



Investigating Malware with Free Tools & Magnet AXIOM Cyber

Doug Metz, Senior Security Forensics Specialist
Magnet Forensics

A large block of binary code (0s and 1s) displayed in a grid pattern, representing digital data or malware code.

About Me



MAGNET
FORENSICS®

The Auxtera Project



BAKER STREET FORENSICS

D . F . I . R .



HTCIA

Delaware Valley - Philadelphia



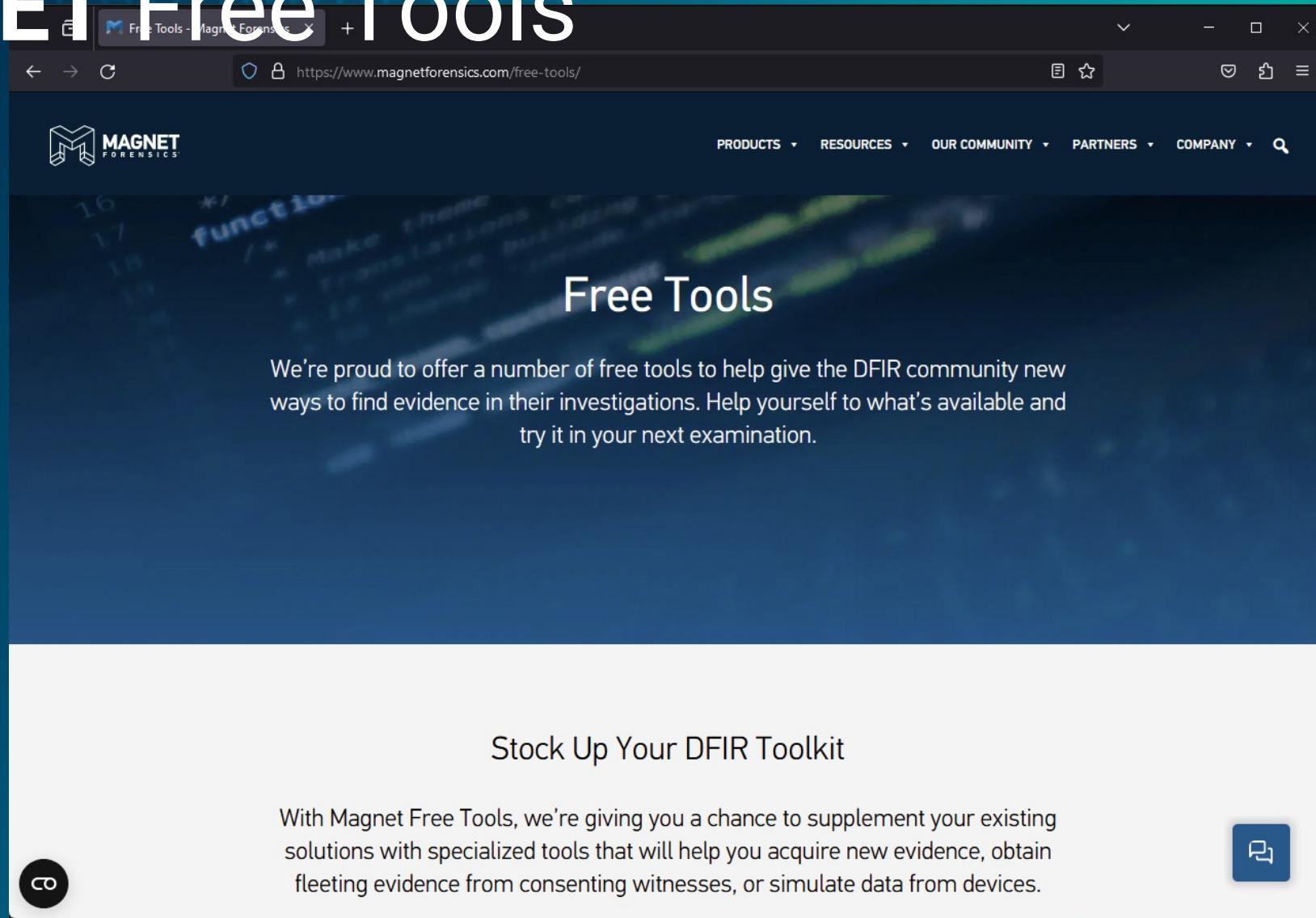


Investigating Malware with Free Tools & Magnet AXIOM Cyber

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



The screenshot shows a web browser window displaying the 'Free Tools' page of the Magnet Forensics website. The URL in the address bar is <https://www.magnetforensics.com/free-tools/>. The page has a dark blue header with the Magnet Forensics logo and navigation links for PRODUCTS, RESOURCES, OUR COMMUNITY, PARTNERS, COMPANY, and a search icon. The main content area features a blurred background image of a computer screen with code and the title 'Free Tools' in large white text. Below the title is a descriptive paragraph: 'We're proud to offer a number of free tools to help give the DFIR community new ways to find evidence in their investigations. Help yourself to what's available and try it in your next examination.' At the bottom of the page, there is a call-to-action section with the heading 'Stock Up Your DFIR Toolkit' and a paragraph explaining the purpose of the free tools. A small circular icon with the letters 'co' is visible on the left side of this section.

We're proud to offer a number of free tools to help give the DFIR community new ways to find evidence in their investigations. Help yourself to what's available and try it in your next examination.

Stock Up Your DFIR Toolkit

With Magnet Free Tools, we're giving you a chance to supplement your existing solutions with specialized tools that will help you acquire new evidence, obtain fleeting evidence from consenting witnesses, or simulate data from devices.

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



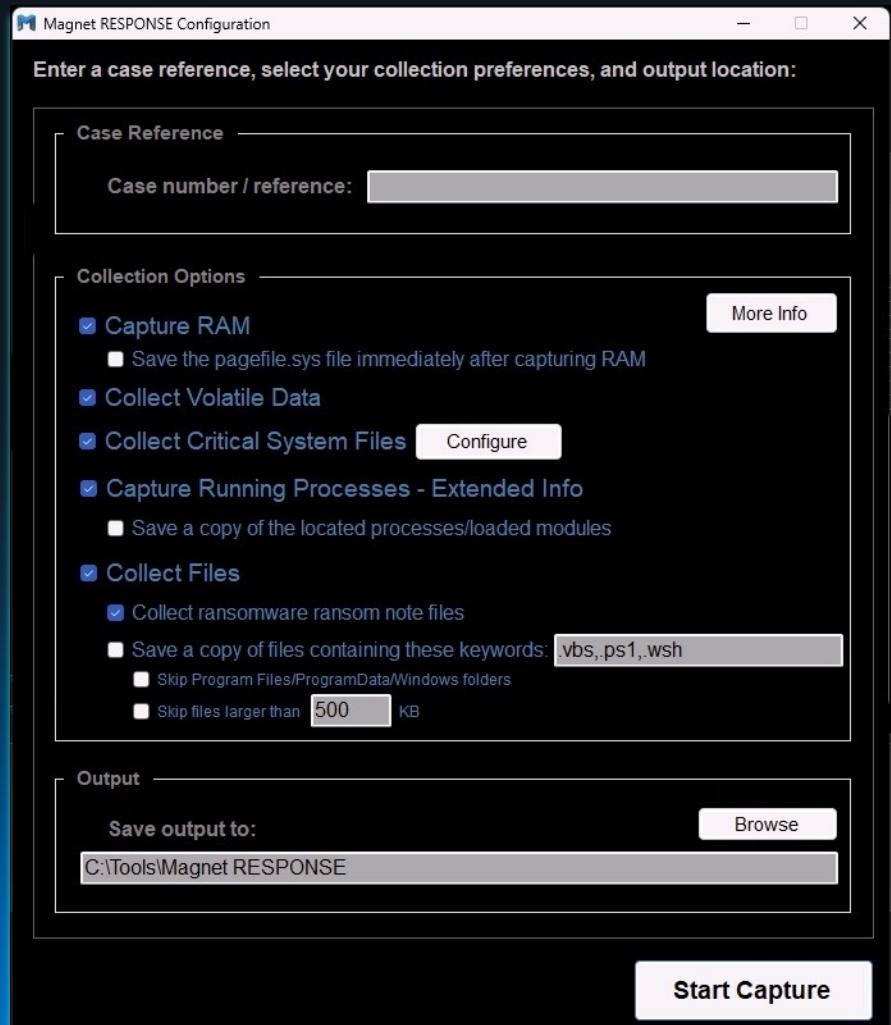
MAGNET RESPONSE

#MVS2024

MAGNET VIRTUAL SUMMIT 2024

MVS

MAGNET RESPONSE



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

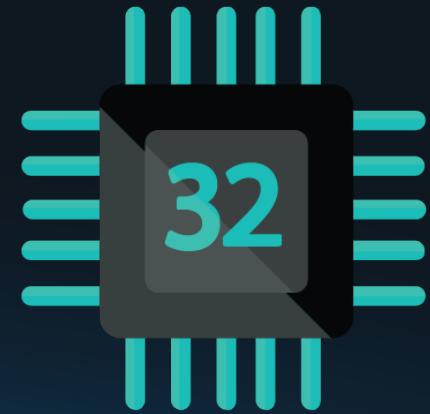
Minimal to no training is required—it's as simple as entering a case name, selecting the collection options and then “start capture.”

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.

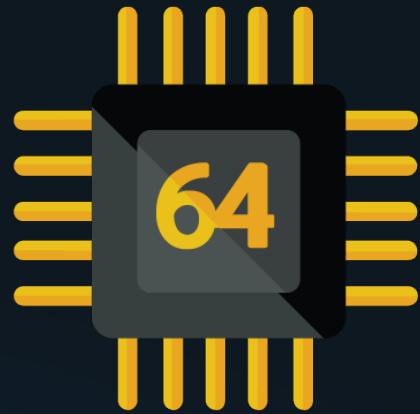
<https://www.magnetforensics.com/resources/magnet-response/>

MAGNET RESPONSE - RAM

Memory collection made easy



VS



MAGNET RESPONSE Output



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
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

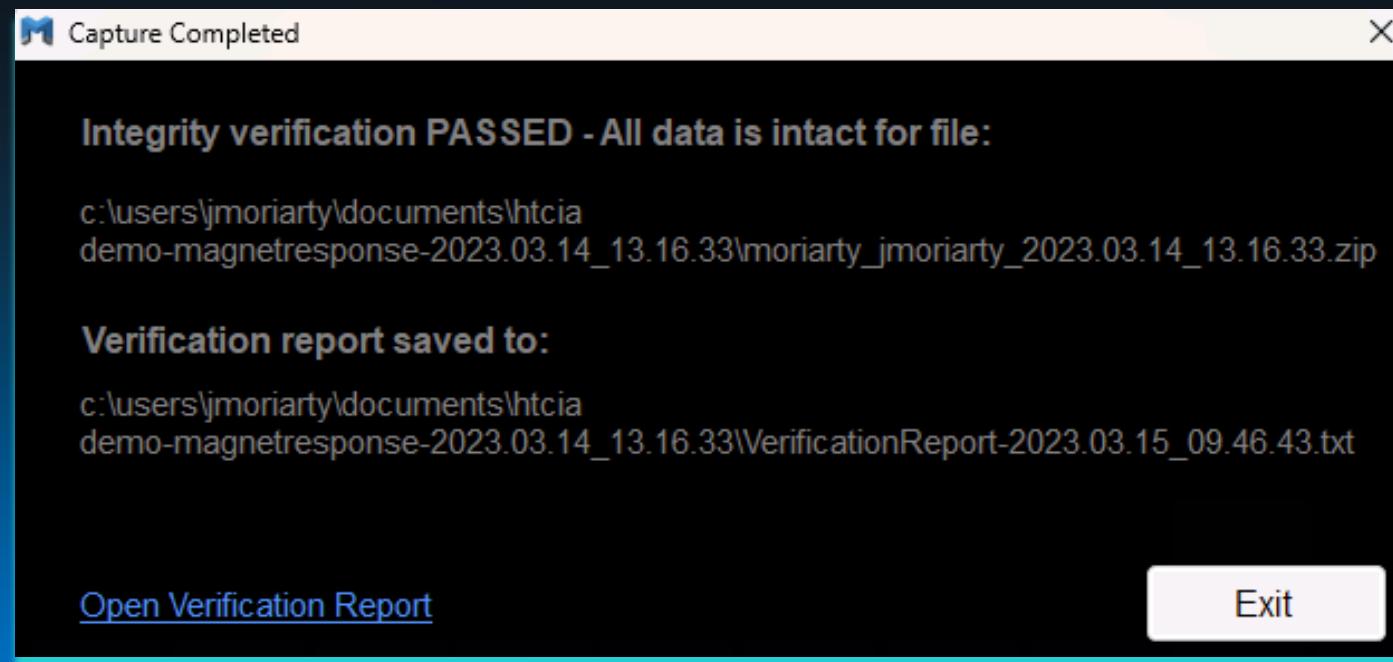
HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 > extracted > Saved_Files				
Name	Date modified	Volatile Data		
Amcache	3/14/2023 1:37 PM			
Browser_History	3/14/2023 1:37 PM			
Jumplists-AutomaticDestinations	3/14/2023 1:37 PM			
Jumplists-CustomDestinations	3/14/2023 1:37 PM			
MFT	3/14/2023 1:37 PM			
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			
SRIIM	3/14/2023 1:37 PM			

HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 > extracted > Volatile_Data				
Name	Date modified	Type	Size	C
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	

MAGNET RESPONSE Verification

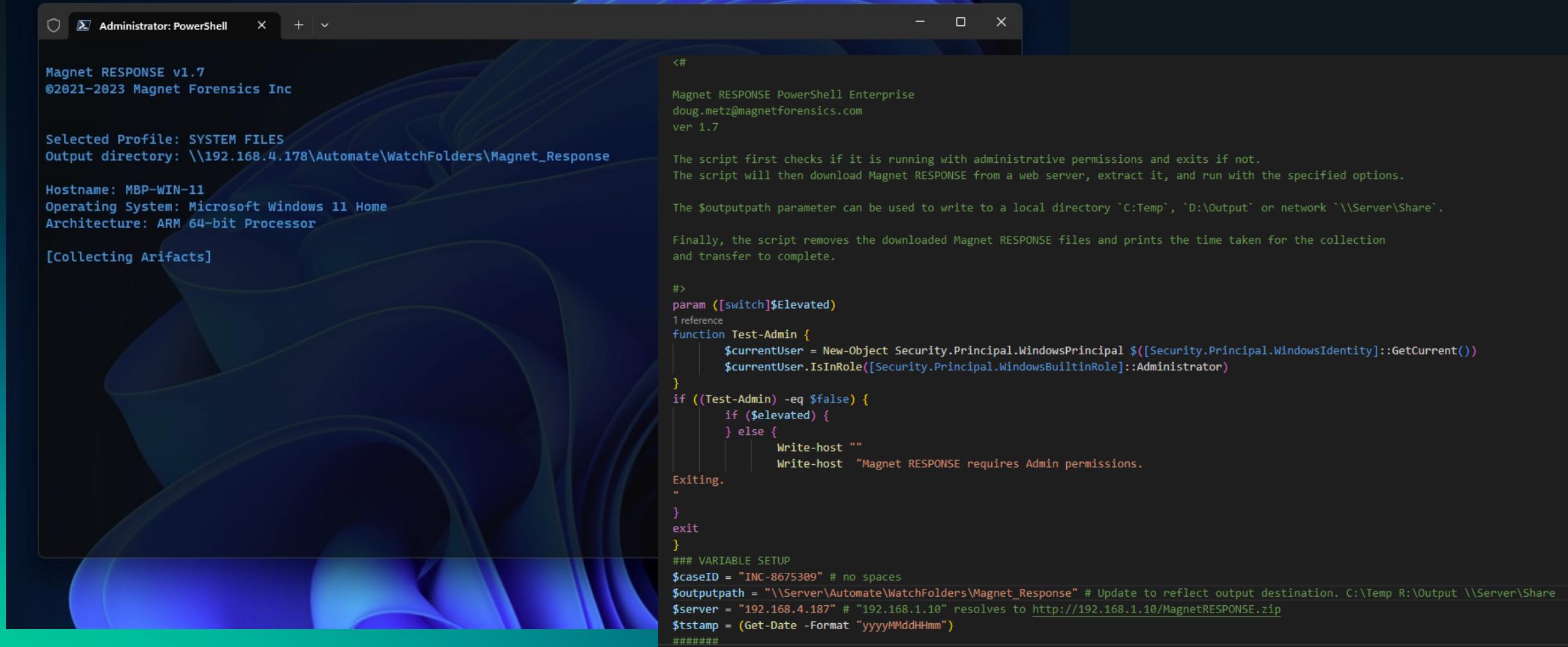
Verifying a Capture Package

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



```
<#  
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.  
}  
#>  
### 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

- /captoreram
 - 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
- /captoreransomnotes
 - 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"
#>
#### System 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

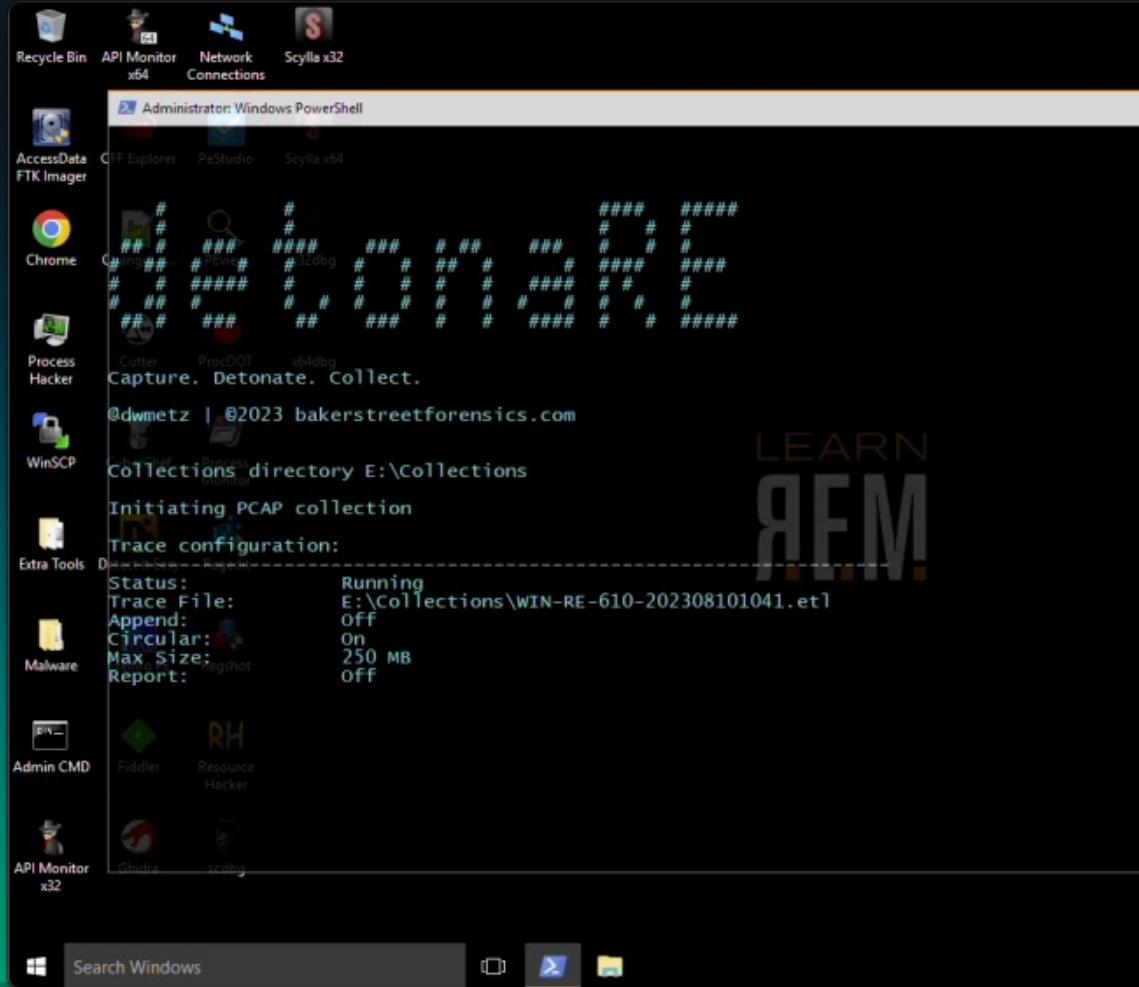
/caseref:caseID – Case ID

\$arguments – Specified in collection profile



Capturing Malware Evidence with **detonaRE**

detonaRE – from Latin, to detonate



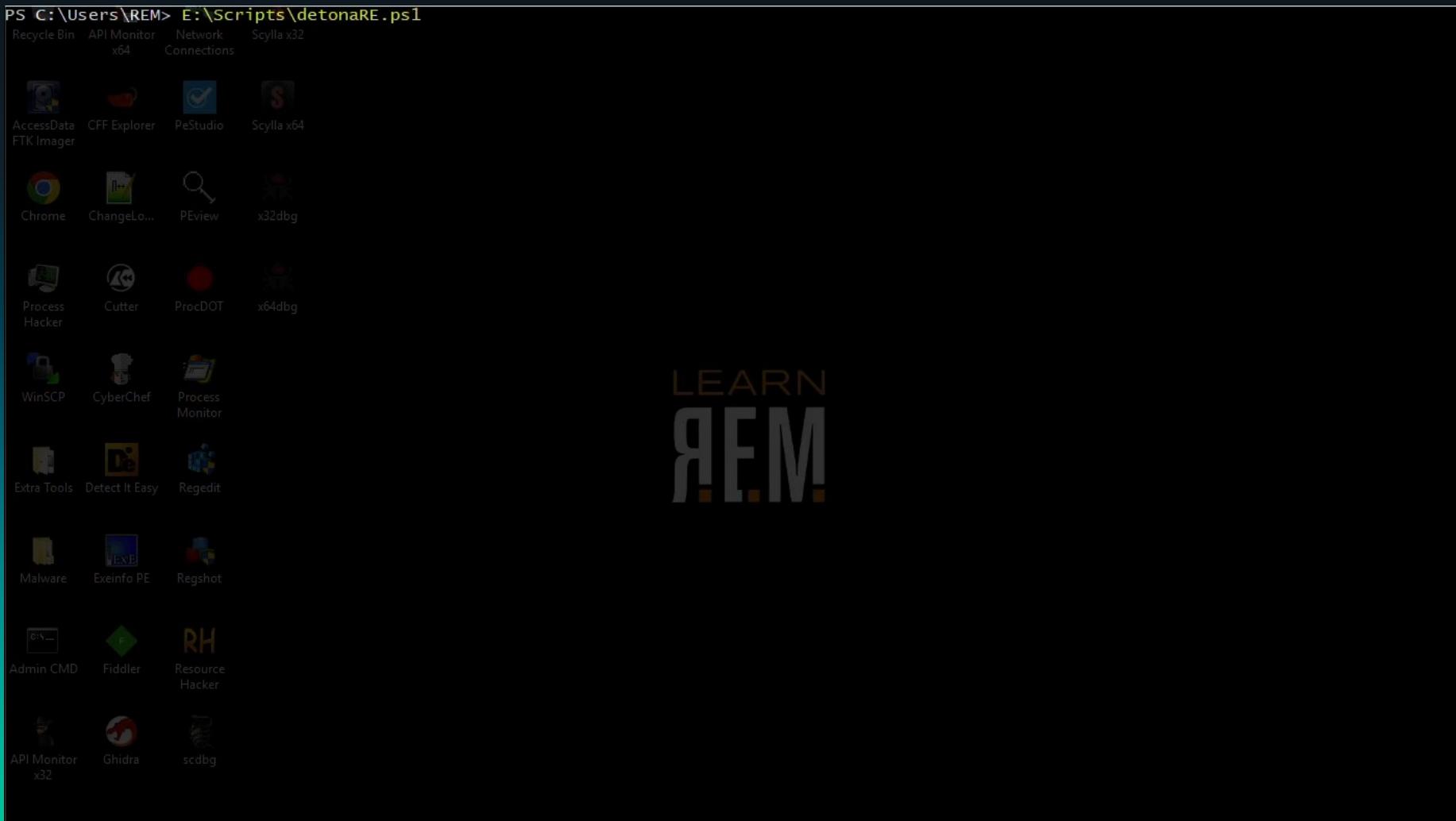
- initiates packet capture
- launches malware sample
- terminates packet capture after specified interval
- initiates evidence collection with [Magnet RESPONSE](#) (memory, process, and triage capture)
- converts collected .etl file (network capture) to .pcap with [etl2pcapng](#).

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



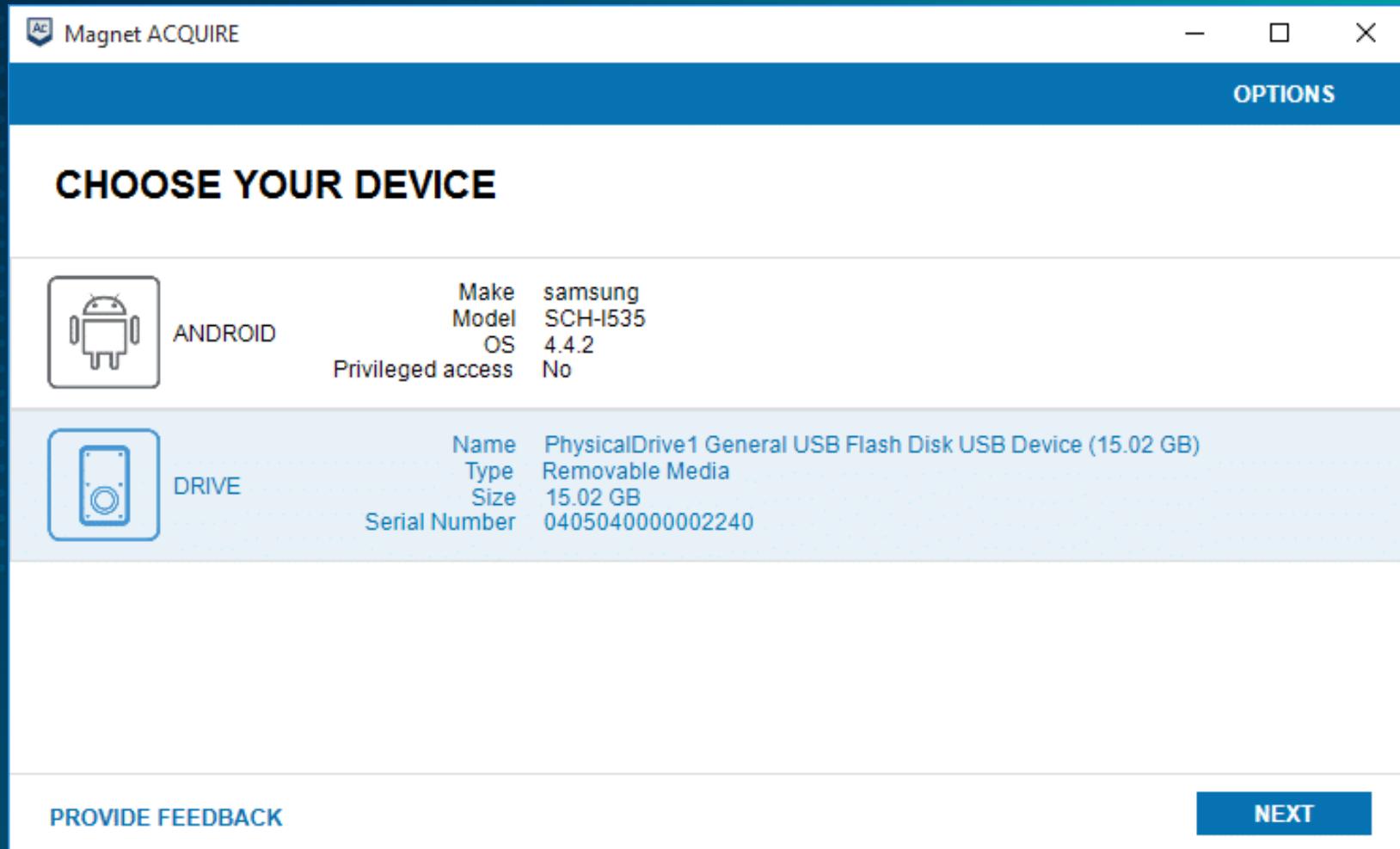
MAGNET ACQUIRE

#MVS2024

MAGNET VIRTUAL SUMMIT 2024

MVS

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

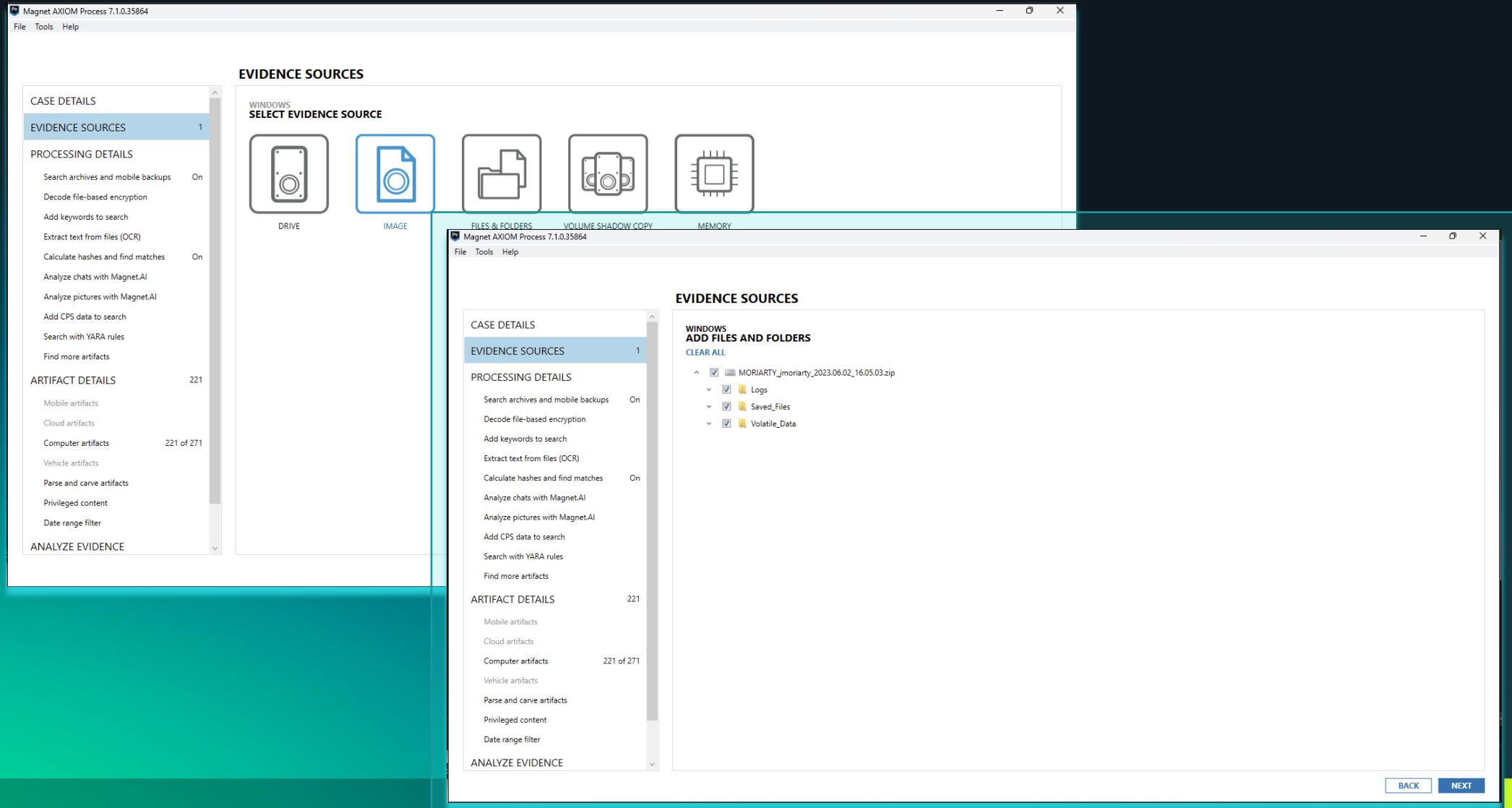


Quick
Root Cause
Analysis

Processing Malware Evidence with **MAGNET AXIOM™ CYBER**

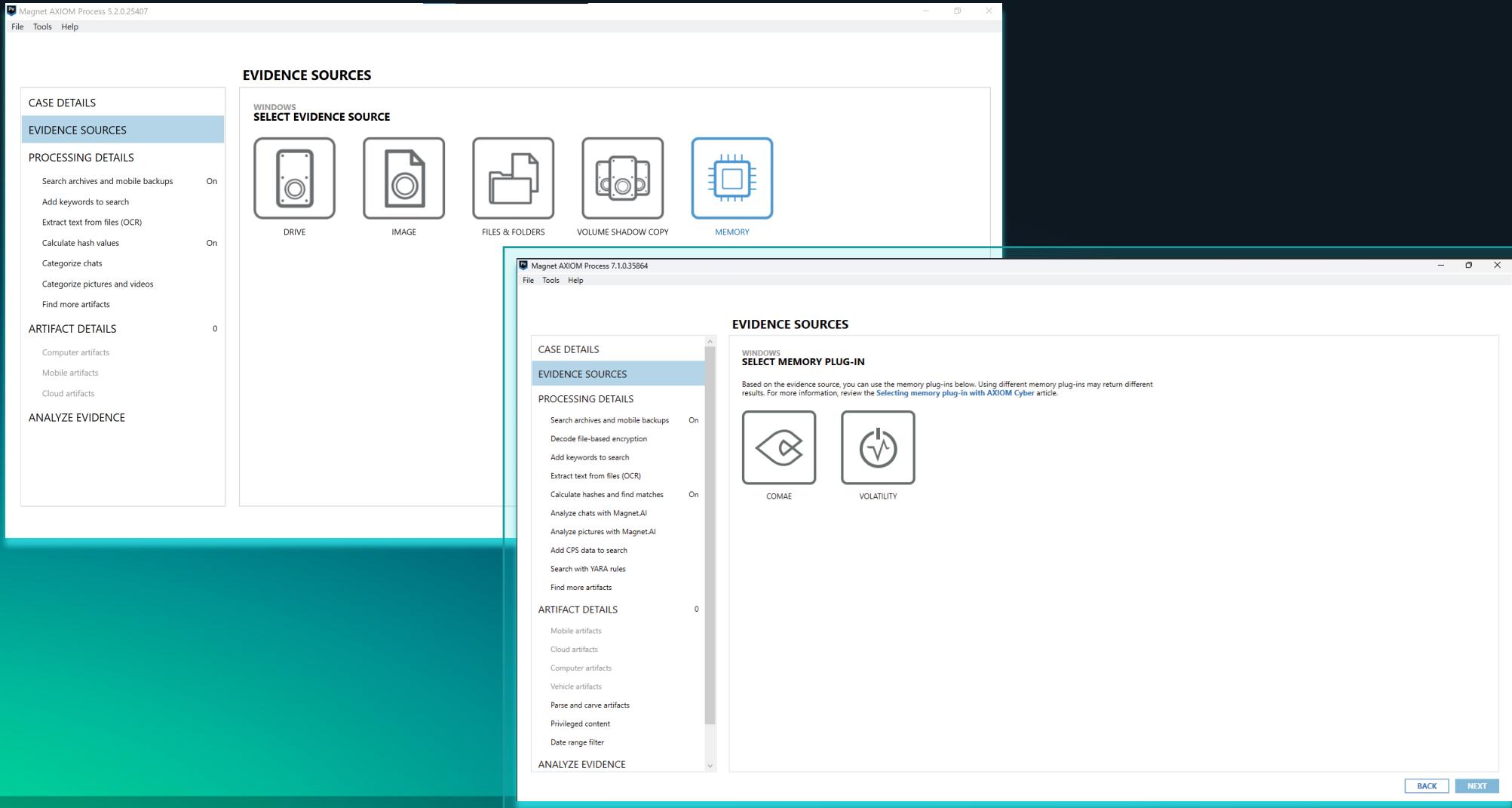
Triage Processing

Computer > Windows > Load Evidence > IMAGE



Comae Memory Processing

Computer > Windows > Load Evidence
> MEMORY



Artifacts from RESPONSE RAM & Triage

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 0

Potential Cloud Evidence Leads

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

No picture added

[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

No picture added

[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 2,508,197

Category	Count
Memory	140,821
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

VirusTotal Lookups with AXIOM Cyber

The screenshot shows the Magnet AXIOM Examine interface. On the left, the file system navigation pane shows evidence from a ZIP archive named 'DESKTOP-4ITDJQH_Walter_2023.05.08_06.41.48.zip'. The main pane displays a list of files under the 'ALL EVIDENCE' section, with 'sihost.exe' selected. A context menu is open over 'sihost.exe', and the option 'Check with VirusTotal' is highlighted with a red box. To the right, the 'sihost.exe' details pane shows its file path and preview content.

Name	Type	File e...	Size ...	Created
CRYPTBASE.dll	File .dll	34,152	9/8/2022 3:07:13.9	
ShareHost.dll	File .dll	1,119,232	2/10/2023 2:12:10	
Windows.Storage.dll	File .dll	7,978,384	2/10/2023 2:12:38	
CoreMessaging.dll	File .dll	984,952	2/10/2023 2:12:51	
CoreUIComponents.dll	File .dll	3,537,520	9/8/2022 3:06:55.2	
mswsock.dll	File .dll	418,416	9/8/2022 3:07:11.1	
8thRadioMedia.dll	File .dll	107,520	9/8/2022 3:07:02.7	
DEVOBJ.dll	File .dll	166,888	9/8/2022 3:07:12.7	
rsaenh.dll	File .dll	207,080	9/8/2022 3:07:12.4	
sspicli.dll	File .dll	188,584	2/10/2023 2:12:56	
uxtheme.dll	File .dll	627,200	2/10/2023 2:13:10	
execemodelproxy.dll	File .dll	80,896	9/8/2022 3:06:39.4	
schannel.DLL	File .DLL	602,624	2/15/2023 3:49:31	
ncryptsslp.dll	File .dll	137,896	9/8/2022 3:07:12.4	
keepaliveprovider.dll	File .dll	72,192	9/8/2022 3:07:00.7	
vm3dum64_10.dll	File .dll	461,752	11/3/2022 3:54:38	
DataExchange.dll	File .dll	237,568	9/8/2022 3:06:38.8	
directmanipulation.dll	File .dll	629,160	9/8/2022 3:06:38.8	
windowscodecs.dll	File .dll	1,785,544	9/8/2022 3:06:56.8	
sihost.exe	File .exe			

VirusTotal Lookups with AXIOM Cyber

The screenshot shows the AXIOM Cyber interface with a modal dialog and a background VirusTotal analysis page.

Modal Dialog (Left):

- Header: "Opening VirusTotal"
- Text: "VirusTotal will now open in an internet browser. AXIOM Examine will share this file's hash with VirusTotal to search for any known information about the file, but will not upload the file itself."
- Text: "If a hash doesn't yet exist for this file, AXIOM Examine will generate a hash and then share the hash value with VirusTotal. Depending on the file size, this process might take some time."
- Checkboxes:
 - Don't show me this again
- Buttons: "CANCEL" and "OPEN VIRUSTOTAL"

VirusTotal Analysis Page (Background):

- File Hash: 8ee21a0ba8849d31c265b4090a9e2ebe8ba66f58a8f71d4e96509e8a78f7db00
- File Name: sibhost.exe
- File Type: EXE
- Analysis Status: 0 / 72
- File distributed by Microsoft
- Size: 109.00 KB
- Last Analysis Date: 1 day ago
- Tags: assembly, checks-disk-space, detect-debug-environment, idle, long-sleeps, 64bits, known-distributor
- Actions: Reanalyze, Similar, More

Analysis Results Table:

Scanning Engine	Result
AhnLab-V3	Undetected
ALYac	Undetected
Arcabit	Undetected
AVG	Undetected
Baidu	Undetected
BitDefenderTheta	Undetected
ClamAV	Undetected
CMC	Undetected
Cybereason	Undetected
CrowdStrike Falcon	Undetected
Cylance	Undetected

VirusTotal Queries with PowerShell

```
.,;:::cccccc:;.          . . . . .
.:ccc1lll0o0ddx;.        .'cl0oddo1cc::::.
.:ccc1lll0o0ddxo.       ..coxxxxd1:,'..
'ccccclll0o0ddd'       ...'lxkxxxo:'.
'ccccclll0o0ddd'       ..:lx0k1,:oxo..
':ccccclll0o0ddo.     .:dk0000kkd''.
.:ccccclll0o0odo.   ...;lxk00000kkd;
.:ccccclll0o0dddc:coxKKK000000x:.
'ccccclll0o0o0ddxxxxxxkkk0000x:.
.ccc1ll0o0o0dddxxxxxxxkxlc..
':lll0o0o0dddxxxxxxc:.
.'';:clo0dd0d0c:...
.....''

Mal-Hash v1.6
https://github.com/dwmetz/Mal-Hash
@dwmetz | bakerstreetforensics.com

[ Enter path and filename: /Users/dmetz/Desktop/MALWARE/IcedID/52d3dd78d3f1a14e18d0689ed8c5b43372f9e76401ef1ff68522575e6251d2cf.exe ]]

Submitting SHA256 hash 52D3DD78D3F1A14E18D0689ED8C5B43372F9E76401EF1FF68522575E6251D2CF to Virus Total

VIRUS TOTAL RESULTS:

scans      : @{Bkav=; Lionic=; Elastic=; MicroWorld-eScan=; CMC=; CAT-QuickHeal=; ALYac=; Cylance=; Zillya=; Sangfor=;
             K7AntiVirus=; Alibaba=; K7GW=; CrowdStrike=; BitDefenderTheta=; VirIT=; Cyren=; Symantec=; tehtris=; ESET-NOD32=;
             APEX=; Paloalto=; ClamAV=; Kaspersky=; BitDefenders=; NANO-Antivirus=; SUPERAntiSpyware=; Avast=; Tencent=; TACHYON=;
             Emsisoft=; Baidu=; F-Secure=; DrWeb=; VIPRE=; TrendMicro=; McAfee-GW-Edition=; Trapmine=; FireEye=; Sophos=;
             Ikarus=; Jiangmin=; Webroot=; Google=; Avira=; Antiy-AVL=; Microsoft=; Gridinsoft=; Xcitium=; Arcabit=; ViRobot=;
             ZoneAlarm=; GData=; Cynet=; AhnLab-V3=; Acronis=; McAfee=; MAX=; VBA32=; MalwareBytes=; Panda=; Zoner=;
             TrendMicro-HouseCall=; Rising=; Yandex=; SentinelOne=; MaxSecure=; Fortinet=; AVG=; Cybereason=; DeepInstinct=}
scan_id    : 52d3dd78d3f1a14e18d0689ed8c5b43372f9e76401ef1ff68522575e6251d2cf-1689086525
sha1       : 704b84d525eeefca6fa7eeb1cf0c94f861310c224
resource   : 52D3DD78D3F1A14E18D0689ED8C5B43372F9E76401EF1FF68522575E6251D2CF
response_code: 1
scan_date  : 2023-07-11 14:42:05
```

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.*

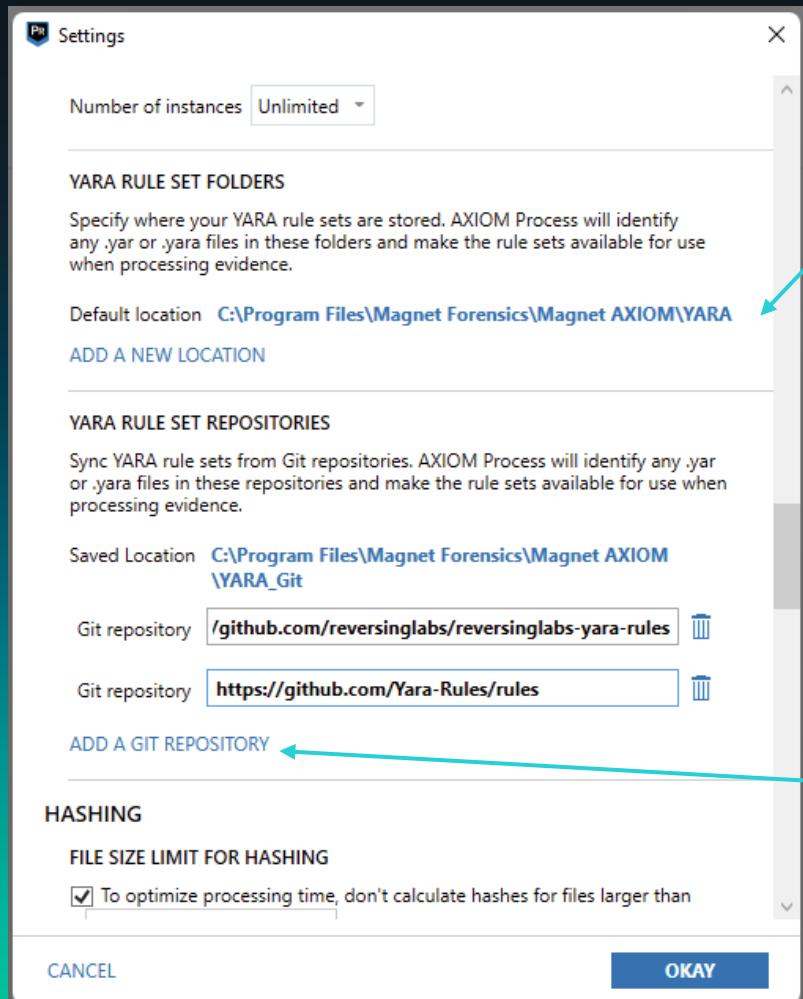
MAGNET AXIOM CYBER & YARA

#MVS2024

MAGNET VIRTUAL SUMMIT 2024

MVS

YARA Repositories



Manually add rules to this folder



Add additional GitHub repositories to sync

Processing with YARA Rules

The screenshot shows the 'SEARCH WITH YARA RULES' interface in Magnet AXIOM. On the left, there's a sidebar with 'CASE DETAILS' and 'PROCESSING DETAILS' sections. Under 'PROCESSING DETAILS', 'Search with YARA rules' is selected. The main area displays 'YARA RULE SETS' with a note about using YARA rules to identify matching files. It shows a list of rule sets with columns for 'Enabled', 'Rule set name', 'Source path', and 'Date created'. A search bar at the top allows filtering by name or source path. At the bottom right, there are 'BACK' and 'GO TO FIND MORE ARTIFACTS' buttons.

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.Vity.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.Mockety.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	4/5/2023 12:02:59 PM
<input type="checkbox"/>	Win32.Virus.Negty.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

New YARA Rules

Magnet AXIOM Process 7.7.0.38007
File Tools Help

SEARCH WITH YARA RULES

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 folder(s) and 2 Git repo(s). [EDIT](#)

Search by name or source path...

Enabled	Rule set name	Source path	Source	Date created
<input type="checkbox"/>	Win32.Ransomware.Ladon.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input checked="" type="checkbox"/>	JJencode.yar	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers	Git	12/8/2023 10:49:32 AM
<input type="checkbox"/>	Win32.Ransomware.LeChiffre.ya...	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	packer.yar	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers	Git	12/8/2023 10:49:32 AM
<input type="checkbox"/>	Win32.Ransomware.LockBit.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	Win32.Ransomware.Lolkeky.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	Win32.Ransomware.LooCipher....	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	packer_compiler_signatures.yar	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers	Git	12/8/2023 10:49:32 AM
<input type="checkbox"/>	Win32.Ransomware.Lorenz.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	Win32.Ransomware.Mafia.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	peid.yar	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers	Git	12/8/2023 10:49:32 AM
<input type="checkbox"/>	Win32.Ransomware.Magniber.y...	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	tweetable-polyslot-png.yar	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA_Git\rules\packers	Git	12/8/2023 10:49:33 AM
<input type="checkbox"/>	Win32.Ransomware.Major.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM
<input type="checkbox"/>	Win32.Ransomware.Makop.yara	C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022...	Magnet Forensics	12/13/2022 3:14:57 PM

Rules selected: 0

SELECT ALL ADD NEW RULE SET REFRESH SYNC WITH GIT

BACK GO TO FIND MORE ARTIFACTS

Search with YARA rules

! On

What's in your YARA?

Organization specific
indicators

Indicators from
previous incidents

Keywords or codewords
for sensitive projects

? ? ?

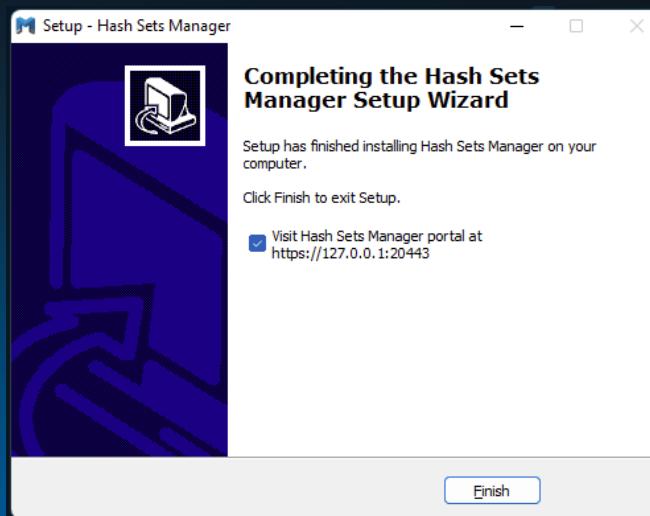
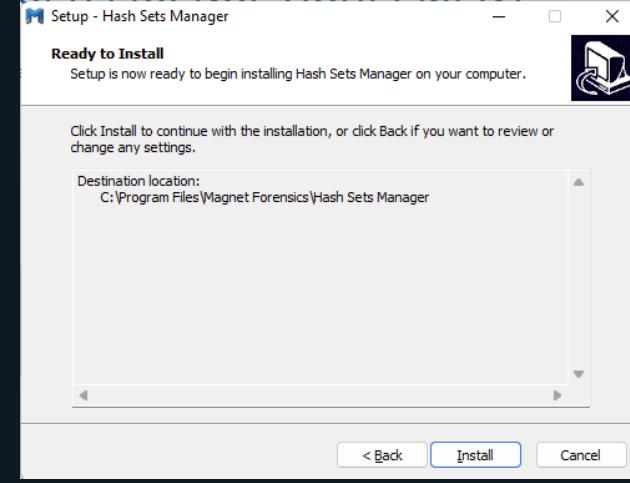
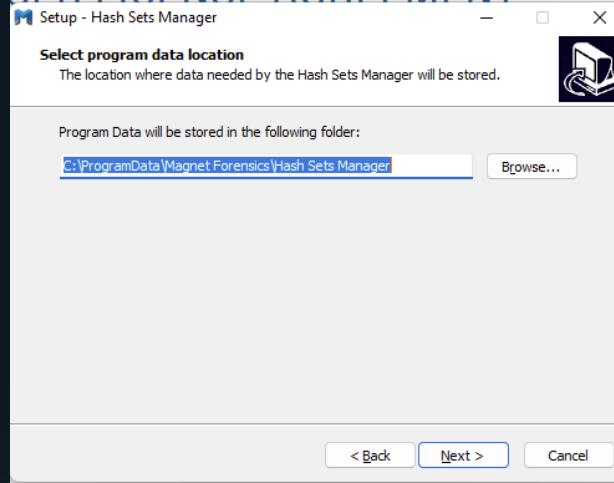
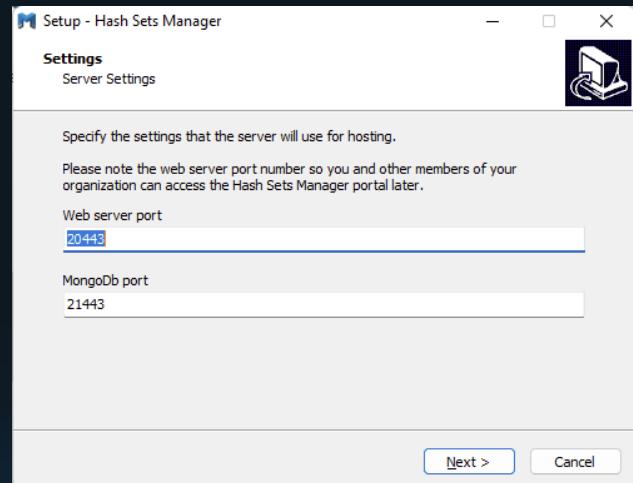
MAGNET Hash Sets Manager

#MVS2024

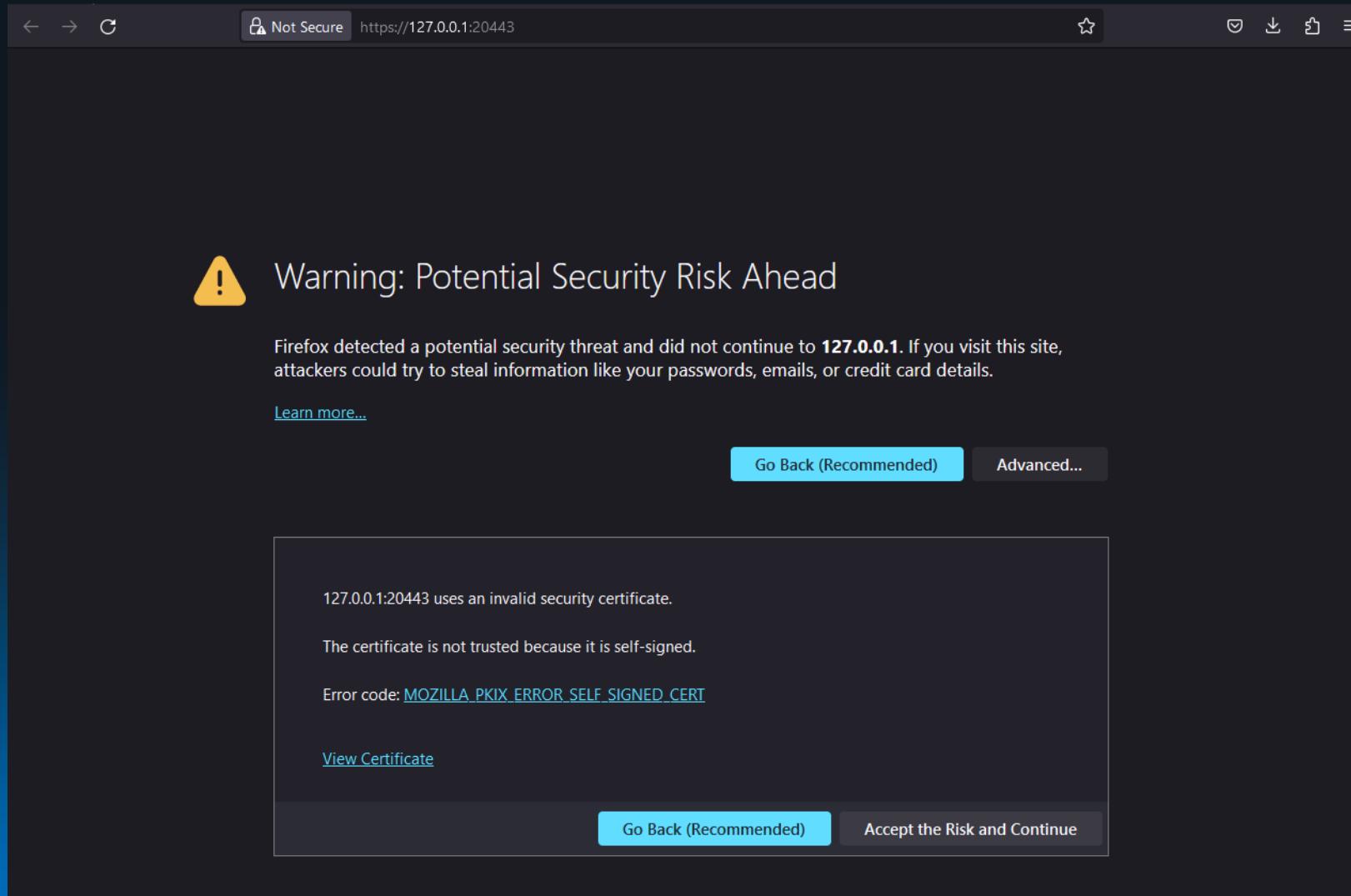
MAGNET VIRTUAL SUMMIT 2024

MVS

Hash Sets Manager (HSM) Installation



HSM Certificate Warning



HSM Dashboard

The screenshot shows a web browser window titled "Hash Sets Manager" at the URL <https://127.0.0.1:20443>. The interface is dark-themed.

Media categorization hash sets:

- ADD HASH SET** button.
- Table headers: Hash set, Date last updated, Categories, Number of records, Priority, Status.
- Text: "When you add a Media categorization hash set to Hash Sets Manager, it will appear here. To begin, click Add hash set."
- Text: "Records Loaded: 0"

Known file hash sets:

- ADD HASH SET** button.
- Table headers: Hash set, Date last updated, Tag, Number of records, Status.
- Text: "When you add a Known file hash set to Hash Sets Manager, it will appear here. To begin, click Add hash set."
- Text: "Records Loaded: 0"

Malware Hash List

The screenshot shows the SourceForge website interface. At the top, there's a navigation bar with links for "Open Source Software", "Business Software", "Resources", "For Vendors", "Help", "Create", "Join", and "Login". A search bar is also present. Below the navigation, there's an advertisement for Avast Software.

The main content area displays the "MantaRay Forensics Files" project page. The title is "MantaRay Forensics Files" and it's described as "An Open Source Project | Since 2013 | SANS SIFT Automation | Hash Sets". It's brought to you by "mantaray4nscs".

The page features a "Files" tab selected, showing a list of files:

Name	Modified	Size	Downloads / Week
Parent folder			
Autopsy	2023-07-30	18	18
EnCase	2023-07-30	2	2
RAW	2023-07-30	1	1
XWays	2023-07-30	0	0
README.txt	2023-07-30	4.4 kB	1
Totals: 5 Items		4.4 kB	22

Below the file list, there's a note: "30 July 2023" and "VirusShare.com MantaRay Forensics Refined Hash Set (v.2023_Q2)".

On the right side of the main content, there's another advertisement for "Grayscale" and a "Recommended Projects" sidebar listing "Brakeman", "Apache OpenOffice", "KeePass", and "DeSmuME".

HSM – Adding a Hash Set

The screenshot shows the Hash Sets Manager application interface. On the left is a vertical navigation bar with a logo, 'Hash Sets Manager', and three menu items: 'Hash Sets' (selected), 'Settings', and 'About'.

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

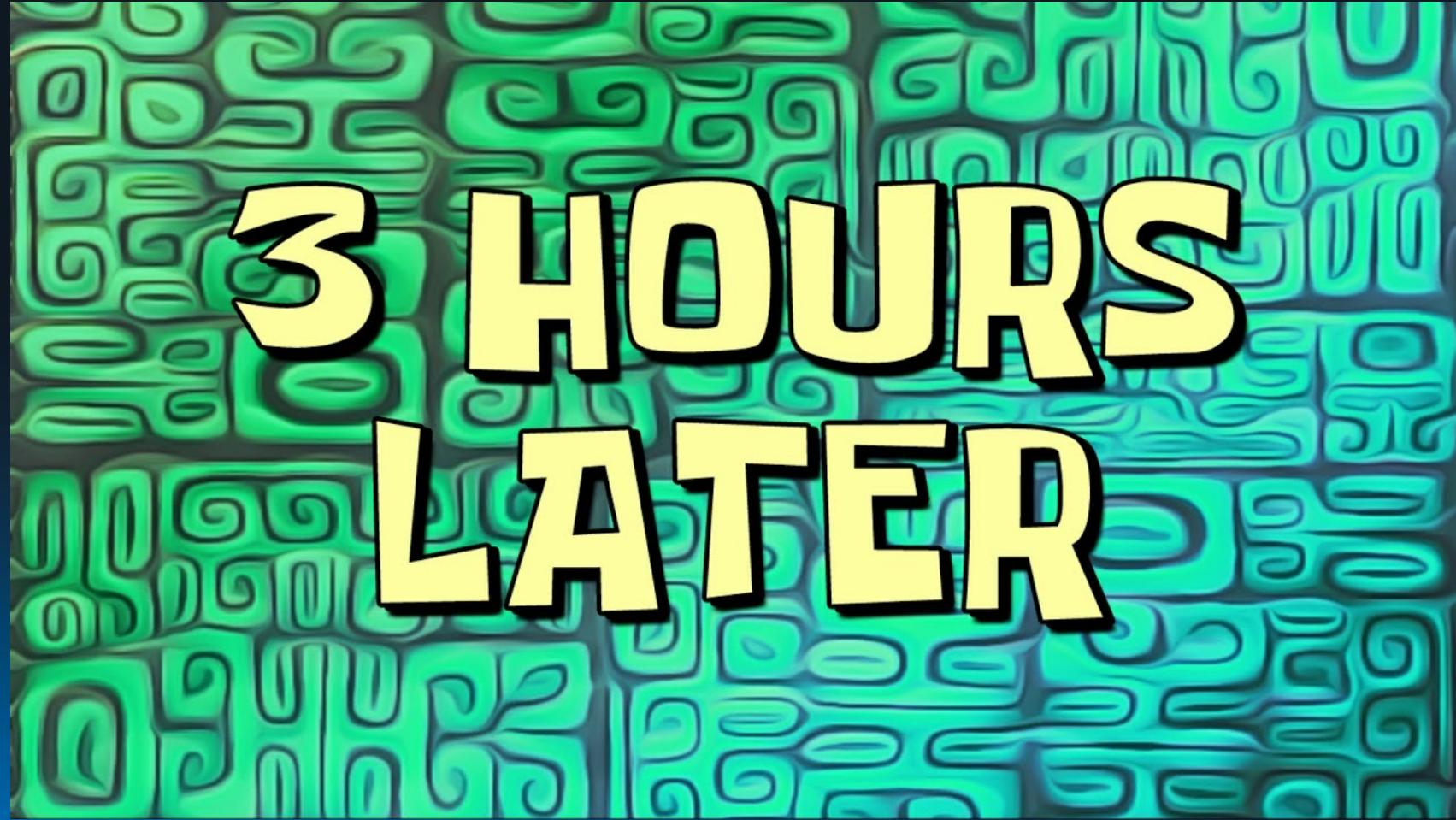
Hash set	Date last updated	Categories	Number of records	Priority	Status
----------	-------------------	------------	-------------------	----------	--------

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: 40,000

Hash set	Date last updated	Tag	Number of records	Status
VirusShare 2023 Q2	2023-12-08 10:19:13 -0500	■ VirusShare	40000	Processing hash set... (refresh icon) (trash icon)



HSM - Ready

The screenshot shows the Hash Sets Manager application interface. On the left is a vertical navigation menu with options: Hash Sets (selected), Settings, and About. The main content area is divided into two sections:

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

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.					

Records Loaded: 0

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.

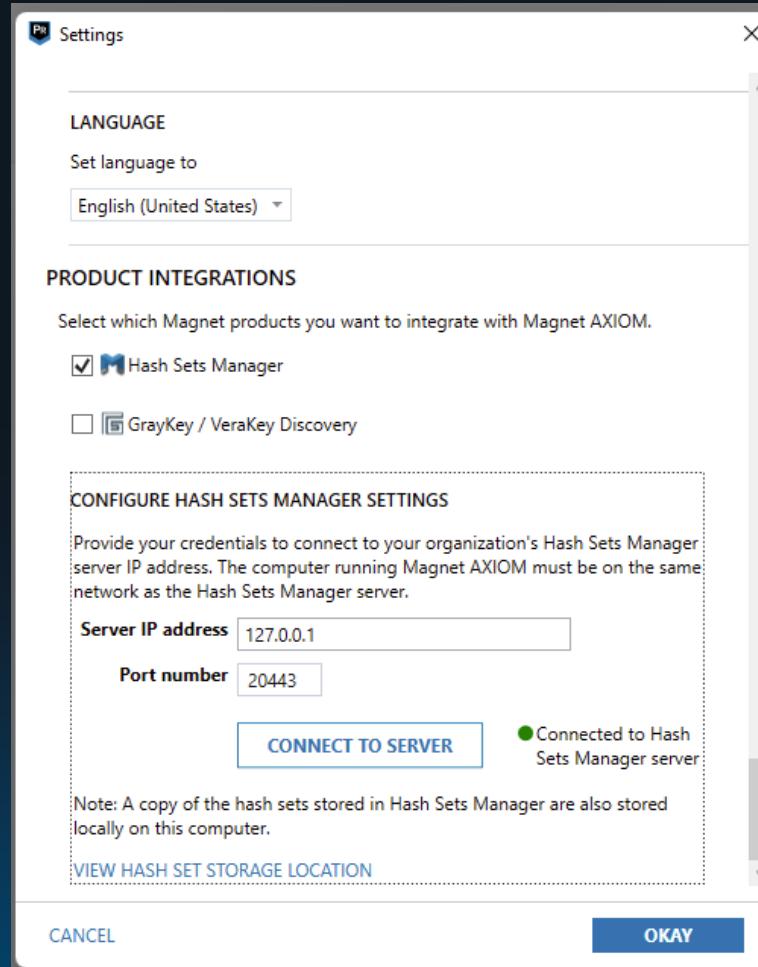
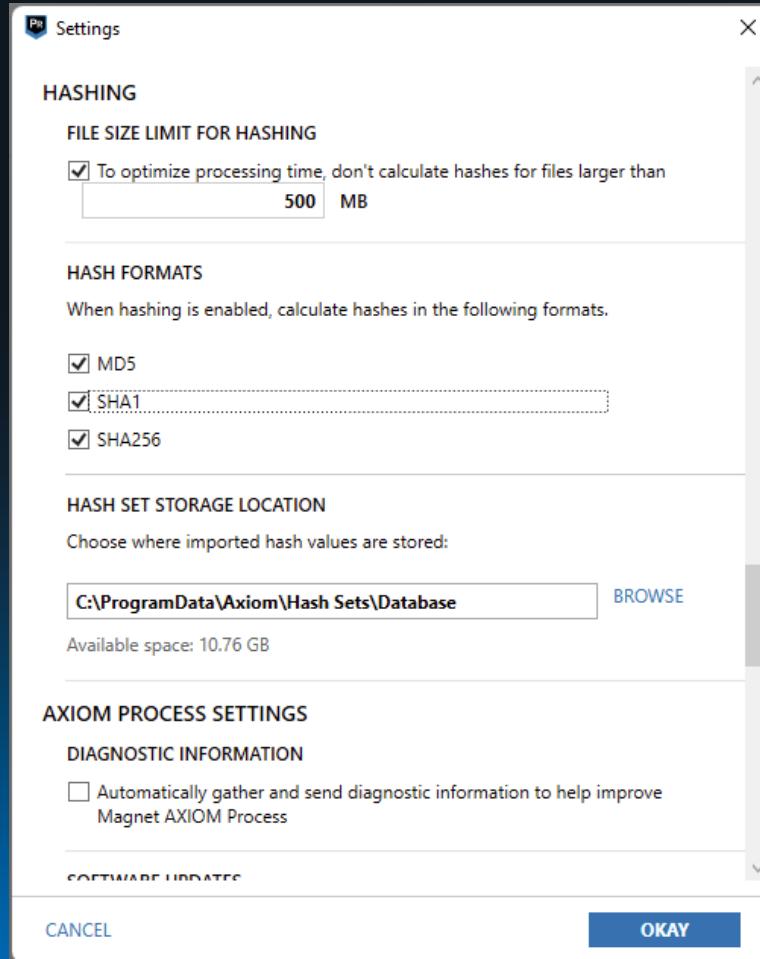
ADD HASH SET

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

Records Loaded: 40,937,452

UPDATE EXPORT

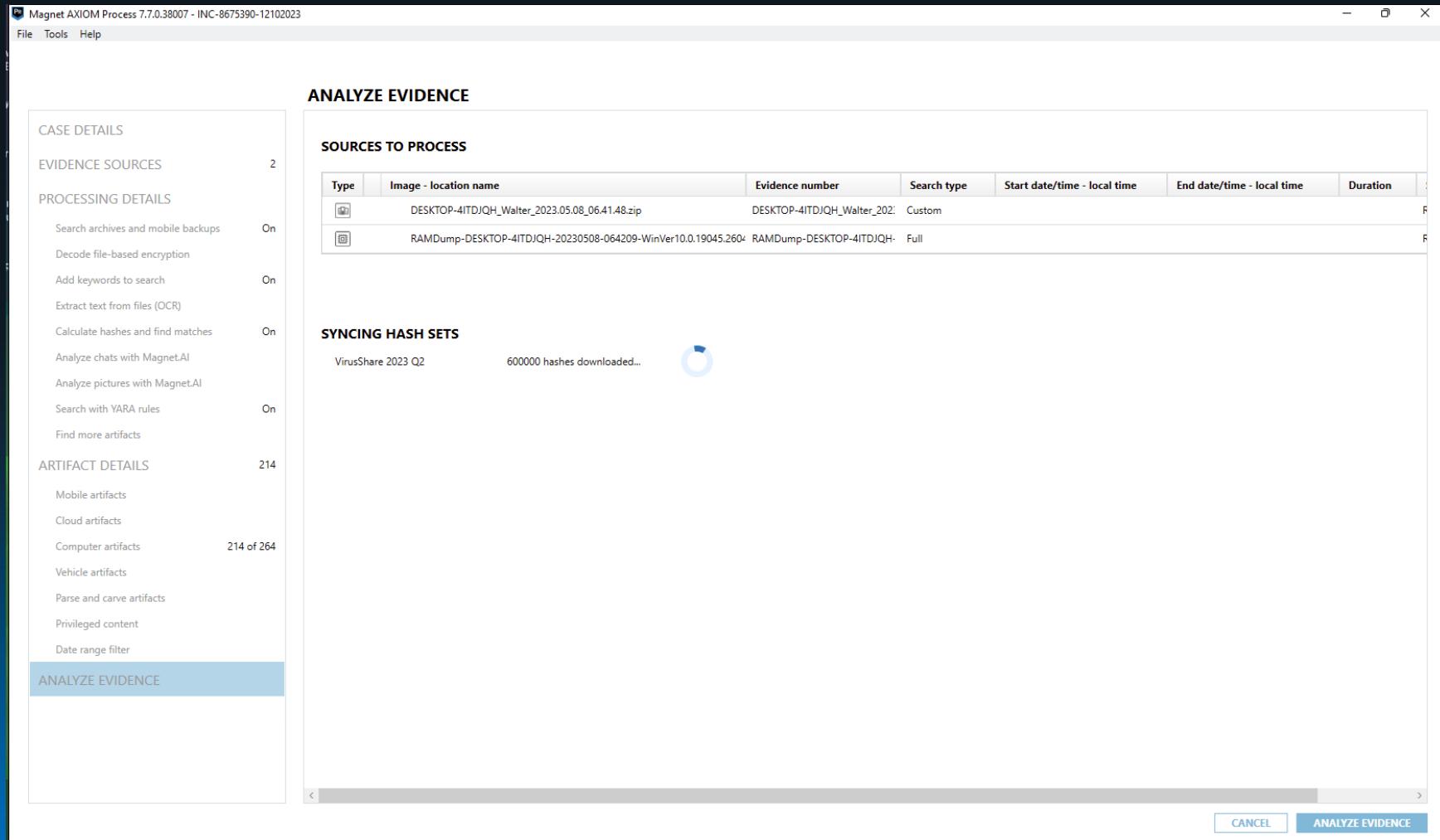
HSM - AXIOM Configuration



Auto Tagging Hash Matches

The screenshot shows the Magnet AXIOM Process 7.7.0.38007 software interface. The main window title is "CALCULATE HASHES AND FIND MATCHES". On the left, there's a sidebar with "CASE DETAILS" and "EVIDENCE SOURCES" sections. The "EVIDENCE SOURCES" section has a count of 2. Under "PROCESSING DETAILS", several options are listed: "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" (selected, On), "Analyze chats with Magnet.AI", "Analyze pictures with Magnet.AI", "Search with YARA rules", and "Find more artifacts". The "ARTIFACT DETAILS" section shows 214 artifacts, categorized by type: Mobile artifacts, Cloud artifacts, Computer artifacts (214 of 264), Vehicle artifacts, Parse and carve artifacts, Privileged content, and Date range filter. The "ANALYZE EVIDENCE" section is currently empty. The main content area includes sections for "CALCULATE HASH VALUES FOR ALL FILES", "SEARCH FOR MATCHES FROM HASH SETS", "INTEGRATE WITH HASH SETS MANAGER", and "TAG KNOWN FILES WITH MATCHING HASH VALUES". In the "TAG KNOWN FILES WITH MATCHING HASH VALUES" section, it says "Hash sets selected: 1" and lists one item: "VirusShare 2023 Q2" (Enabled, File source, Date loaded: 12/8/2023 9:38:08 PM, Number of records: 40937452, Tag: VirusShare, Source: Hash Sets Manager, Status: Will be downloaded at start of scan). At the bottom, there are buttons for "BACK", "GO TO ANALYZE CHATS WITH MAGNET.AI", and a yellow "IGNORE NON-RELEVANT FILES" button.

AXIOM HSM Hash Sync

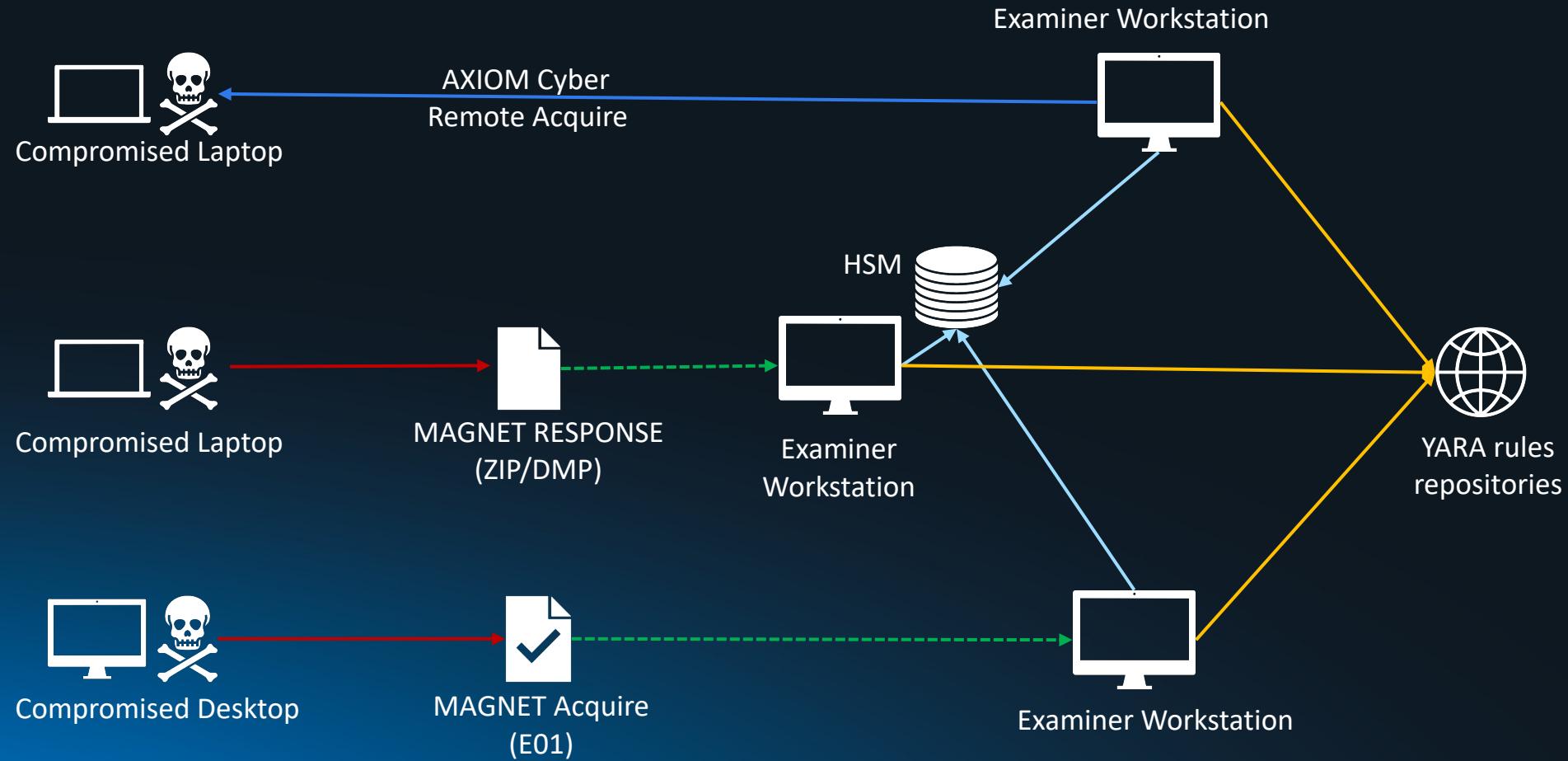


Auto Tagged Results

The screenshot shows the Magnet Forensics Evidence interface. The top navigation bar includes filters for Content types, Date and time, Tags and comments, Profiles, Partial results, Keyword lists, and Skin tone. A search bar with a 'Find...' placeholder and a magnifying glass icon is also present. The main area displays a list of evidence items under the heading 'EVIDENCE (152,045)'. The items are categorized by type: Artifact, Operating System, File System Information, Documents, and Text Documents. Each item has a preview icon, name, and file details like size and date. On the right, there's a sidebar for managing tags, with a 'RESET' button and a 'MANAGE TAGS' link. A list of available tags includes Untagged items, Bookmark, Evidence, Exceptions, Of interest, VirusShare, and Comments. At the bottom of the sidebar are 'CANCEL' and 'OKAY' buttons.

File Type	File Name	Size (Bytes)	Created Date/Time	Last Modified Date/Time
Text Documents	IP_Info.txt	3930	5/8/2023 1:52:41.000 PM	5/8/2023 1:52:41.000 PM
Text Documents	Firewall_Info.txt	2955	5/8/2023 1:52:42.000 PM	5/8/2023 1:52:42.000 PM

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

