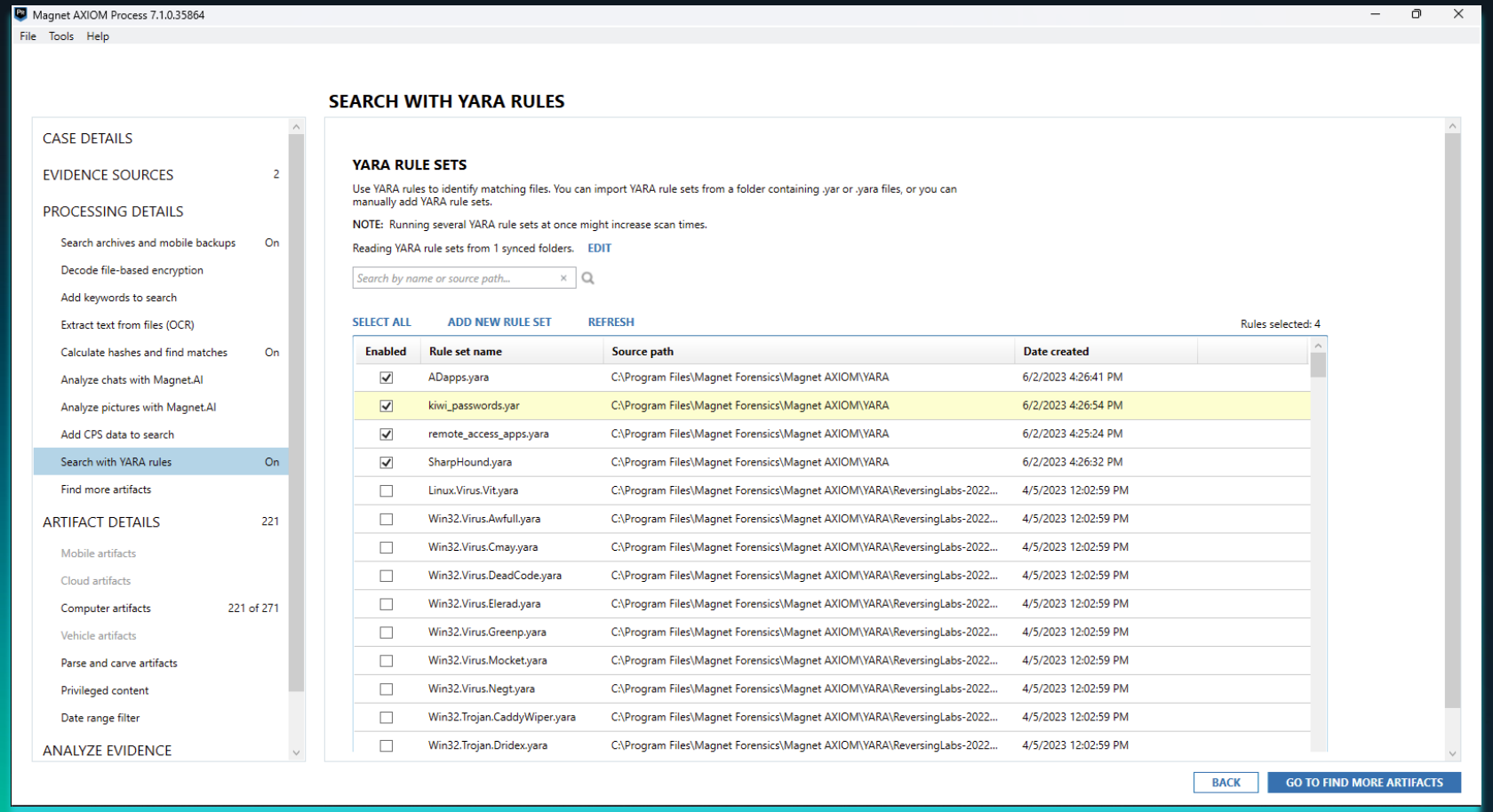
YARA Repositories



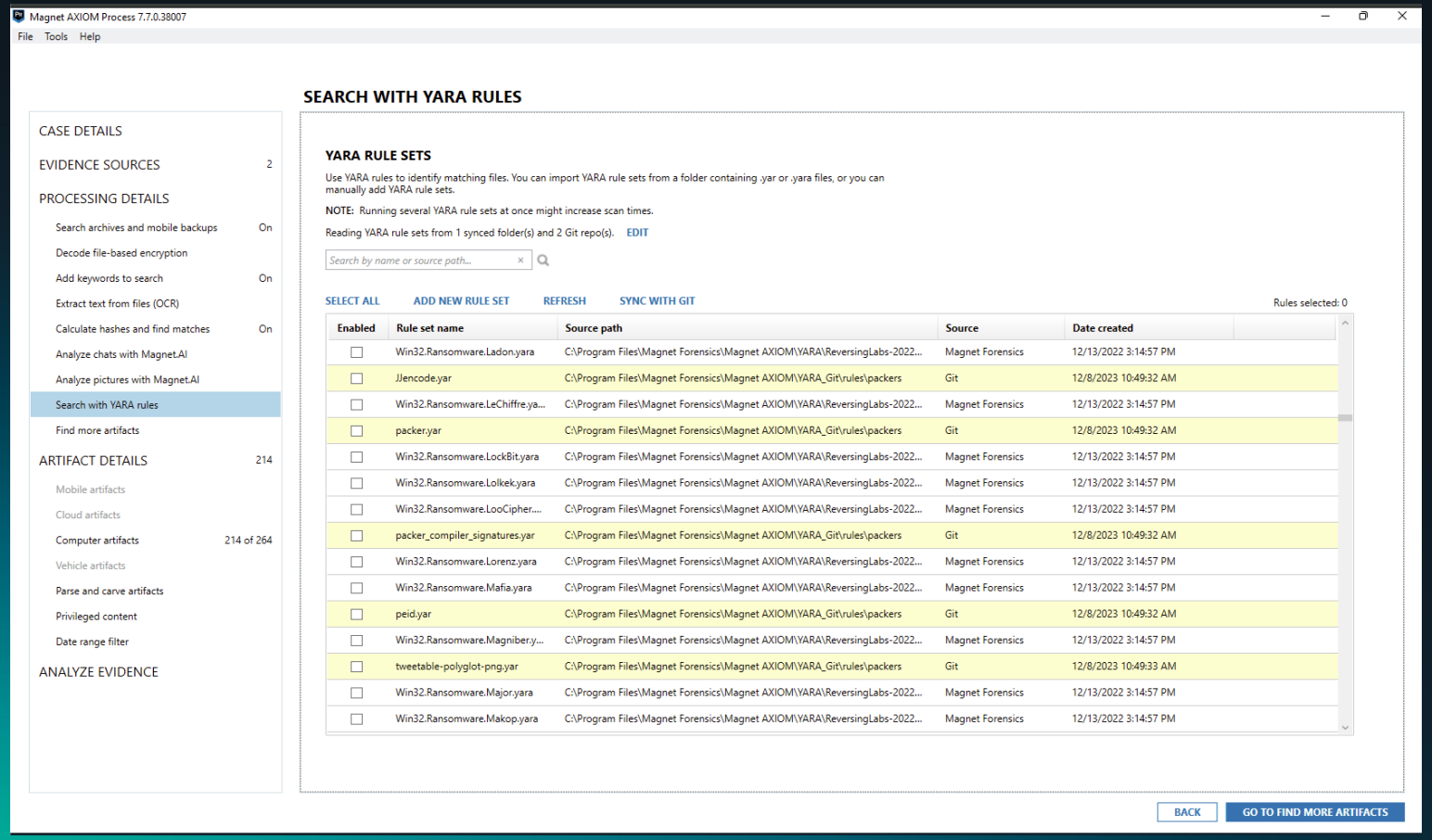
Manually add rules to this folder

Add additional GitHub repositories to sync

Processing with YARA Rules



New YARA Rules



What’s in your YARA?

Organization specific indicators

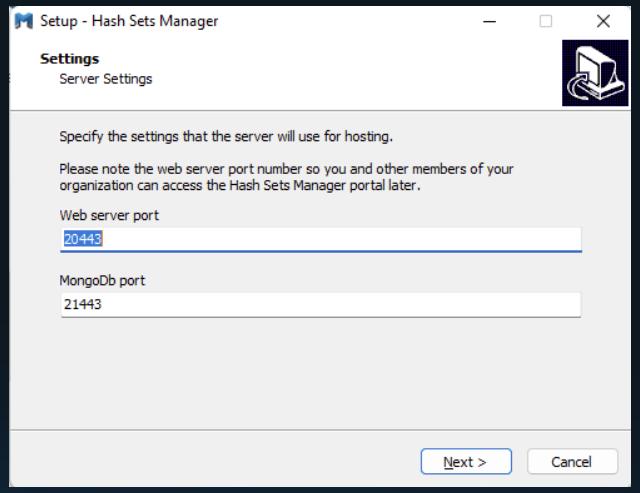
Indicators from previous incidents

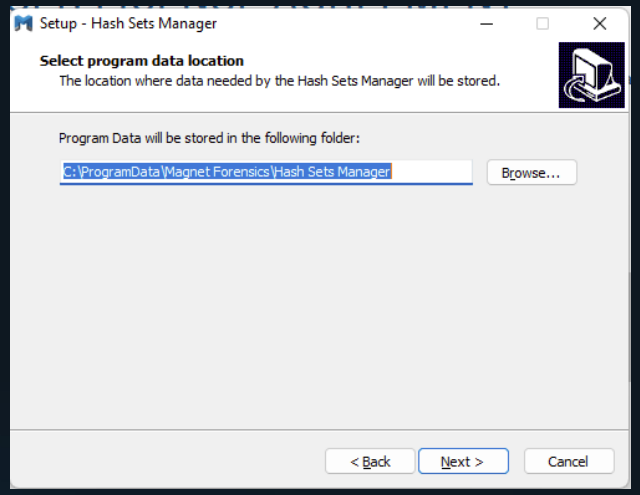
Keywords or codewords for sensitive projects

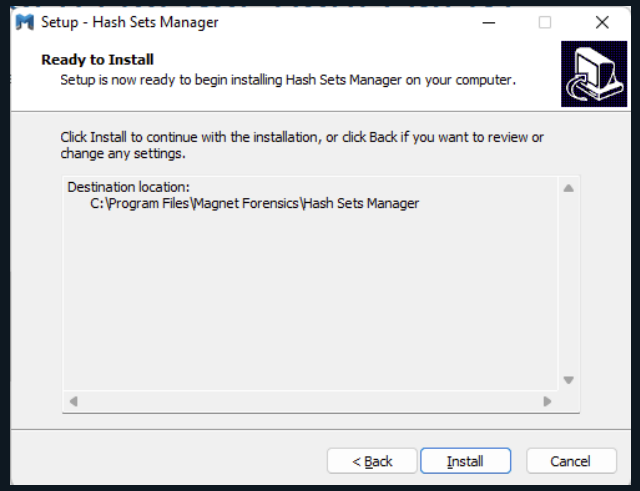
? ? ?

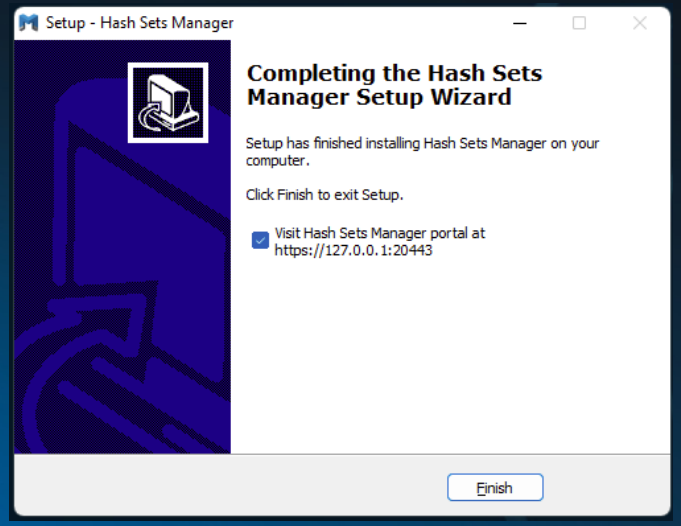
MAGNET Hash Sets Manager

Hash Sets Manager (HSM) Installation

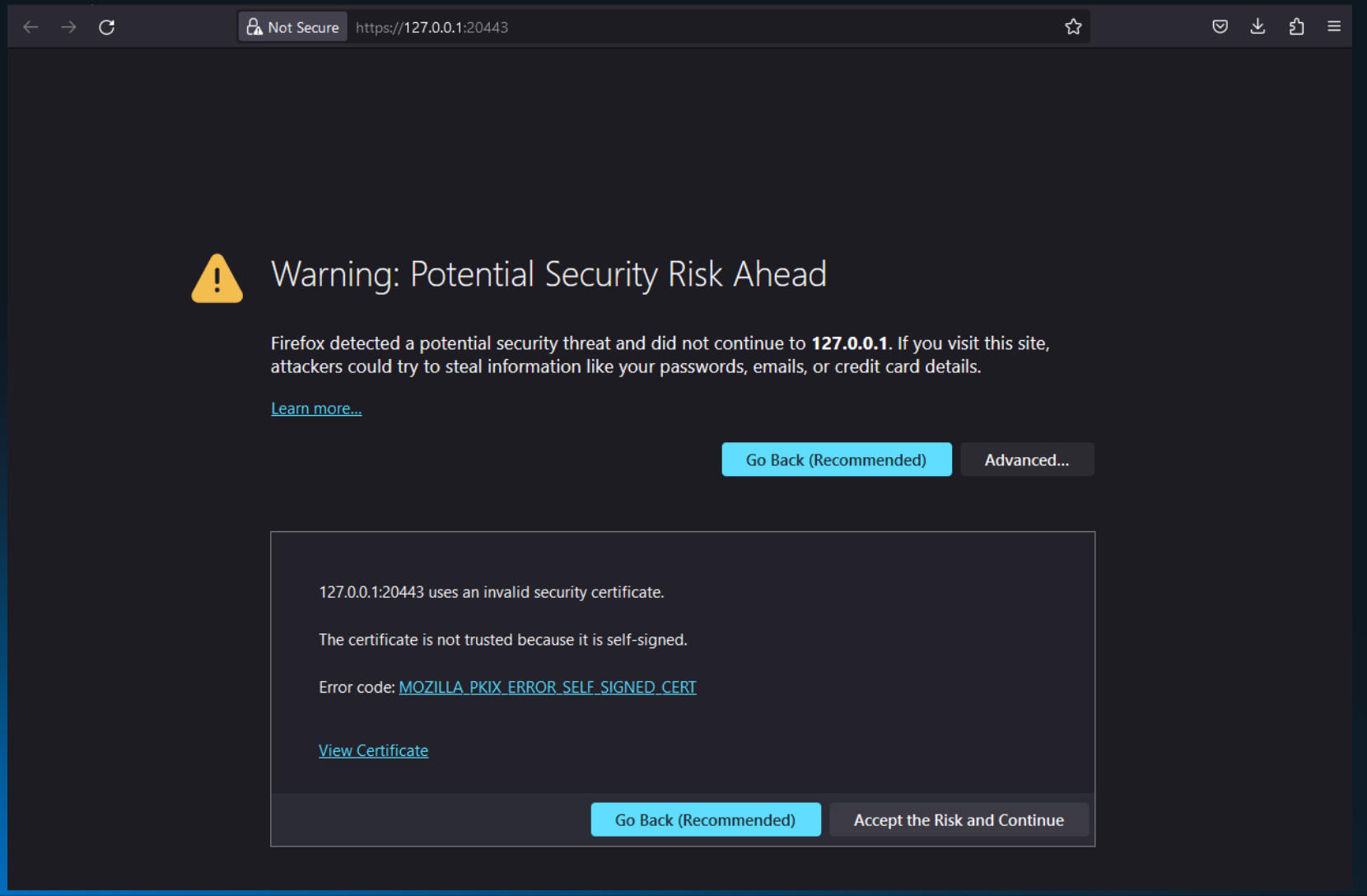




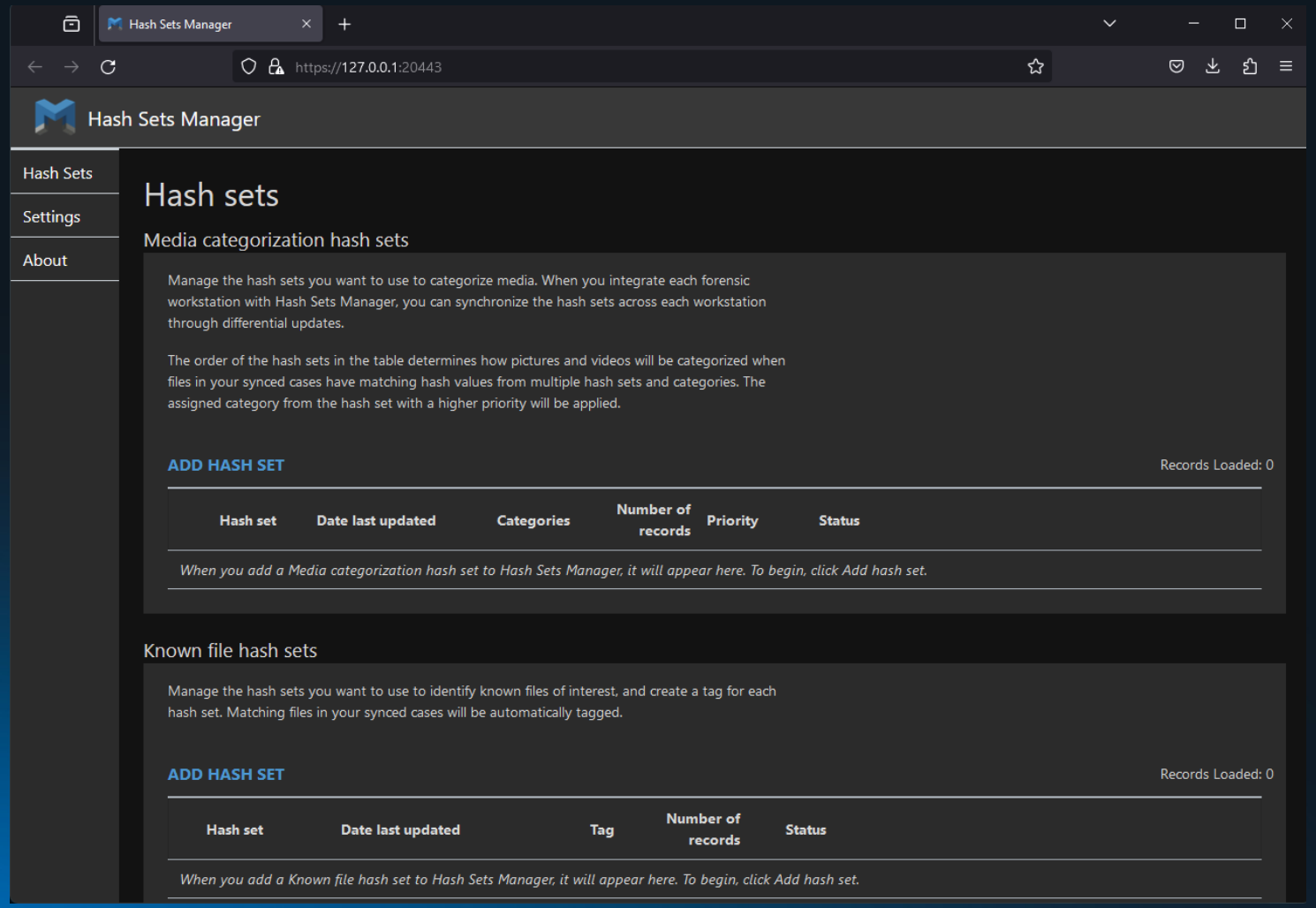




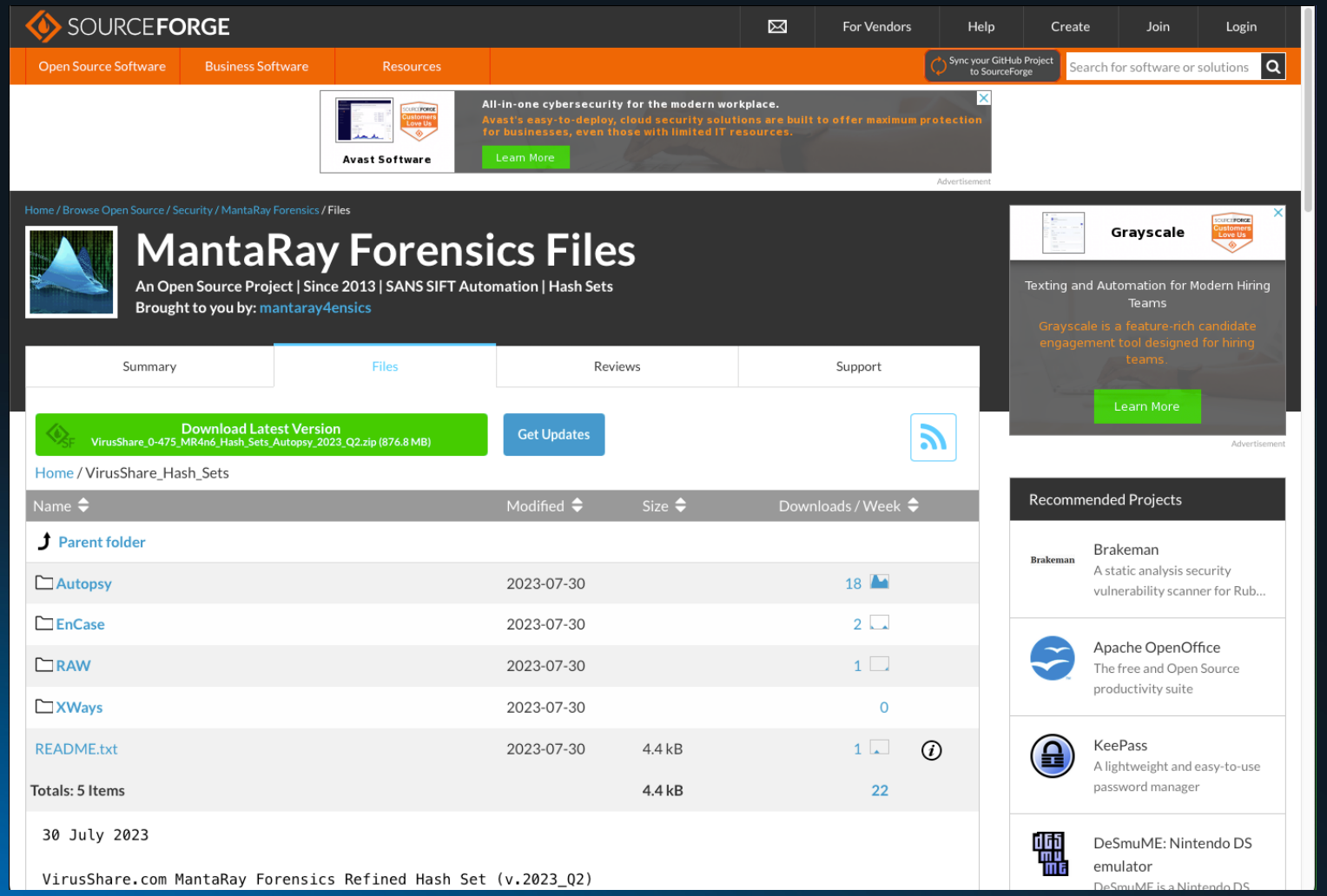
HSM Certificate Warning



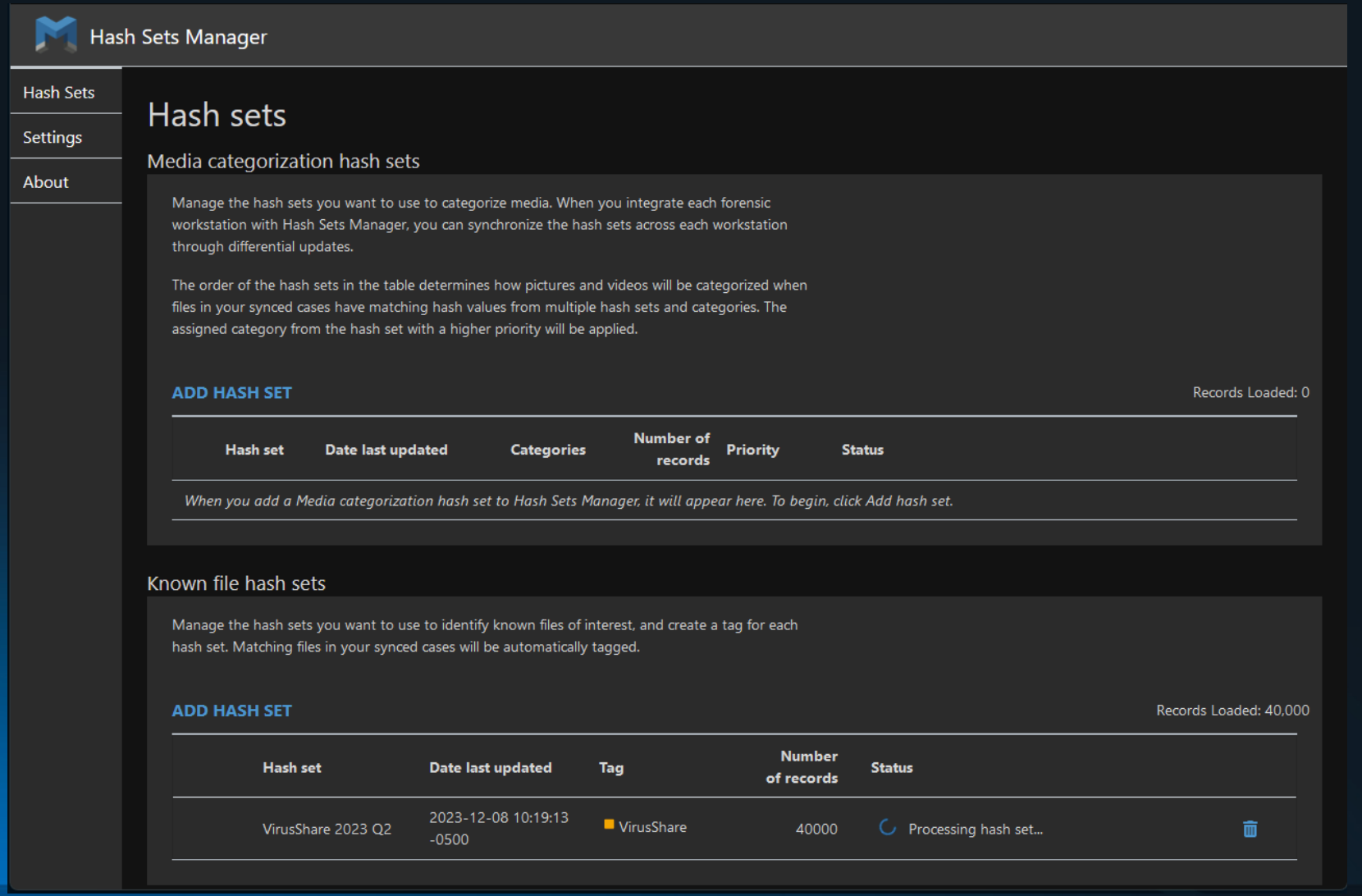
HSM Dashboard

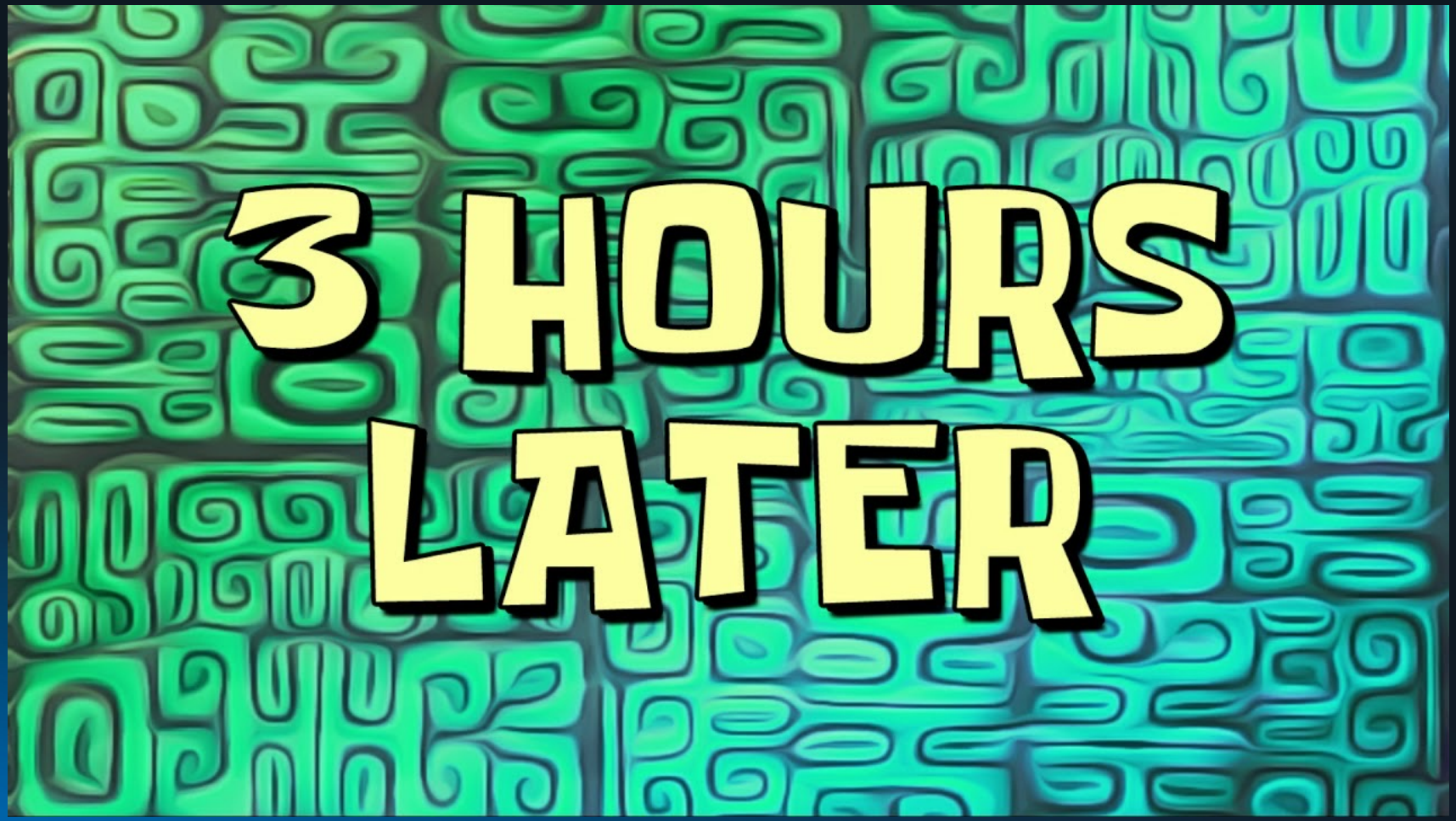


Malware Hash List

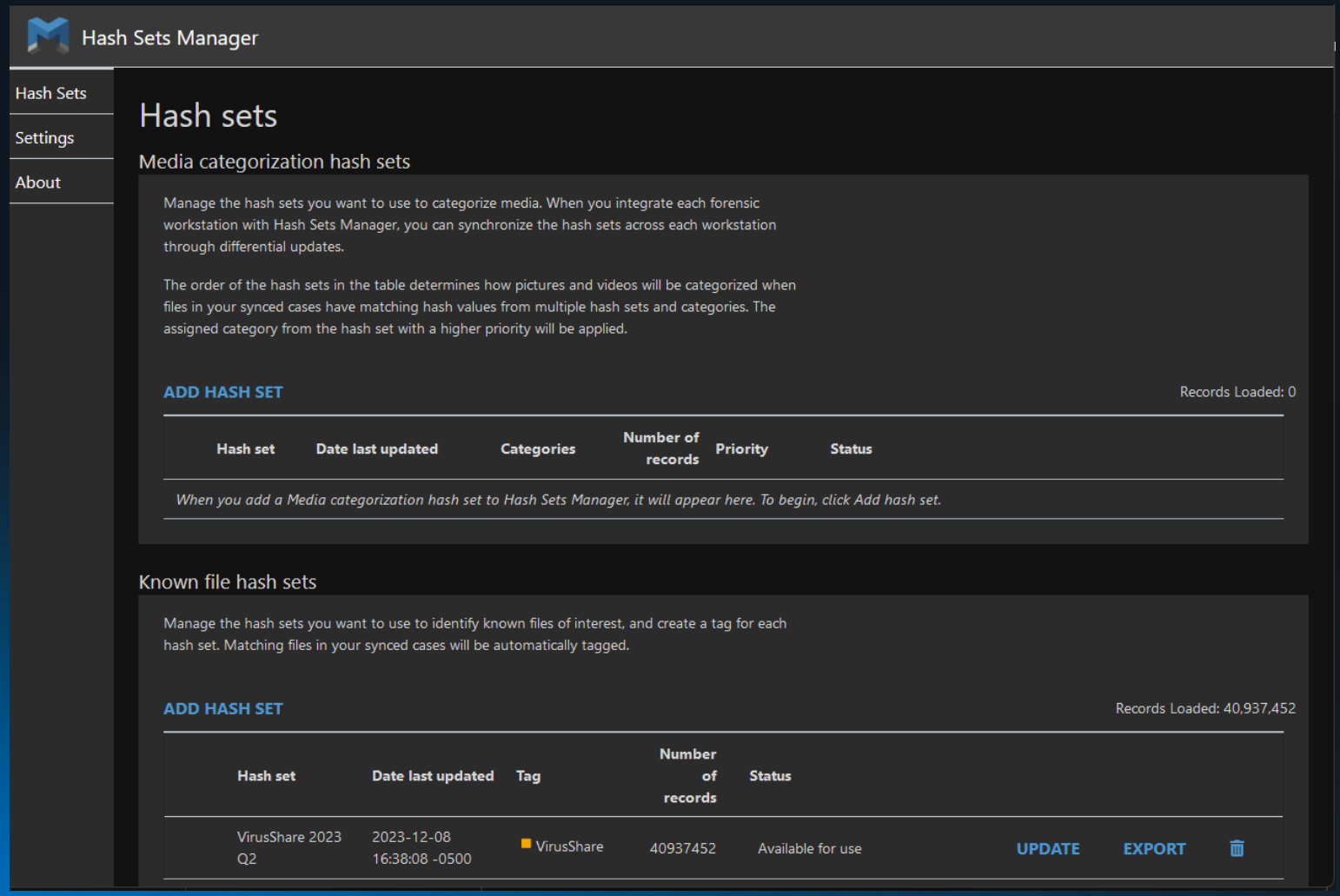


HSM – Adding a Hash Set

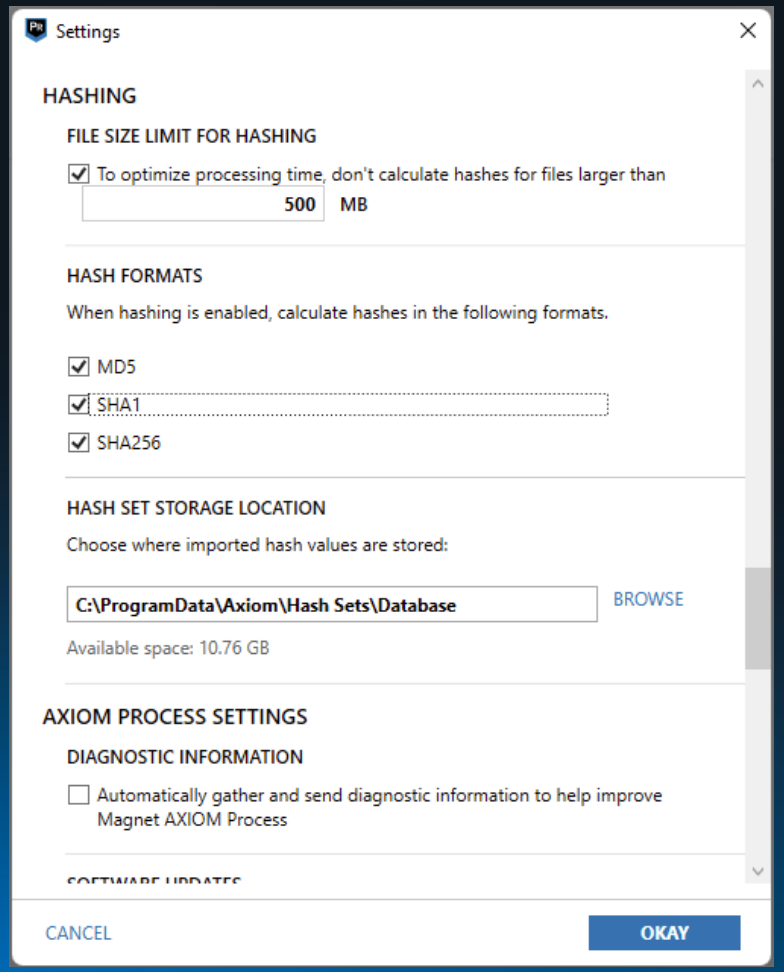


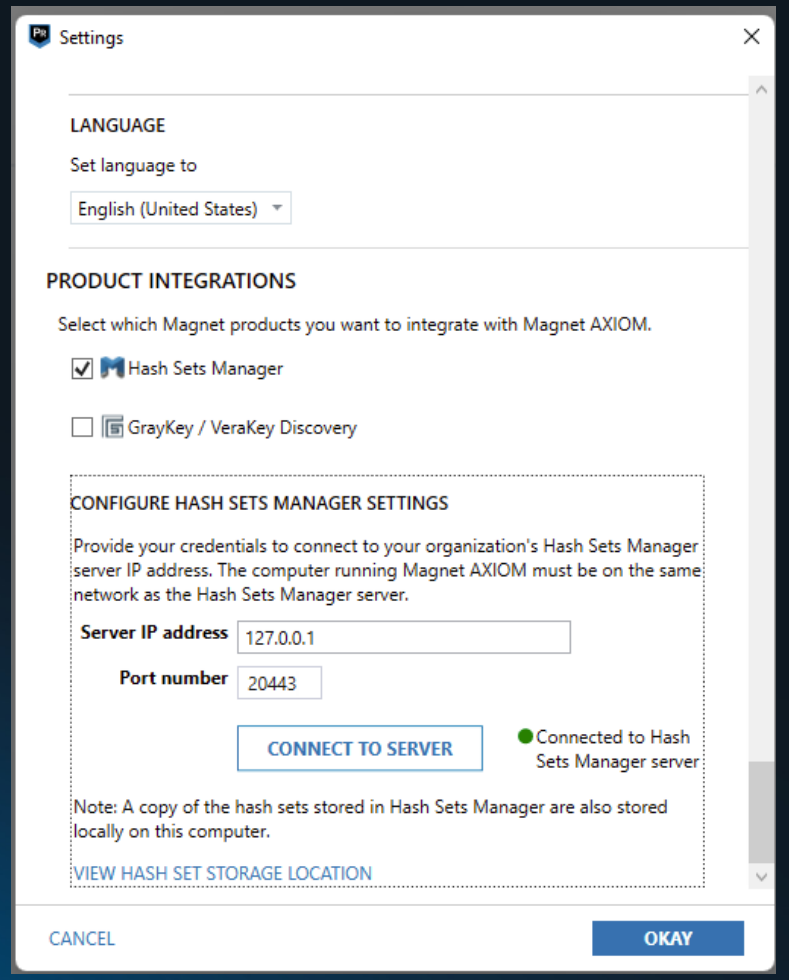

3 HOURS
LATER

HSM - Ready

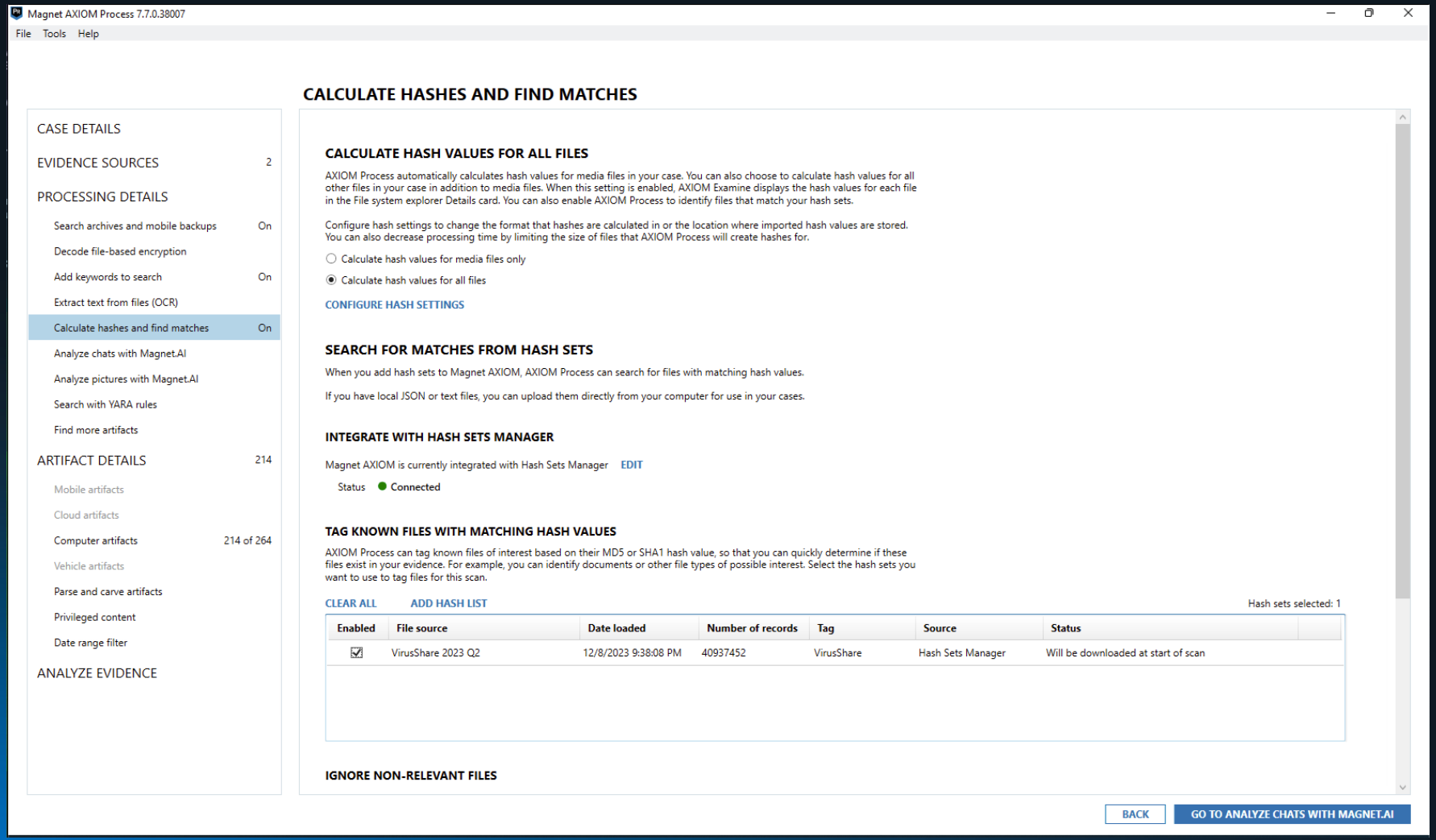

Hash Sets Manager
Hash Sets
Settings
About
Hash sets
Media categorization hash sets
Manage the hash sets you want to use to categorize media. When you integrate each forensic workstation with Hash Sets Manager, you can synchronize the hash sets across each workstation through differential updates.
The order of the hash sets in the table determines how pictures and videos will be categorized when files in your synced cases have matching hash values from multiple hash sets and categories. The assigned category from the hash set with a higher priority will be applied.
ADD HASH SET
Records Loaded: 0
Hash set
Date last updated
Categories
Number of records
Priority
Status
When you add a Media categorization hash set to Hash Sets Manager, it will appear here. To begin, click Add hash set.
Known file hash sets
Manage the hash sets you want to use to identify known files of interest, and create a tag for each hash set. Matching files in your synced cases will be automatically tagged.
ADD HASH SET
Records Loaded: 40,937,452
Hash set
Date last updated
Tag
Number of records
Status
VirusShare 2023 Q2
2023-12-08 16:38:08 -0500
VirusShare
40937452
Available for use
UPDATE
EXPORT

HSM - AXIOM Configuration

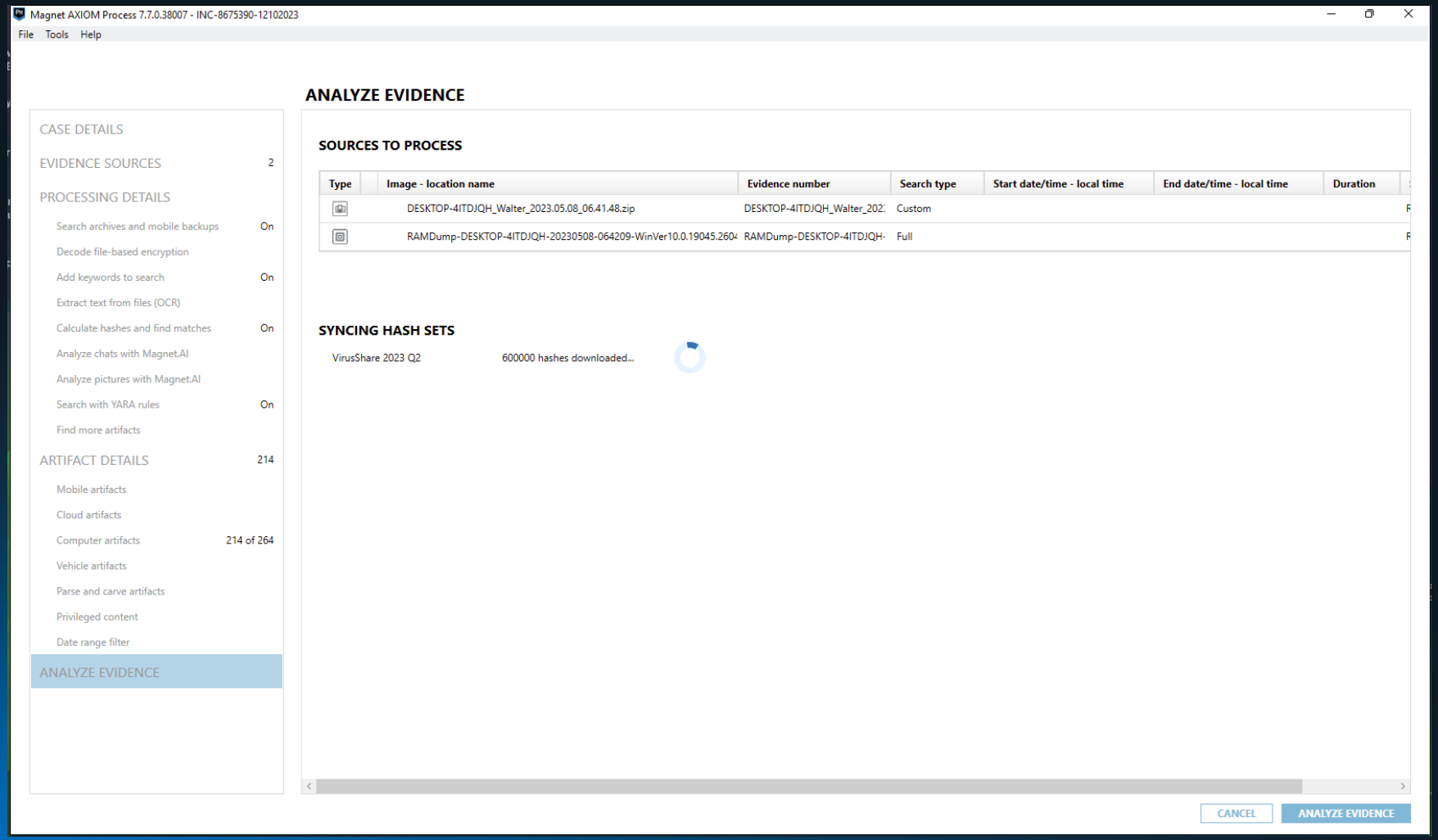




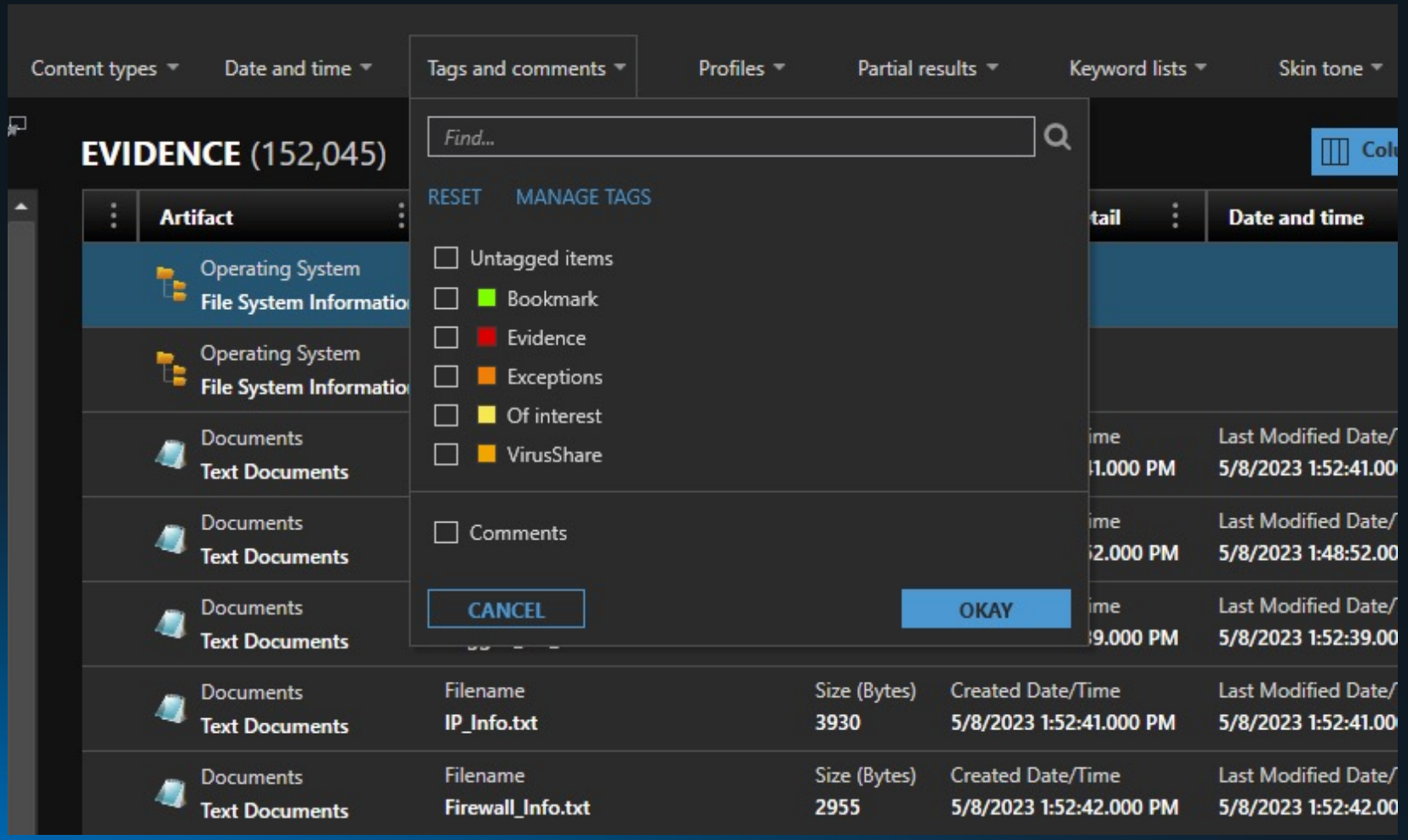
Auto Tagging Hash Matches



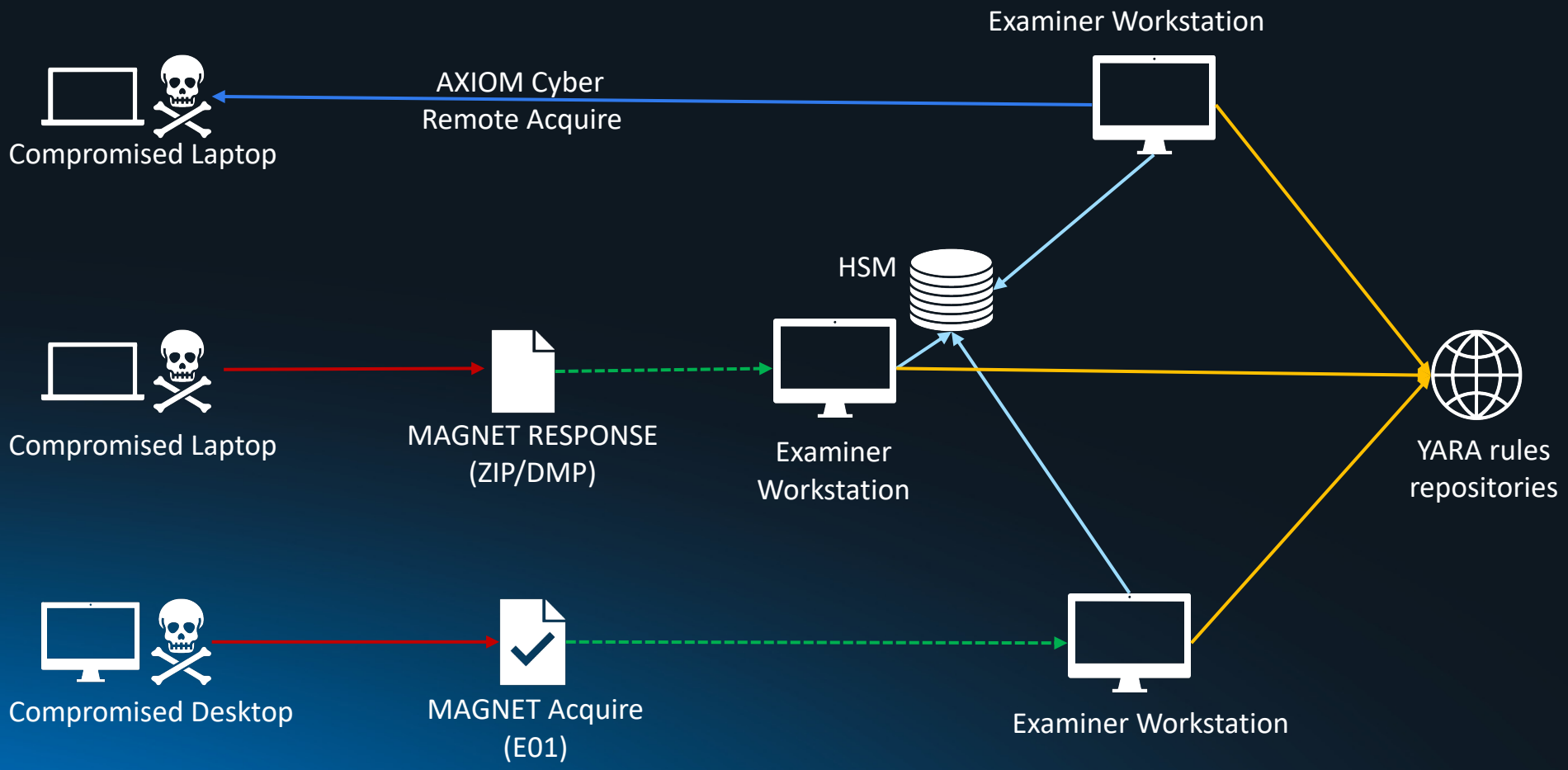
AXIOM HSM Hash Sync



Auto Tagged Results



Connected and Collected



Summary

- There are multiple free tools available for triage collection and RAM capture;
- Tool selection is based on accessibility of the endpoint and the desired collection data;
- Networked and Isolated forensic collection options;
- Scripting collections with PowerShell;
- Leveraging YARA repositories with AXIOM Cyber;
- Integrating known malicious hashes into examination process;
- It Depends.

Resources

Investigating Malware With Free Tools & Magnet AXIOM Cyber

Magnet Forensics Free Tools http://magnetforensics.com/free-tools/

- MAGNET RESPONSE
- MAGNET DUMPIT (WINDOWS, LINUX)
- MAGNET HASH SETS MANAGER
- MAGNET ACQUIRE

Auxtera Project https://theauxteraproject.com

Baker Street Forensics https://bakerstreetforensics.com

detonaRE https://github.com/dwmetz/detonaRE

HTCIA - High Tech Crime Investigators Association https://www.htcia.org

Magnet AXIOM Cyber https://www.magnetforensics.com/magnet-axiom-cyber

Magnet RESPONSE PowerShell https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell

Mal-Hash.ps1 & VTHashSub.ps1 https://github.com/dwmetz/Mal-Hash

VirusShare Hash Lists https://sourceforge.net/projects/mantarayforensics/files/VirusShare_Hash_Sets

Virus Total https://www.virustotal.com

YARA https://virustotal.github.io/yara

Thank You

https://github.com/dwmetz

https://bakerstreetforensics.com

doug.metz@magnetforensics.com

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

https://infosec.exchange/@dwmetz

~~@dwmetz~~