MVS Magnet Virtual Summit 2025

Unlocking DFIR: Free Resources for Efficient Triage and Acquisition

Doug Metz,
Senior Security Forensics Specialist

MVS

Doug Metz, MCFE, GCFA, GCFE, GREM

- Joined Magnet in 2021
- Incident Response Manager
- HTCIA, Delaware Valley Chapter
- BakerStreetForensics.com

doug.metz@magnetforensics.com

Cyber Unpacked

Exploring enterprise DFIR

HTCIA

Delaware Valley - Philadelphia

BAKER STREET FORENSICS

D.F.I.R.

Triage in DFIR

- Incident Identification
- Impact Assessment
- Urgency Classification
- Containment and Mitigation
- Resource Allocation

The Triage Jump Kit

- Triage Collection
- Memory Acquisition
- Windows, Mac, Linux
- Scalable for ‘mass casualty incident’

Jump Kit Contents

Magnet Acquire

Magnet RAM Capture

DumpIt (Windows & Linux)

Magnet Response

Response PowerShell

Defender Response PowerShell

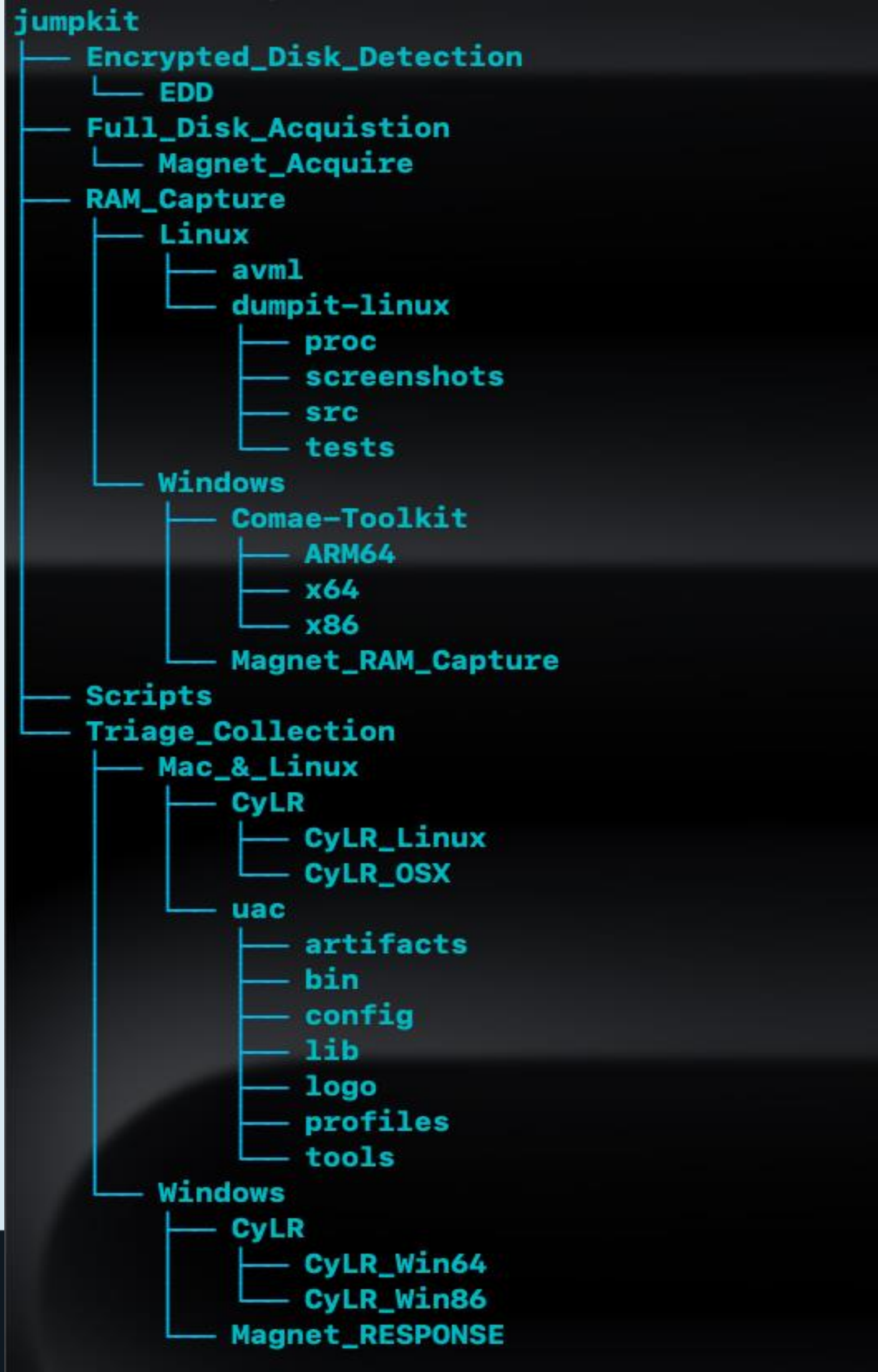
Encrypted Disk Detector

CyberPipe

CyLR

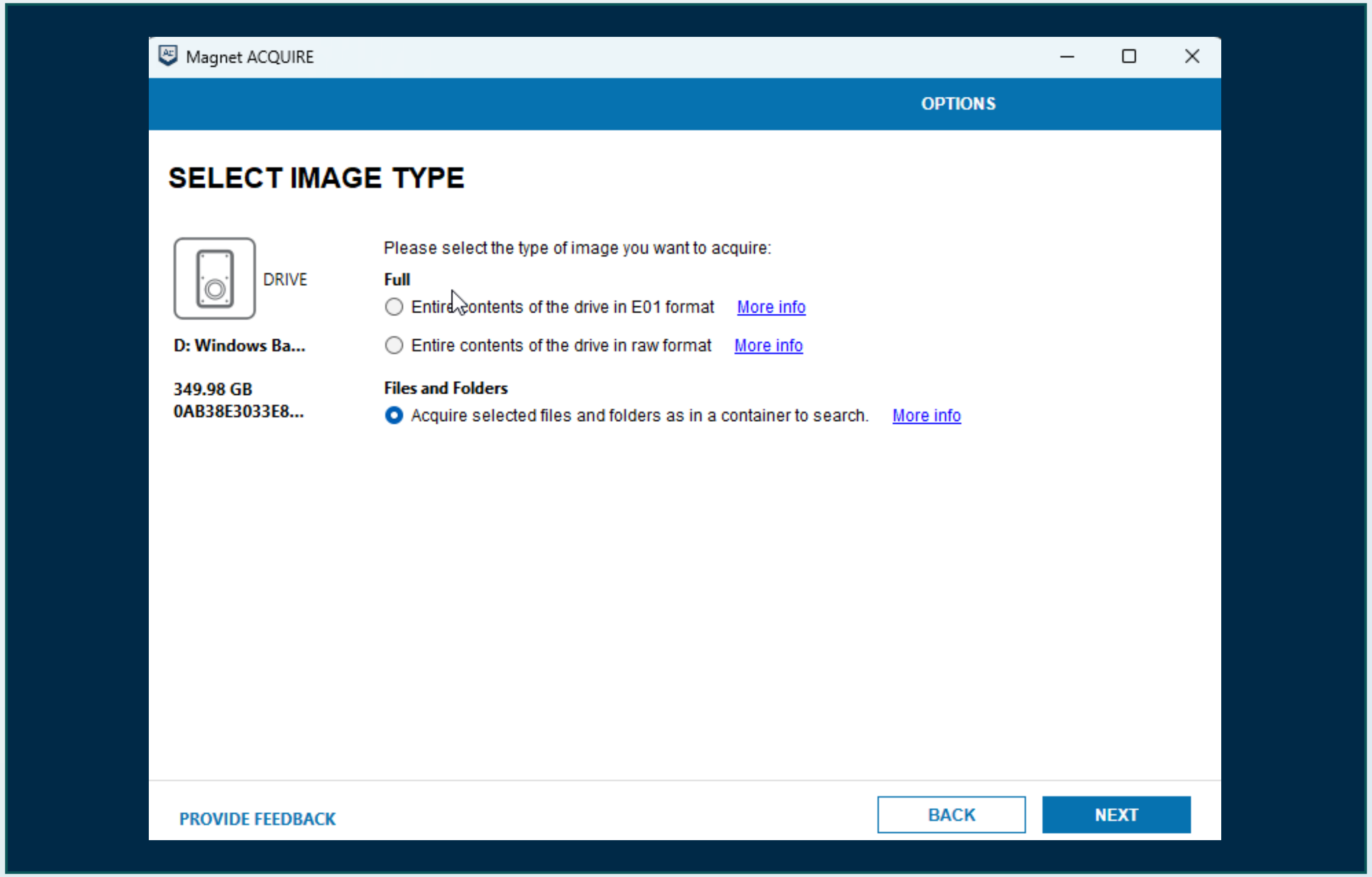
UAC

AVML



```
jumpkit
├── Encrypted_Disk_Detection
│   └── EDD
├── Full_Disk_Acquistion
│   └── Magnet_Acquire
├── RAM_Capture
│   ├── Linux
│   │   ├── avml
│   │   └── dumpit-linux
│   │       ├── proc
│   │       ├── screenshots
│   │       ├── src
│   │       └── tests
│   └── Windows
│       ├── Comae-Toolkit
│       │   ├── ARM64
│       │   ├── x64
│       │   └── x86
│       └── Magnet_RAM_Capture
├── Scripts
└── Triage_Collection
    ├── Mac_&_Linux
    │   ├── CyLR
    │   │   ├── CyLR_Linux
    │   │   └── CyLR_OSX
    │   └── uac
    │       ├── artifacts
    │       ├── bin
    │       ├── config
    │       ├── lib
    │       ├── logo
    │       ├── profiles
    │       └── tools
    └── Windows
        ├── CyLR
        │   ├── CyLR_Win64
        │   └── CyLR_Win86
        └── Magnet_RESPONSE
```

Magnet Acquire



SELECT IMAGE TYPE

DRIVE

D: Windows Ba...

349.98 GB
0AB38E3033E8...

Please select the type of image you want to acquire:

Full

○ Entire contents of the drive in E01 format More info

○ Entire contents of the drive in raw format More info

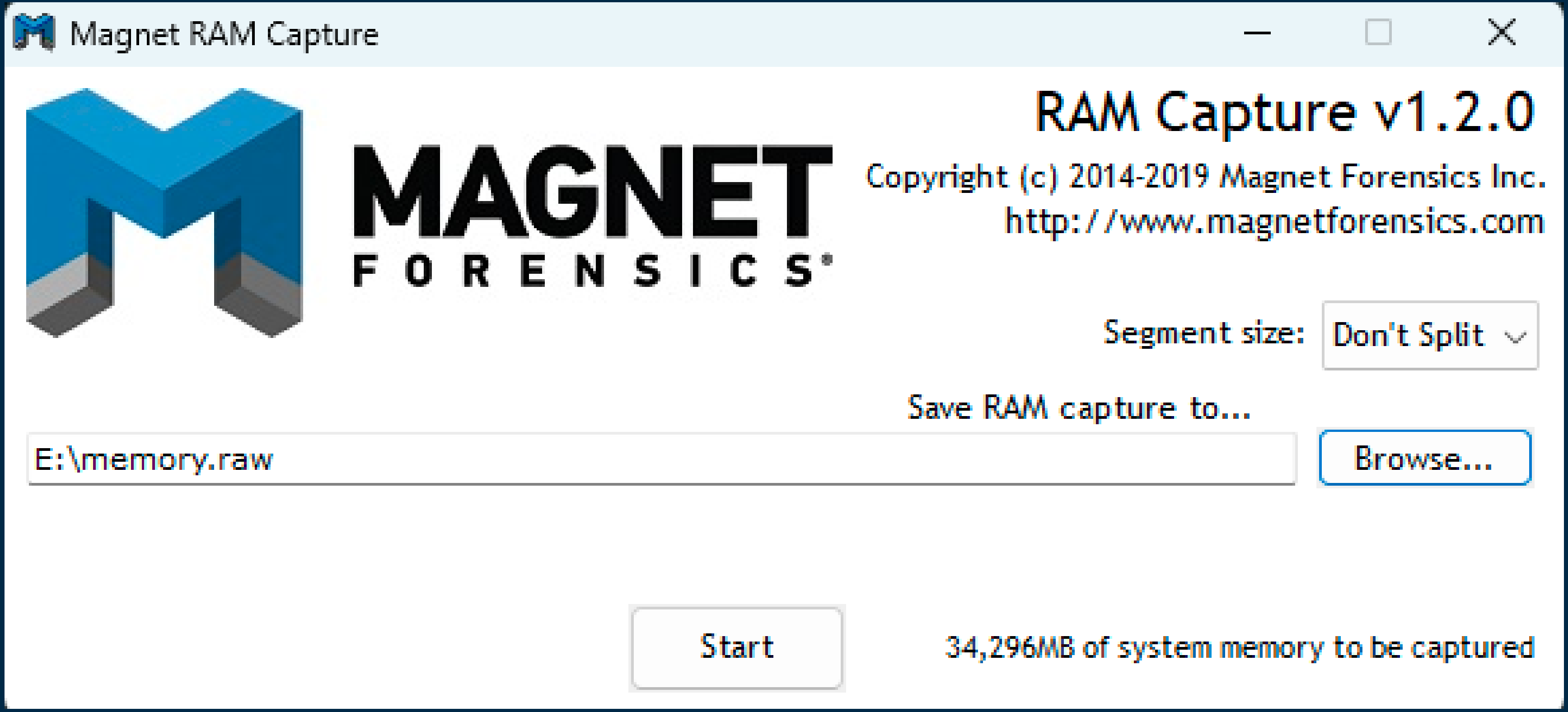
Files and Folders

● Acquire selected files and folders as in a container to search. More info

- Dead box acquisition
- Hard drives and removable media
- Full Disk Image
- Patient 0
- iOS & Android acquisition

Magnet RAM Capture

- Windows Memory Acquisition
- GUI
- RAW Format
- Legacy to Modern Windows systems
- x86 & x64



RAM Capture v1.2.0

Copyright (c) 2014-2019 Magnet Forensics Inc.
http://www.magnetforensics.com

Segment size: Don't Split

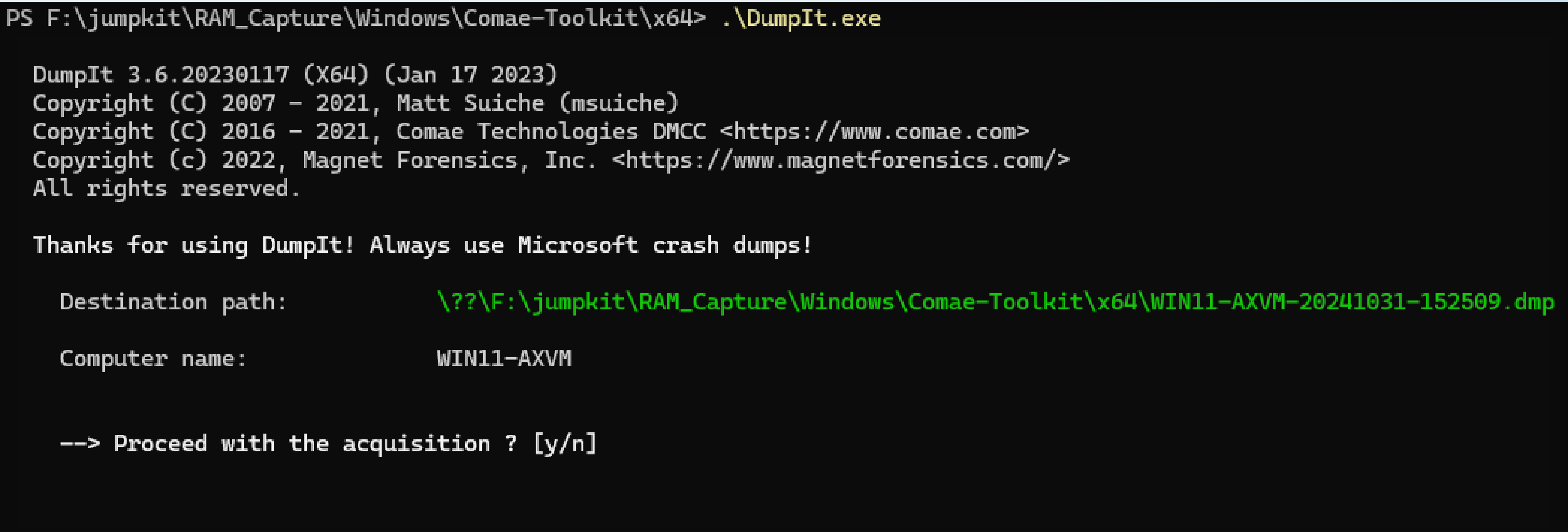
Save RAM capture to...

E:\memory.raw

34,296MB of system memory to be captured

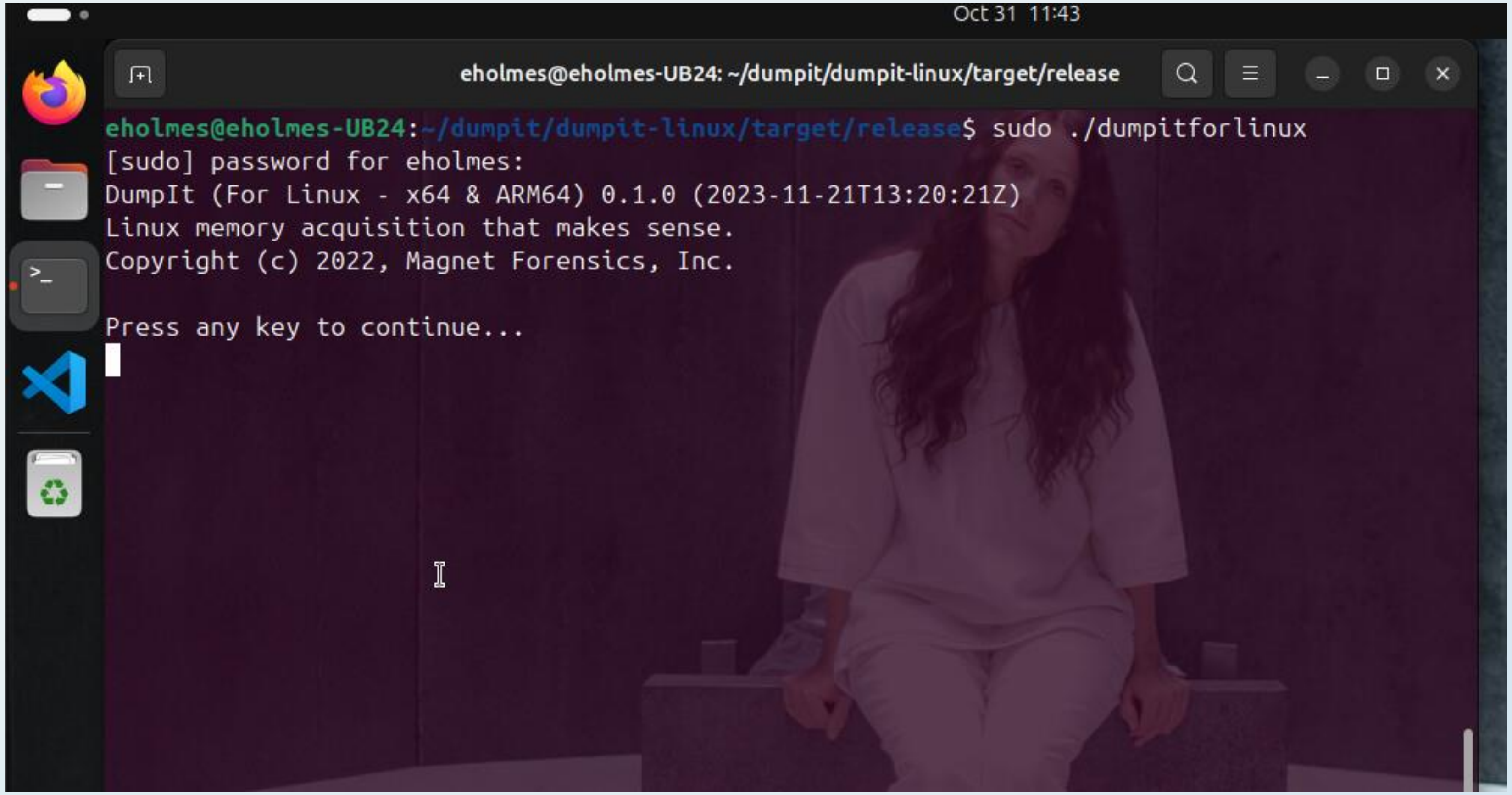
DumpIt for Windows

- Windows Memory Acquisition
- CLI
- DMP (default) or RAW Format
- Legacy to Modern Windows systems
- x86 & x64 and ARM



```
PS F:\jumpkit\RAM_Capture\Windows\Comae-Toolkit\x64> .\DumpIt.exe

  DumpIt 3.6.20230117 (X64) (Jan 17 2023)
  Copyright (C) 2007 - 2021, Matt Suiche (msuiche)
  Copyright (C) 2016 - 2021, Comae Technologies DMCC <https://www.comae.com>
  Copyright (c) 2022, Magnet Forensics, Inc. <https://www.magnetforensics.com/>
  All rights reserved.

  Thanks for using DumpIt! Always use Microsoft crash dumps!

    Destination path:           \??\F:\jumpkit\RAM_Capture\Windows\Comae-Toolkit\x64\WIN11-AXVM-20241031-152509.dmp

    Computer name:              WIN11-AXVM


    --> Proceed with the acquisition ? [y/n]
```

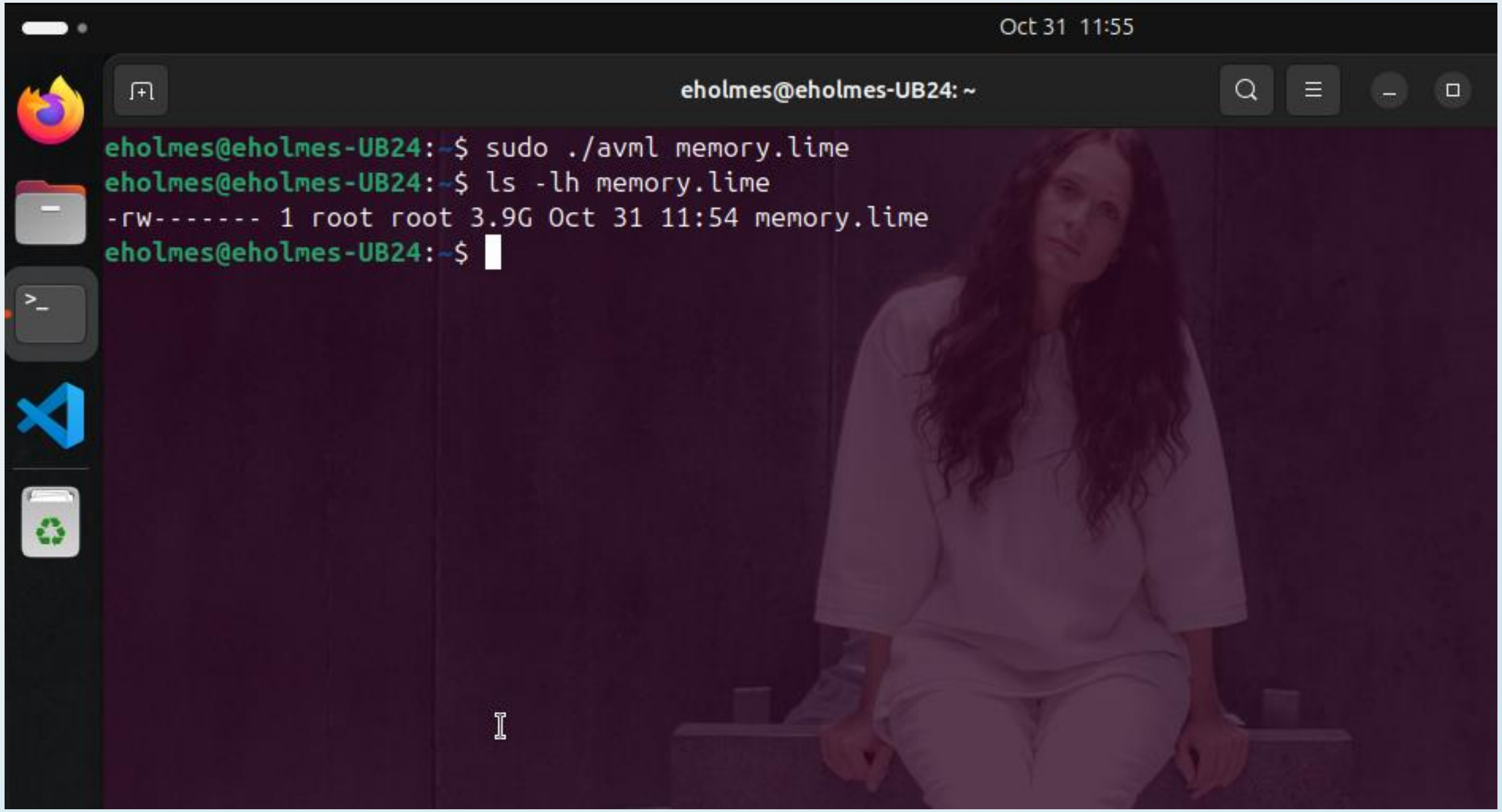
DumpIt for Linux



```
eholmes@eholmes-UB24:~/dumpit/dumpit-linux/target/release$ sudo ./dumpitforlinux
[sudo] password for eholmes:
DumpIt (For Linux - x64 & ARM64) 0.1.0 (2023-11-21T13:20:21Z)
Linux memory acquisition that makes sense.
Copyright (c) 2022, Magnet Forensics, Inc.

Press any key to continue...
```

- Open-Source
- Magnet GitHub
- CLI
- Built in Rust
- Compile for specific kernel versions
- Ubuntu & Redhat
- Core dump

AVML (Acquire Volatile Memory for Linux)

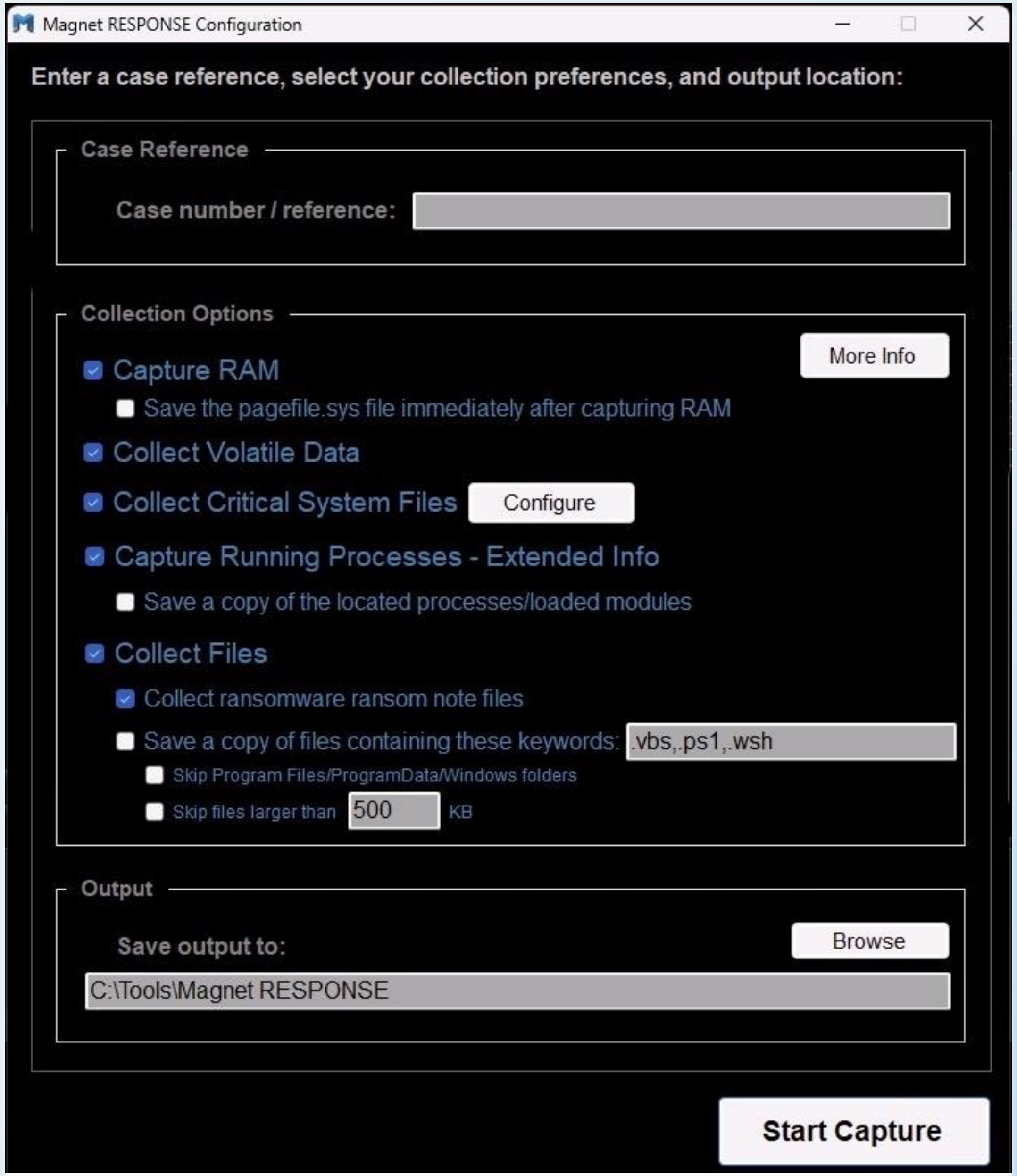


```
eholmes@eholmes-UB24:~$ sudo ./avml memory.lime
eholmes@eholmes-UB24:~$ ls -lh memory.lime
-rw------- 1 root root 3.9G Oct 31 11:54 memory.lime
eholmes@eholmes-UB24:~$ 
```

- Open-Source
- Developed by Microsoft
- CLI
- Built in Rust
- Run ready
- Ubuntu, Redhat, Debian, Oracle…
- LIME output

Magnet RESPONSE

- Free triage collection tool
- Intuitive interface
- Collects RAM, Volatile info and Operating System artifacts



Magnet RESPONSE Configuration

Enter a case reference, select your collection preferences, and output location:

Case Reference

Case number / reference:

Collection Options

☑ Capture RAM

- □ Save the pagefile.sys file immediately after capturing RAM

☑ Collect Volatile Data

☑ Collect Critical System Files

☑ Capture Running Processes - Extended Info

- □ Save a copy of the located processes/loaded modules

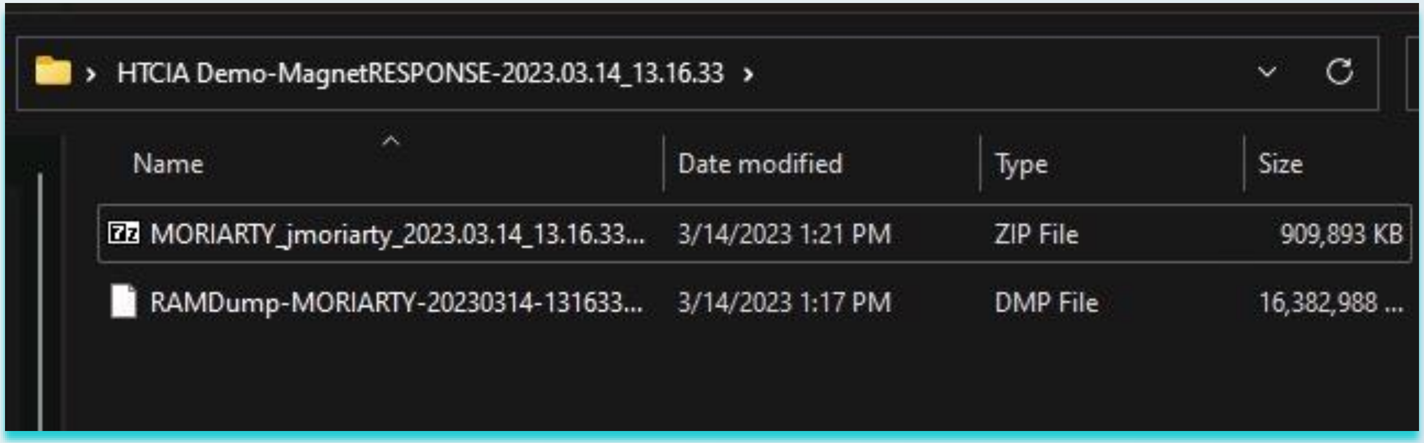
☑ Collect Files

- ☑ Collect ransomware ransom note files
- □ Save a copy of files containing these keywords: .vbs,.ps1,.wsh
  - □ Skip Program Files/ProgramData/Windows folders
  - □ Skip files larger than 500 KB

Output

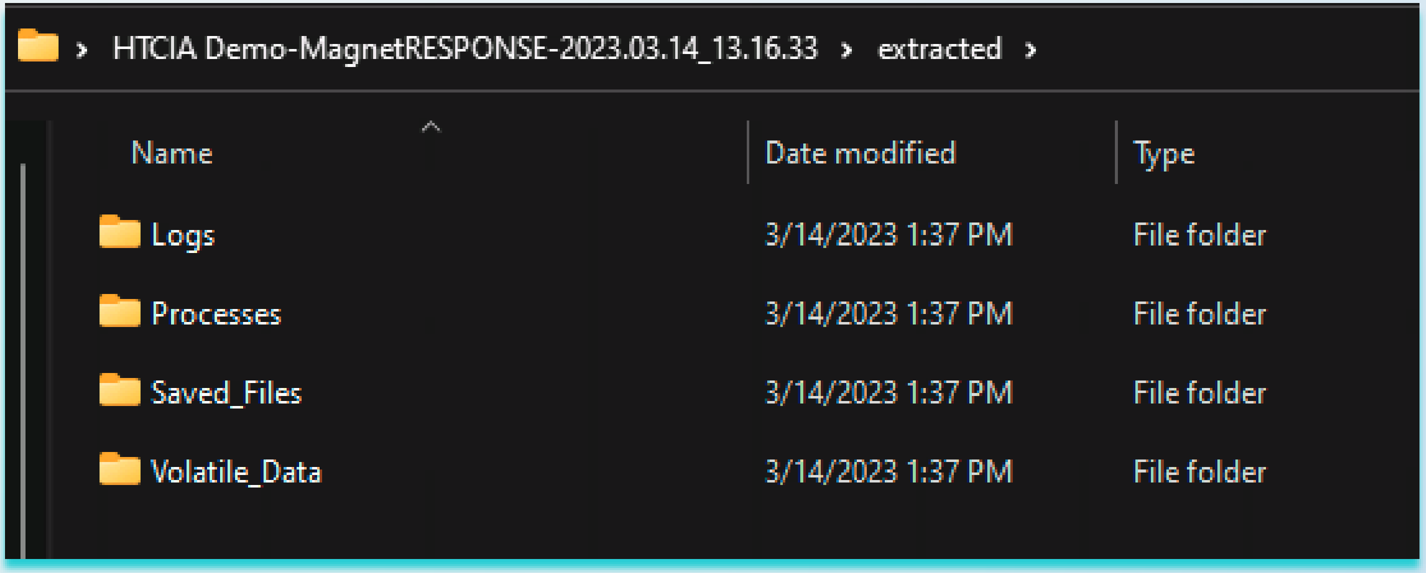
Save output to: C:\Tools\Magnet RESPONSE

Magnet RESPONSE Output



› HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 ›

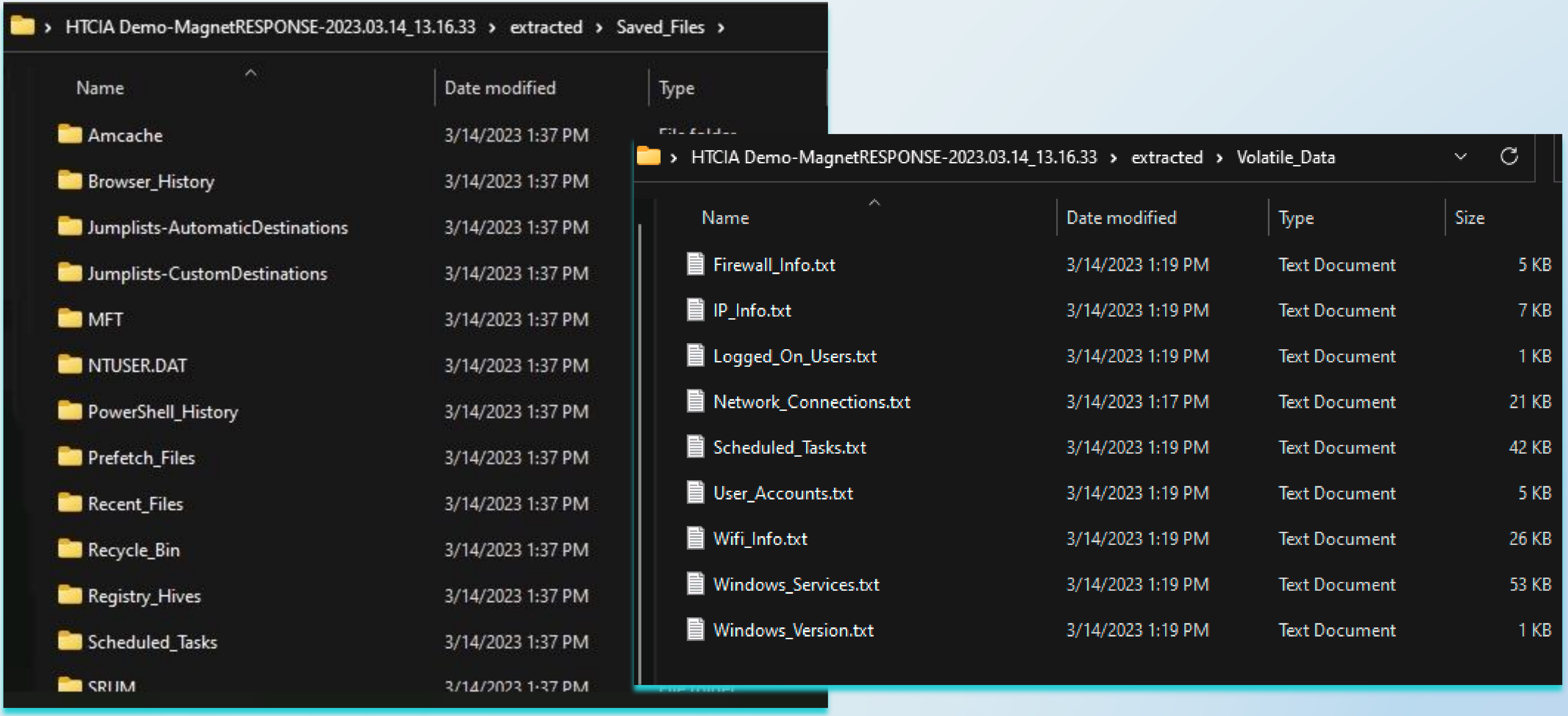
Name	Date modified	Type	Size
MORIARTY_jmoriarty_2023.03.14_13.16.33...	3/14/2023 1:21 PM	ZIP File	909,893 KB
RAMDump-MORIARTY-20230314-131633...	3/14/2023 1:17 PM	DMP File	16,382,988 ...



› 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



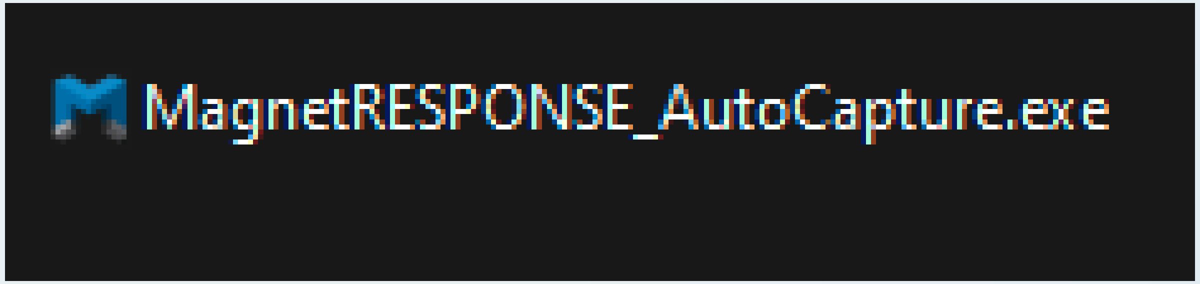
› HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 › extracted › Saved_Files ›

Name	Date modified	Type
Amcache	3/14/2023 1:37 PM	File folder
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	
SRUM	3/14/2023 1:37 PM	

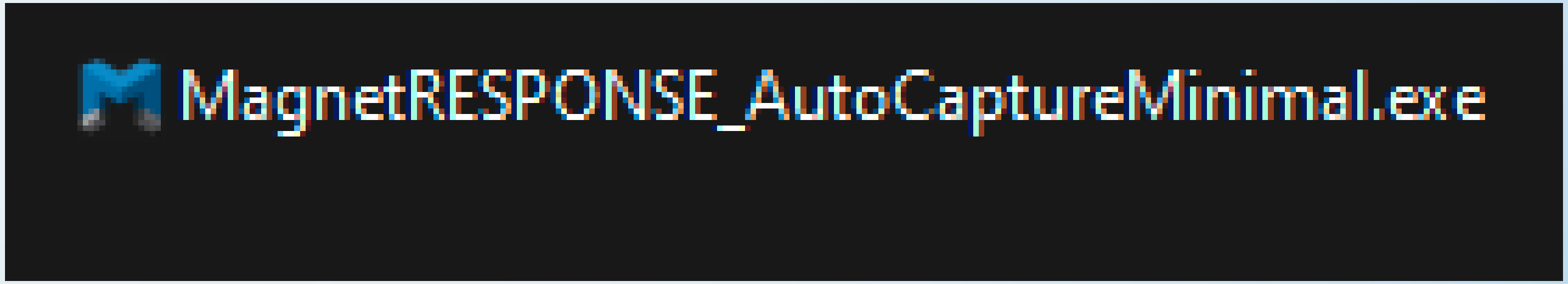
› HTCIA Demo-MagnetRESPONSE-2023.03.14_13.16.33 › extracted › Volatile_Data

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

Auto Collect Options

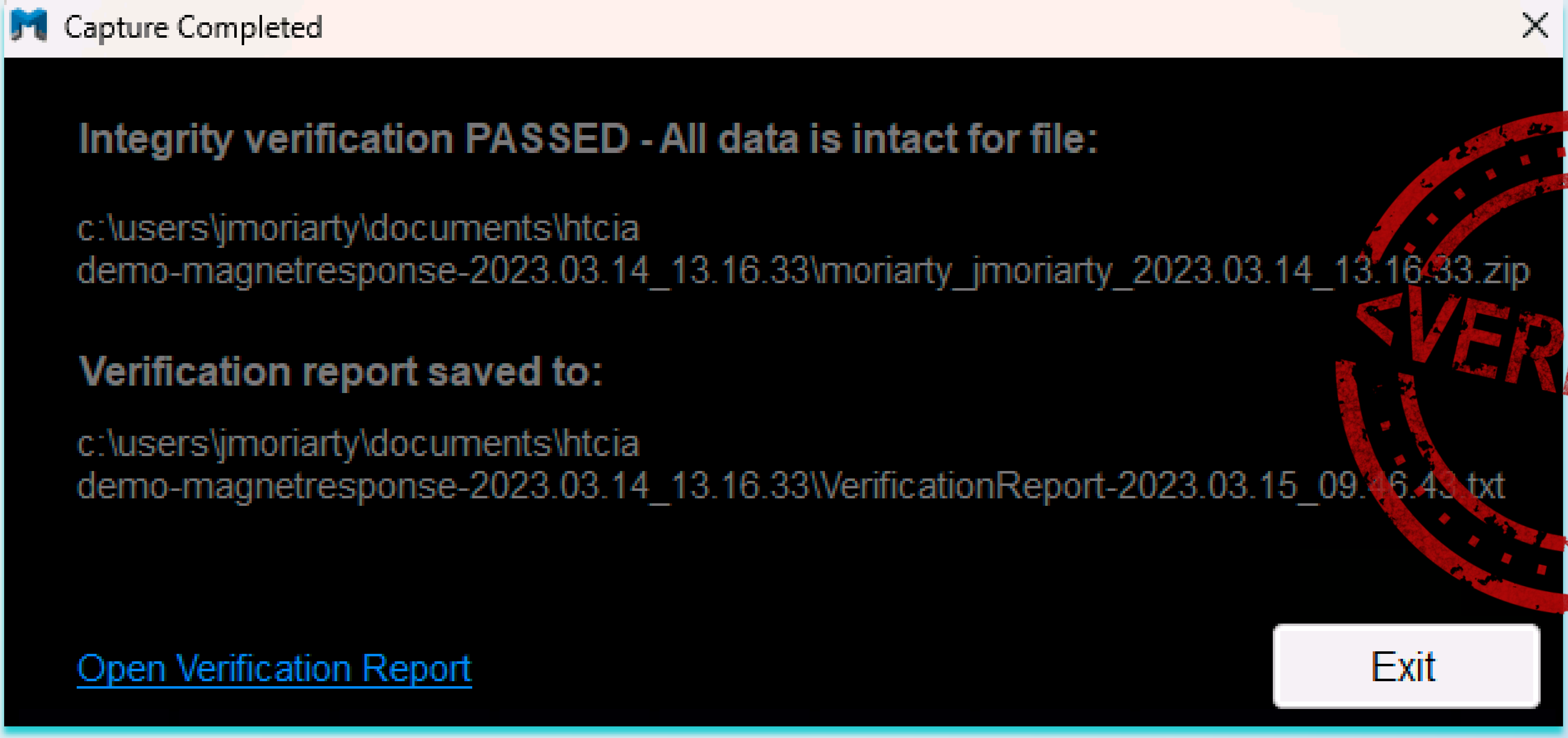


MagnetRESPONSE_AutoCapture.exe



MagnetRESPONSE_AutoCaptureMinimal.exe

Verifying a Capture Package



Capture Completed

Integrity verification PASSED - All data is intact for file:

c:\users\jmoriarty\documents\htcia demo-magnetresponse-2023.03.14_13.16.33\moriarty_jmoriarty_2023.03.14_13.16.33.zip

Verification report saved to:

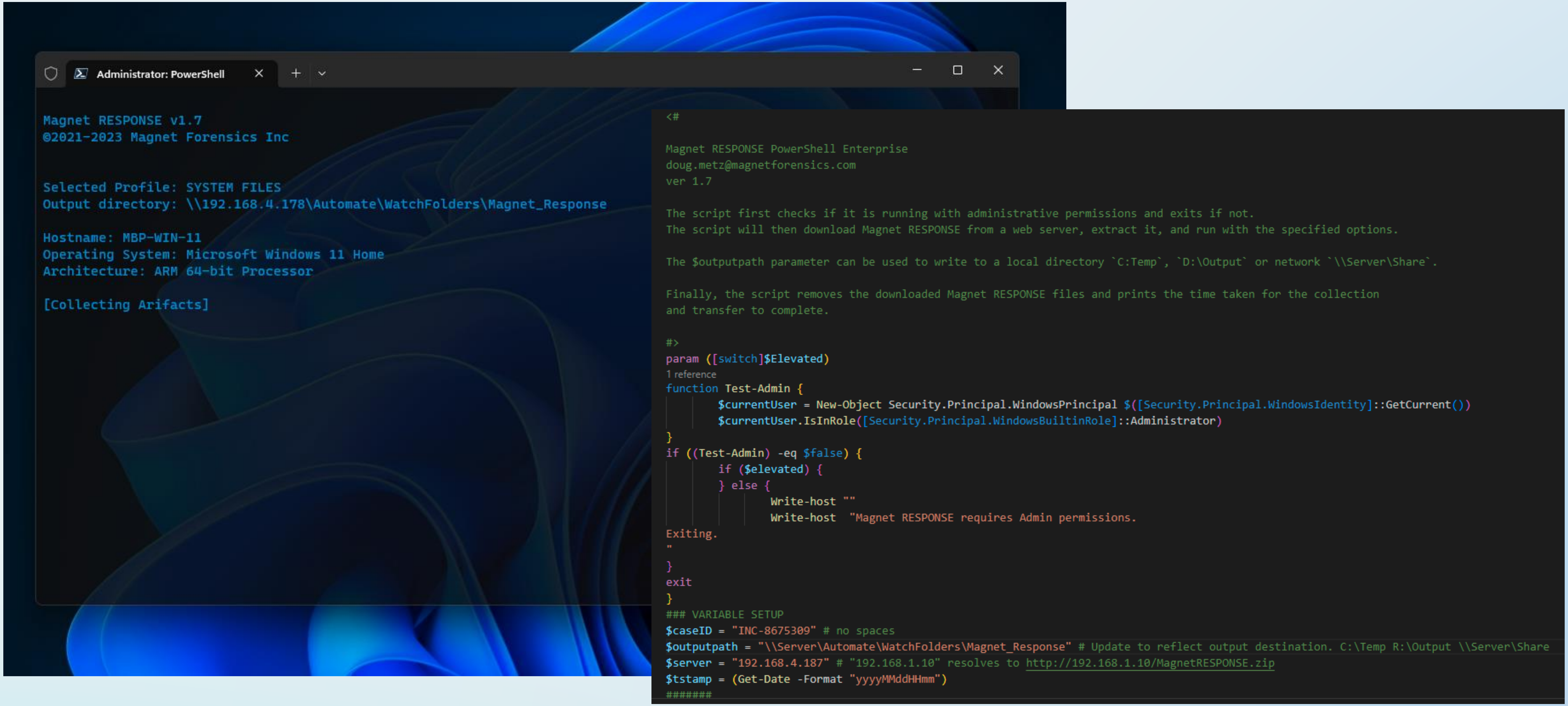
c:\users\jmoriarty\documents\htcia demo-magnetresponse-2023.03.14_13.16.33\VerificationReport-2023.03.15_09.46.43.txt

<VERIFIED>

Magnet RESPONSE CLI

- /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
- /silent - No GUI output to screen

Magnet RESPONSE PowerShell



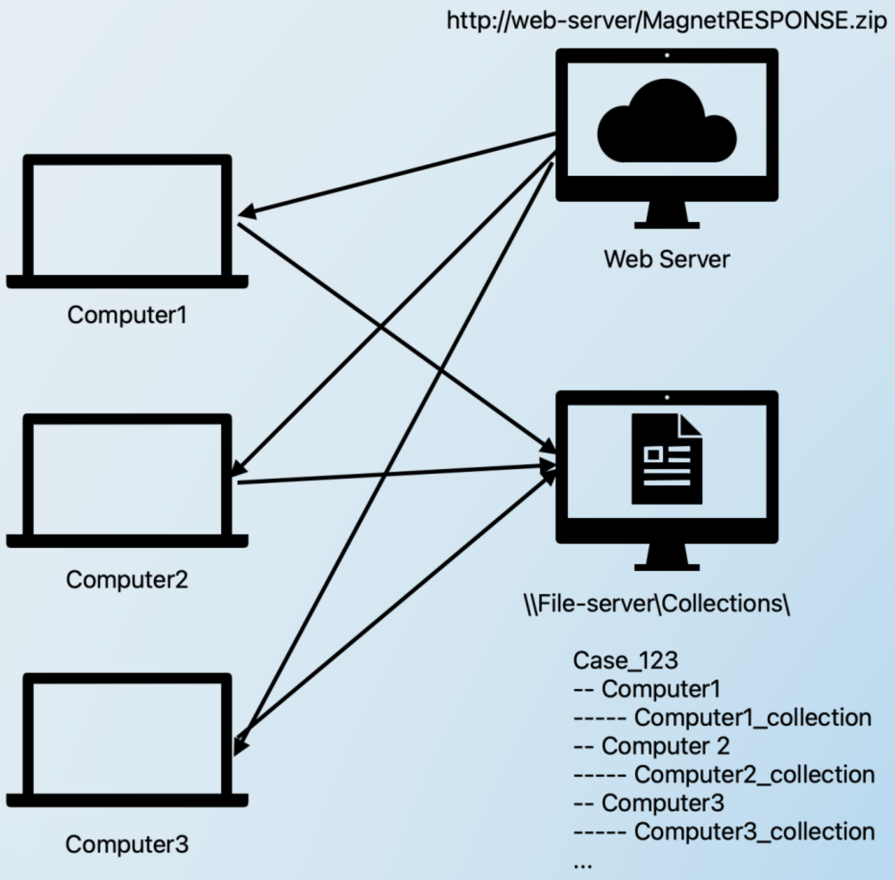
```
Magnet RESPONSE v1.7
©2021-2023 Magnet Forensics Inc


Selected Profile: SYSTEM FILES
Output directory: \\192.168.4.178\Automate\WatchFolders\Magnet_Response

Hostname: MBP-WIN-11
Operating System: Microsoft Windows 11 Home
Architecture: ARM 64-bit Processor

[Collecting Arifacts]
```

```
<#

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")
#######
```

Magnet RESPONSE PowerShell

- Web server hosting MagnetRESPONSE.zip

- File server with folder share for collections


http://web-server/MagnetRESPONSE.zip
Web Server
Computer1
Computer2
Computer3
\\File-server\Collections\
Case_123
-- Computer1
----- Computer1_collection
-- Computer 2
----- Computer2_collection
-- Computer3
----- Computer3_collection
...

Case Variables

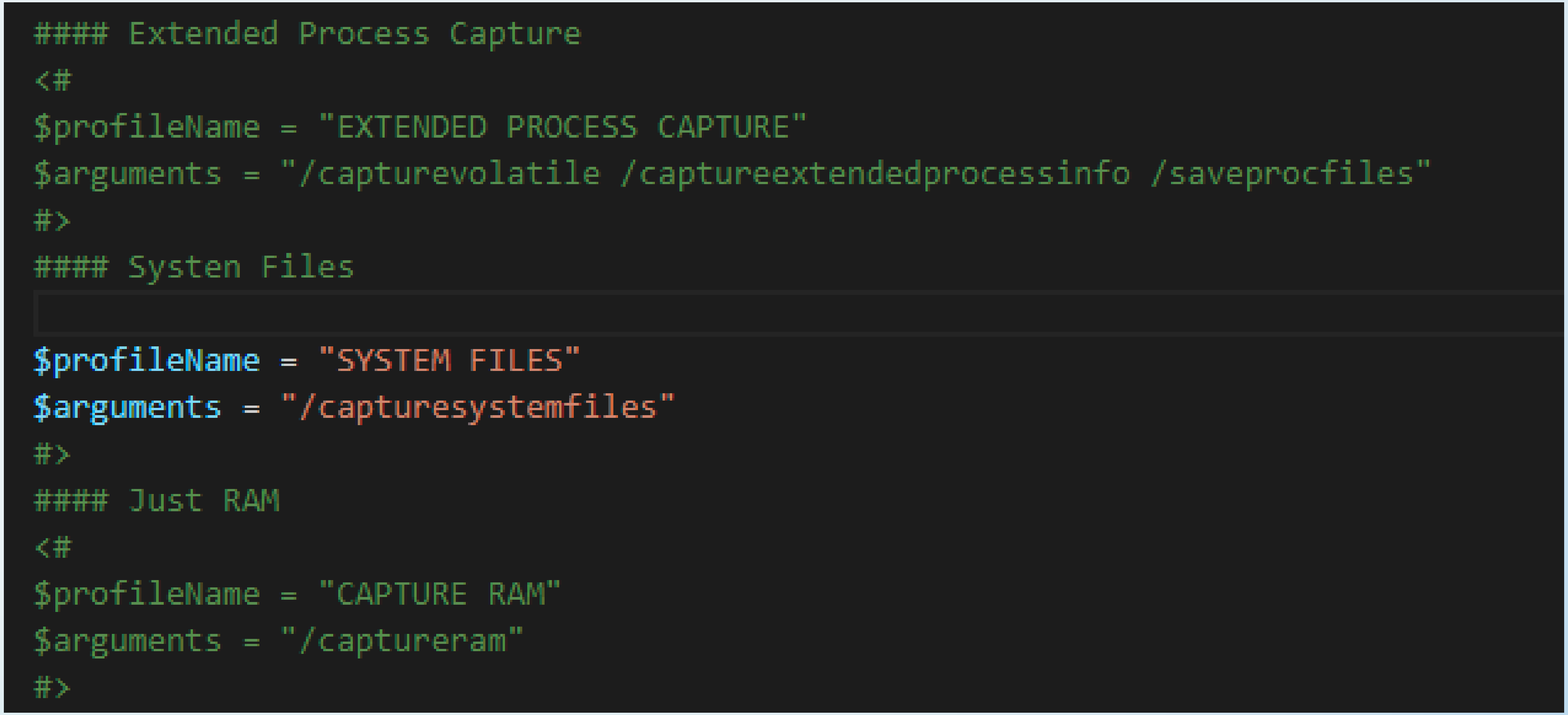
```
### VARIABLE SETUP
$caseID = "demo-161" # no spaces
$outputpath = ”\\server\share" # Update to reflect output destination.
$server = "192.168.4.187" # "192.168.4.187" resolves to http://192.168.4.187/MagnetRESPONSE.zip
```

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

$outputpath – Where the collection output is sent

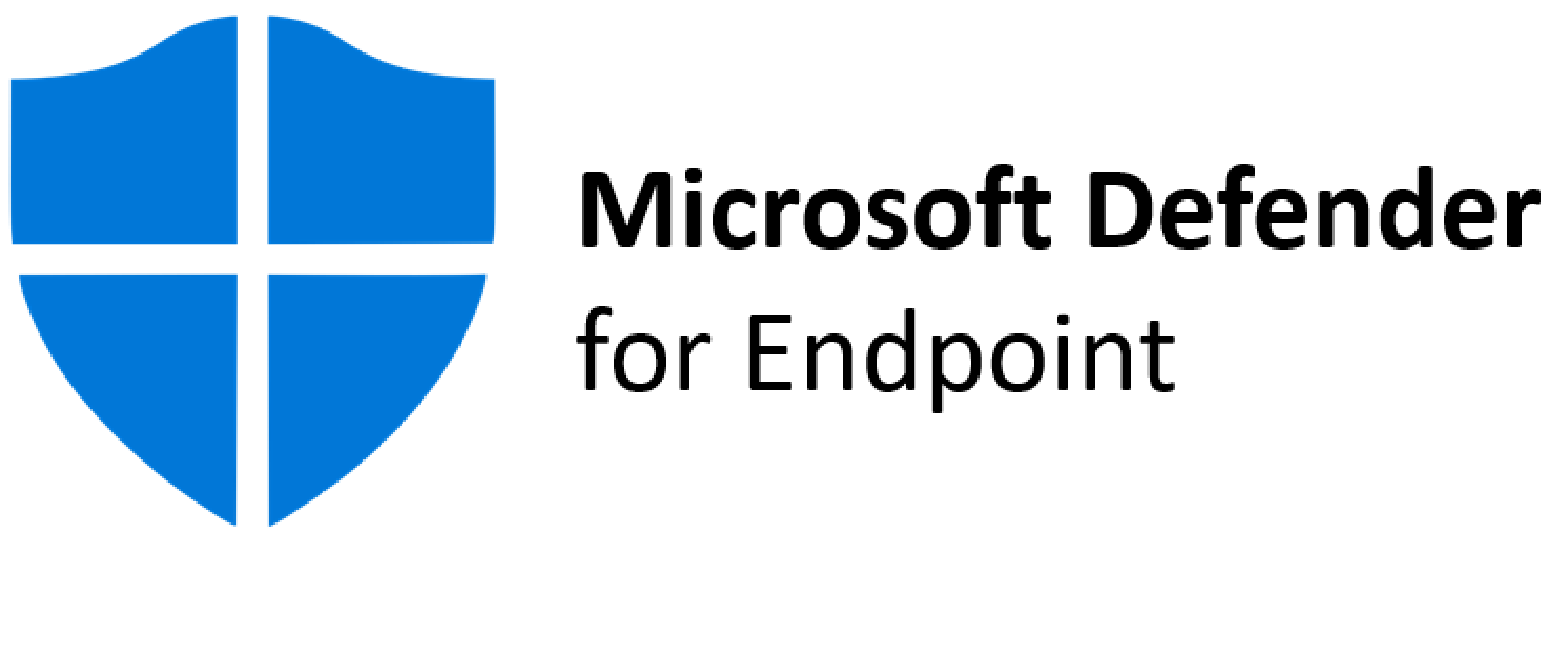
$server – Address for web server hosting MagnetRESPONSE.zip

Collection Profiles



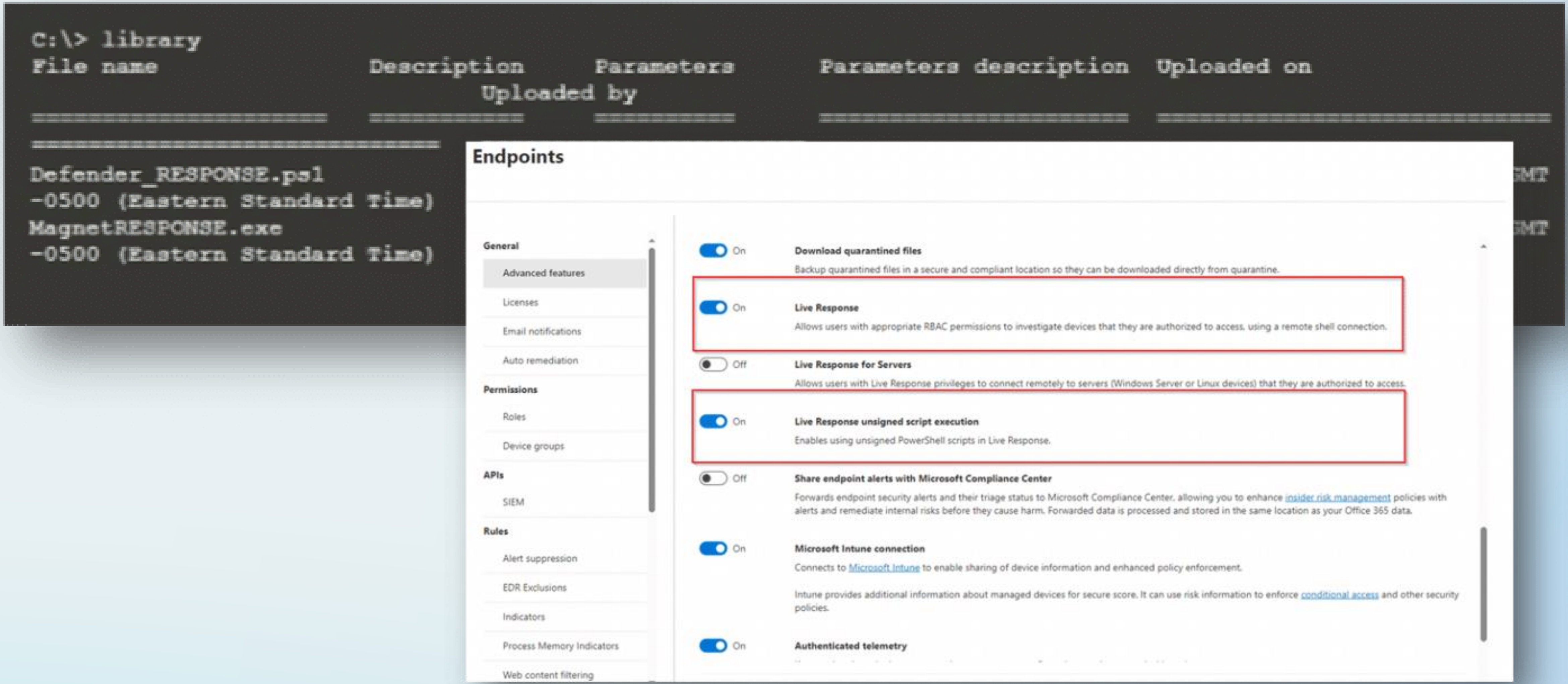
```
#### Extended Process Capture
<#
$profileName = "EXTENDED PROCESS CAPTURE"
$arguments = "/capturevolatile /captureextendedprocessinfo /saveprocfiles"
#>
#### Systen Files

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

Magnet RESPONSE and



Microsoft Defender
for Endpoint

Defender_RESPONSE.ps1



```
C:\> library
File name                 Description    Parameters      Parameters description   Uploaded on
                                  Uploaded by

=======================   ============   ===========     ========================   ============================
================================

Defender_RESPONSE.ps1                                                                                        GMT
-0500 (Eastern Standard Time)
MagnetRESPONSE.exe                                                                                           GMT
-0500 (Eastern Standard Time)
```

Endpoints

On **Download quarantined files**
Backup quarantined files in a secure and compliant location so they can be downloaded directly from quarantine.

On **Live Response**
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.

Off **Live Response for Servers**
Allows users with Live Response privileges to connect remotely to servers (Windows Server or Linux devices) that they are authorized to access.

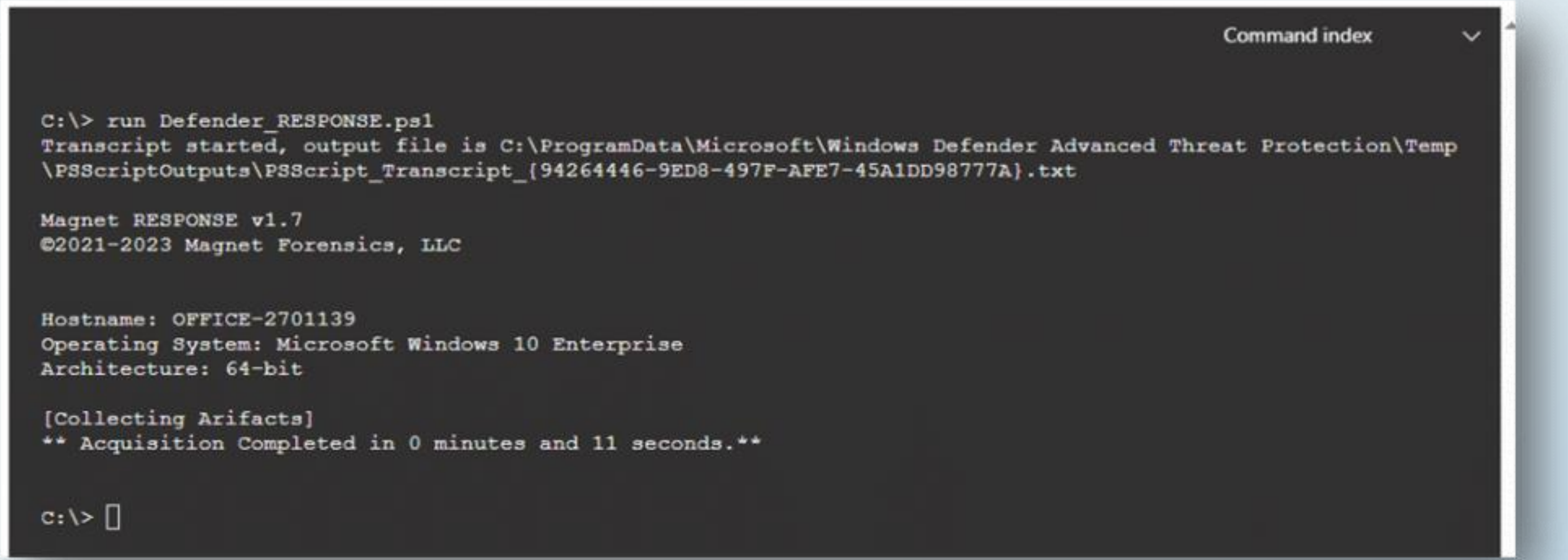
On **Live Response unsigned script execution**
Enables using unsigned PowerShell scripts in Live Response.

Off **Share endpoint alerts with Microsoft Compliance Center**
Forwards endpoint security alerts and their triage status to Microsoft Compliance Center, allowing you to enhance insider risk management policies with alerts and remediate internal risks before they cause harm. Forwarded data is processed and stored in the same location as your Office 365 data.

On **Microsoft Intune connection**
Connects to Microsoft Intune to enable sharing of device information and enhanced policy enforcement.

Intune provides additional information about managed devices for secure score. It can use risk information to enforce conditional access and other security policies.

On **Authenticated telemetry**



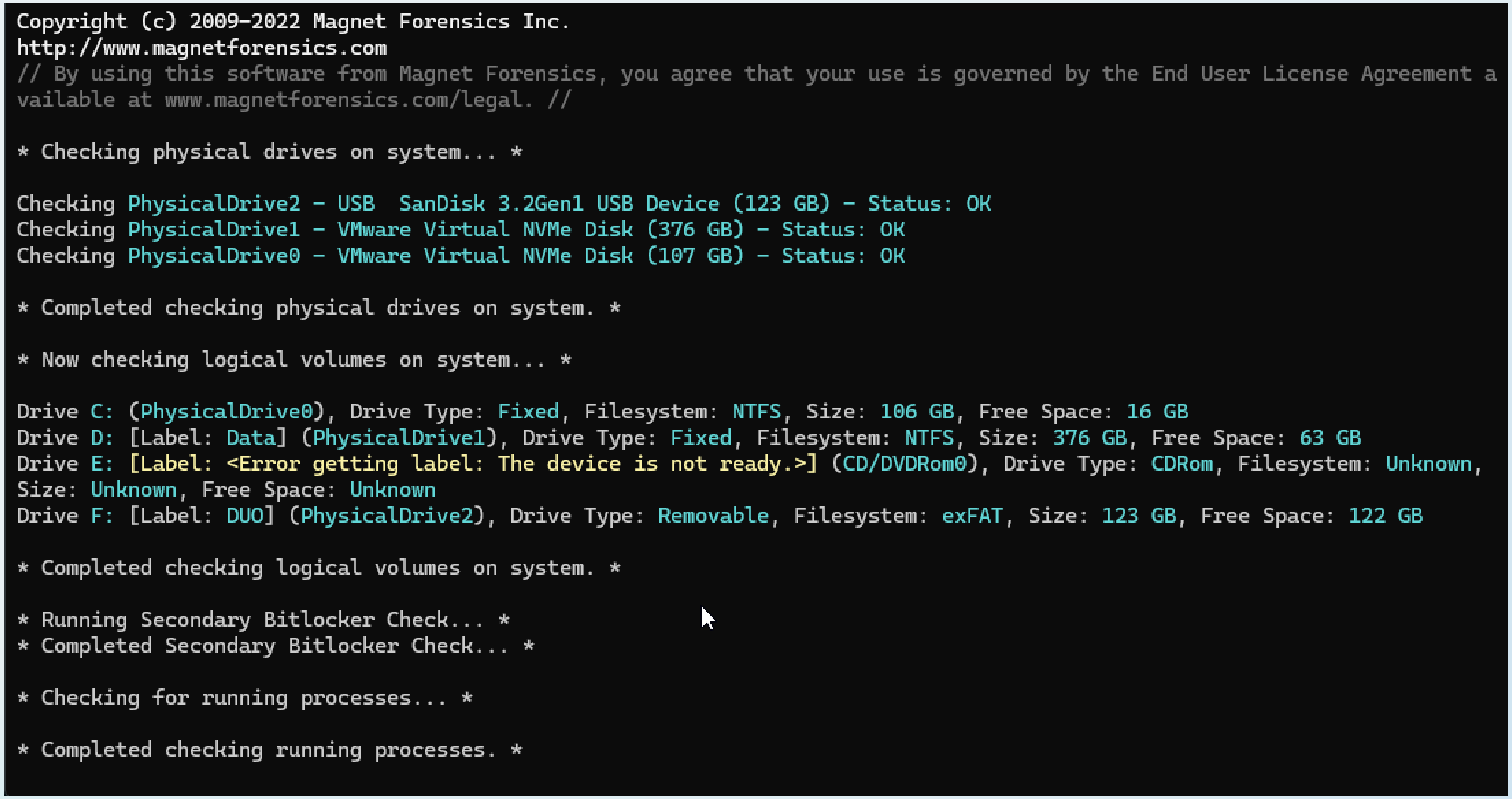
```
C:\> run Defender_RESPONSE.ps1
Transcript started, output file is C:\ProgramData\Microsoft\Windows Defender Advanced Threat Protection\Temp
\PSScriptOutputs\PSScript_Transcript_{94264446-9ED8-497F-AFE7-45A1DD98777A}.txt

Magnet RESPONSE v1.7
©2021-2023 Magnet Forensics, LLC


Hostname: OFFICE-2701139
Operating System: Microsoft Windows 10 Enterprise
Architecture: 64-bit

[Collecting Arifacts]
** Acquisition Completed in 0 minutes and 11 seconds.**


C:\> 
```

Retrieving the Data from the Defender console:

Once the script finishes, the zipped output will be saved to “C:\Temp\RESPONSE” on the remote machine.

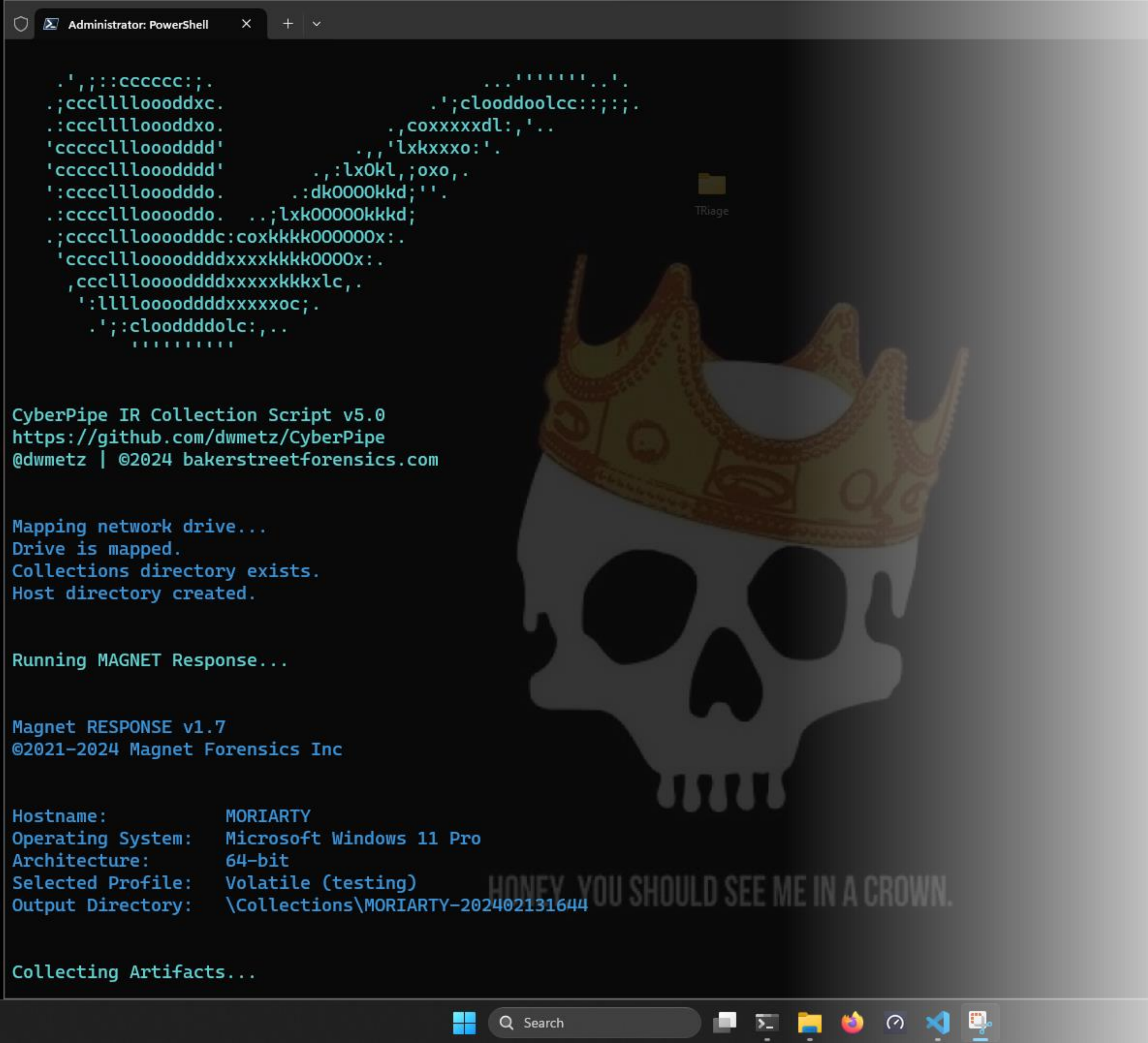
- Navigate to the output folder using the command — cd c:\Temp\RESPONSE
- List files using the “dir” command
- Copy the zip filename
- Download <filename.zip>

Encrypted Disk Detector



```
Copyright (c) 2009-2022 Magnet Forensics Inc.
http://www.magnetforensics.com
// By using this software from Magnet Forensics, you agree that your use is governed by the End User License Agreement a
vailable at www.magnetforensics.com/legal. //

* Checking physical drives on system... *

Checking PhysicalDrive2 - USB  SanDisk 3.2Gen1 USB Device (123 GB) - Status: OK
Checking PhysicalDrive1 - VMware Virtual NVMe Disk (376 GB) - Status: OK
Checking PhysicalDrive0 - VMware Virtual NVMe Disk (107 GB) - Status: OK

* Completed checking physical drives on system. *

* Now checking logical volumes on system... *

Drive C: (PhysicalDrive0), Drive Type: Fixed, Filesystem: NTFS, Size: 106 GB, Free Space: 16 GB
Drive D: [Label: Data] (PhysicalDrive1), Drive Type: Fixed, Filesystem: NTFS, Size: 376 GB, Free Space: 63 GB
Drive E: [Label: <Error getting label: The device is not ready.>] (CD/DVDRom0), Drive Type: CDRom, Filesystem: Unknown,
Size: Unknown, Free Space: Unknown
Drive F: [Label: DUO] (PhysicalDrive2), Drive Type: Removable, Filesystem: exFAT, Size: 123 GB, Free Space: 122 GB

* Completed checking logical volumes on system. *

* Running Secondary Bitlocker Check... *
* Completed Secondary Bitlocker Check... *

* Checking for running processes... *

* Completed checking running processes. *
```

- CLI
- checks the physical drives for encrypted volumes
- Detects TrueCrypt, PGP, Bitlocker, and other full disk encryption products


Administrator: PowerShell
TRiage
HONEY, YOU SHOULD SEE ME IN A CROWN.
Search

```
    .',;::cccccc:;.                         ...'''''''..'.
   .;cccllllooddxc.                    .';clooddoolcc::;:;.
   .:cccllllooddxo.                .,coxxxxxdl:,'..
   'ccccclllooodddd'            .,,'lxkxxxo:'.
   'ccccclllooodddd'        .,:lxOkl,;oxo,.
   ':ccccllloooddo.       .:dkOOOOkkd;''.
   .:cccclllooooddo.  ..;lxkOOOOOkkd;
   .;cccclllooooddc:coxkkkOOOOOOx:.
    'cccclllooooddddxxxkkkkOOOOx:.
     ,cccllloooodddxxxxxkkkxlc,.
      ':llllooooddddxxxxxoc;.
       .';:cloodddolc:,..
           ''''''''''


CyberPipe IR Collection Script v5.0
https://github.com/dwmetz/CyberPipe
@dwmetz | ©2024 bakerstreetforensics.com


Mapping network drive...
Drive is mapped.
Collections directory exists.
Host directory created.


Running MAGNET Response...


Magnet RESPONSE v1.7
©2021-2024 Magnet Forensics Inc


Hostname:           MORIARTY
Operating System:   Microsoft Windows 11 Pro
Architecture:       64-bit
Selected Profile:   Volatile (testing)
Output Directory:   \Collections\MORIARTY-20240213164


Collecting Artifacts...
```

CyberPipe

CyberPipe (v5)

Functions:

- 🐑 Capture a memory image with MAGNET DumpIt for Windows, (x32, x64, ARM64), or MAGNET RAM Capture on legacy systems;
- 💻 Create a Triage collection with MAGNET Response;
- 🔐 Check for encrypted disks with Encrypted Disk Detector;
- 🔑 Recover the active BitLocker Recovery key;
- 💾 Save all artifacts, output, and audit logs to USB or source network drive.

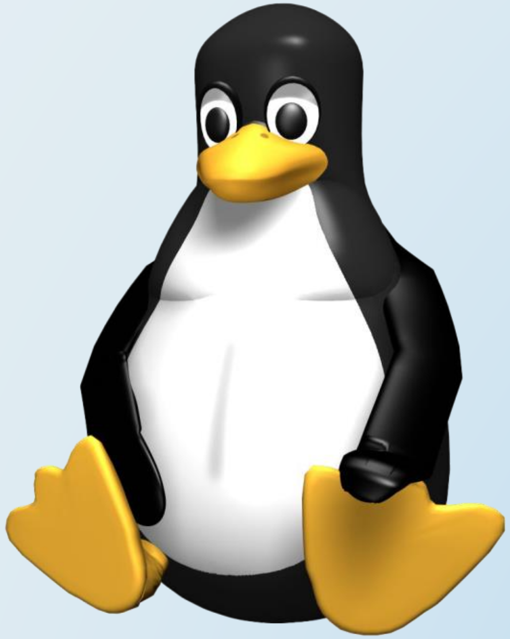
Collection Profiles:

- Volatile Artifacts
- Triage Collection (Volatile, RAM, Pagefile, Triage artifacts)
- Just RAM
- RAM & Pagefile
- or build your own using the RESPONSE CLI options

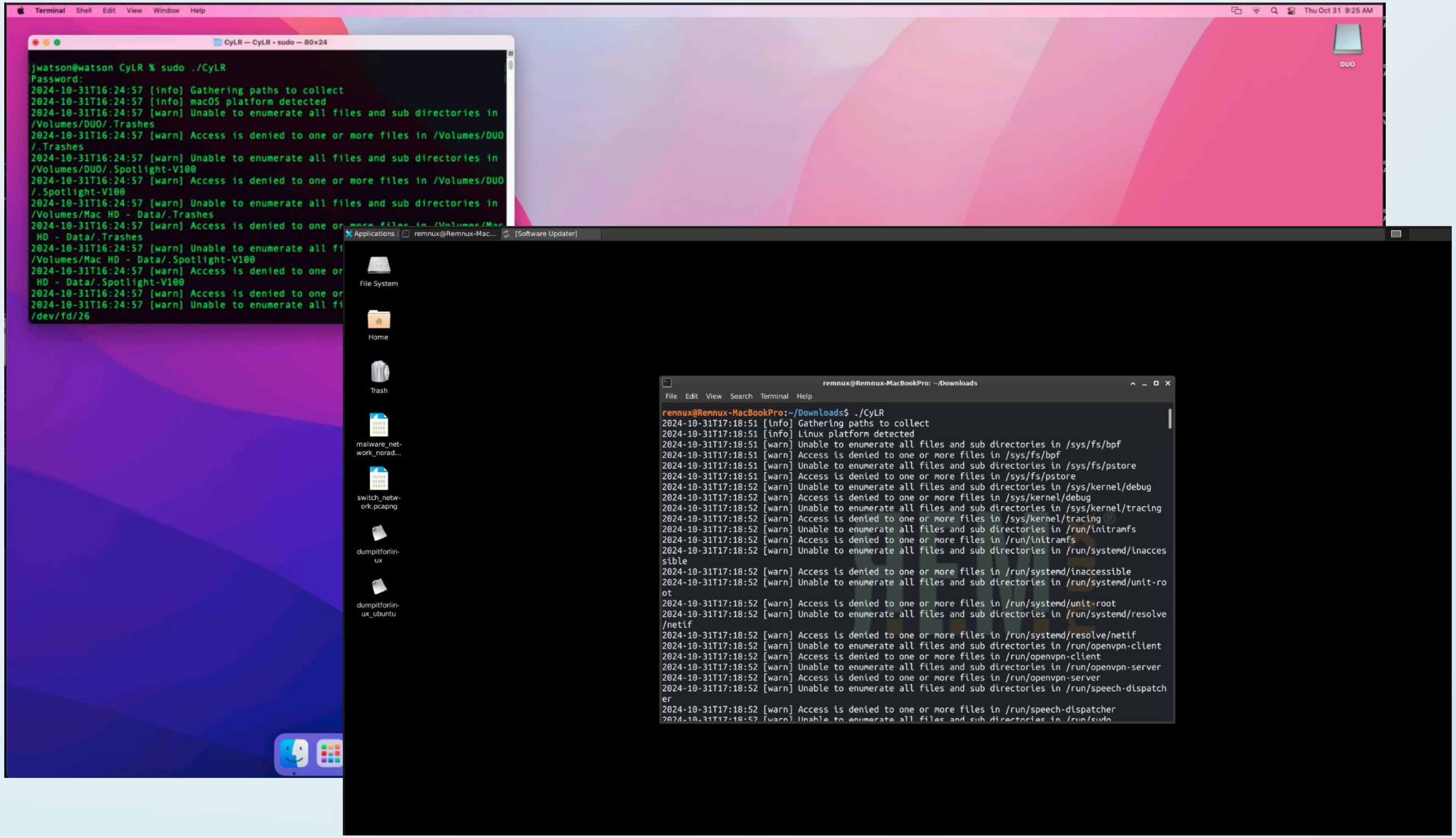
Prerequisites:

- MAGNET Response
- MAGNET Encrypted Disk Detector

Triage Collection for Mac & ‘Nix



CyLR



```
jwatson@watson CyLR % sudo ./CyLR
Password:
2024-10-31T16:24:57 [info] Gathering paths to collect
2024-10-31T16:24:57 [info] macOS platform detected
2024-10-31T16:24:57 [warn] Unable to enumerate all files and sub directories in
/Volumes/DUO/.Trashes
2024-10-31T16:24:57 [warn] Access is denied to one or more files in /Volumes/DUO
/.Trashes
2024-10-31T16:24:57 [warn] Unable to enumerate all files and sub directories in
/Volumes/DUO/.Spotlight-V100
2024-10-31T16:24:57 [warn] Access is denied to one or more files in /Volumes/DUO
/.Spotlight-V100
2024-10-31T16:24:57 [warn] Unable to enumerate all files and sub directories in
/Volumes/Mac HD - Data/.Trashes
2024-10-31T16:24:57 [warn] Access is denied to one or more files in /Volumes/Mac
 HD - Data/.Trashes
2024-10-31T16:24:57 [warn] Unable to enumerate all fi
/Volumes/Mac HD - Data/.Spotlight-V100
2024-10-31T16:24:57 [warn] Access is denied to one or
 HD - Data/.Spotlight-V100
2024-10-31T16:24:57 [warn] Access is denied to one or
2024-10-31T16:24:57 [warn] Unable to enumerate all fi
/dev/fd/26
```

```
remnux@Remnux-MacBookPro:~/Downloads$ ./CyLR
2024-10-31T17:18:51 [info] Gathering paths to collect
2024-10-31T17:18:51 [info] Linux platform detected
2024-10-31T17:18:51 [warn] Unable to enumerate all files and sub directories in /sys/fs/bpf
2024-10-31T17:18:51 [warn] Access is denied to one or more files in /sys/fs/bpf
2024-10-31T17:18:51 [warn] Unable to enumerate all files and sub directories in /sys/fs/pstore
2024-10-31T17:18:51 [warn] Access is denied to one or more files in /sys/fs/pstore
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /sys/kernel/debug
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /sys/kernel/debug
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /sys/kernel/tracing
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /sys/kernel/tracing
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/initramfs
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /run/initramfs
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/systemd/inacces
sible
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /run/systemd/inaccessible
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/systemd/unit-ro
ot
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /run/systemd/unit-root
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/systemd/resolve
/netif
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /run/systemd/resolve/netif
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/openvpn-client
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /run/openvpn-client
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/openvpn-server
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /run/openvpn-server
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/speech-dispatch
er
2024-10-31T17:18:52 [warn] Access is denied to one or more files in /run/speech-dispatcher
2024-10-31T17:18:52 [warn] Unable to enumerate all files and sub directories in /run/sudo
```

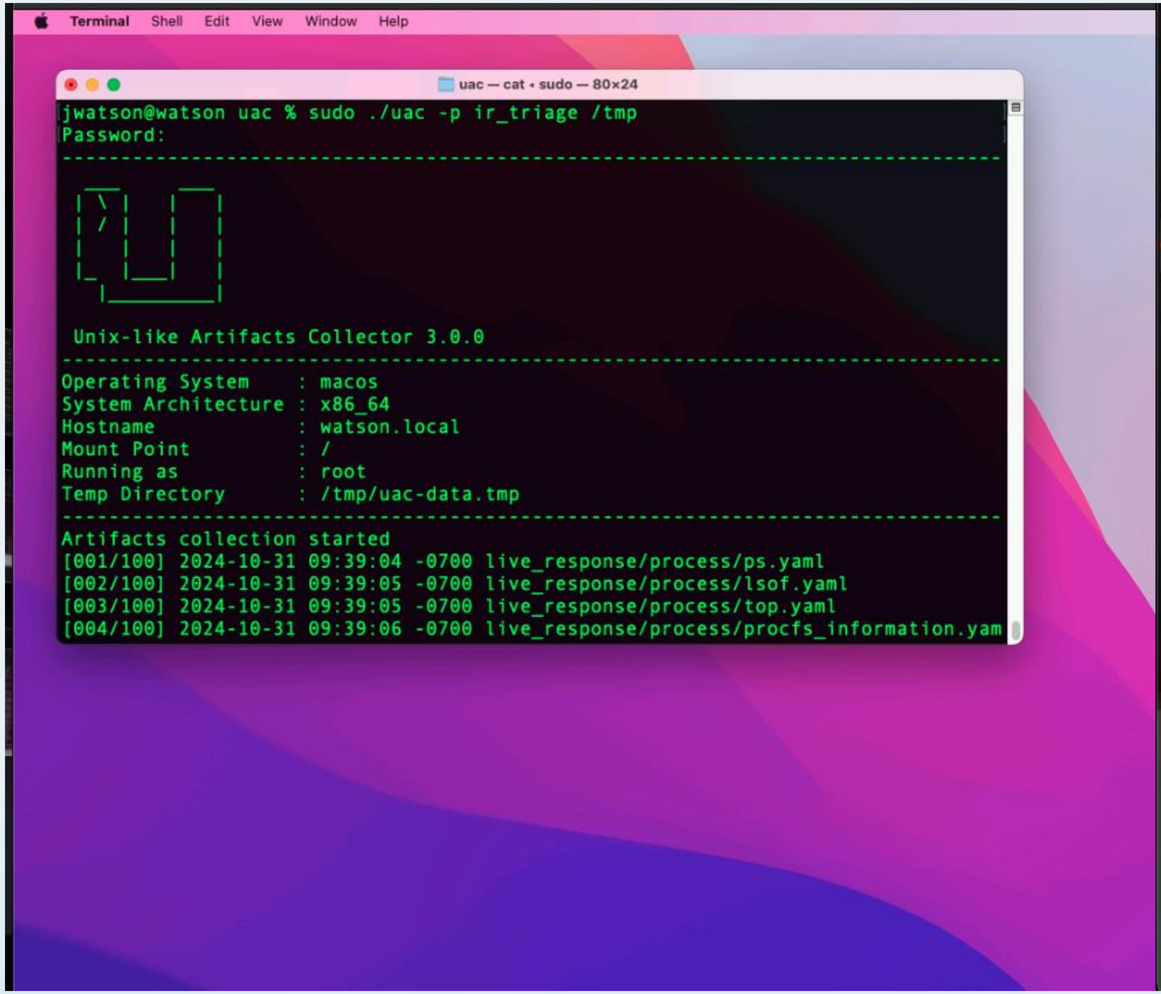
- Triage Collection
- Open-Source
- CLI
- Updated 2021 (v3)
- Windows, Linux, Mac
- Different executables for each
- Output zip file

UAC (Unix-like Artifacts Collector)

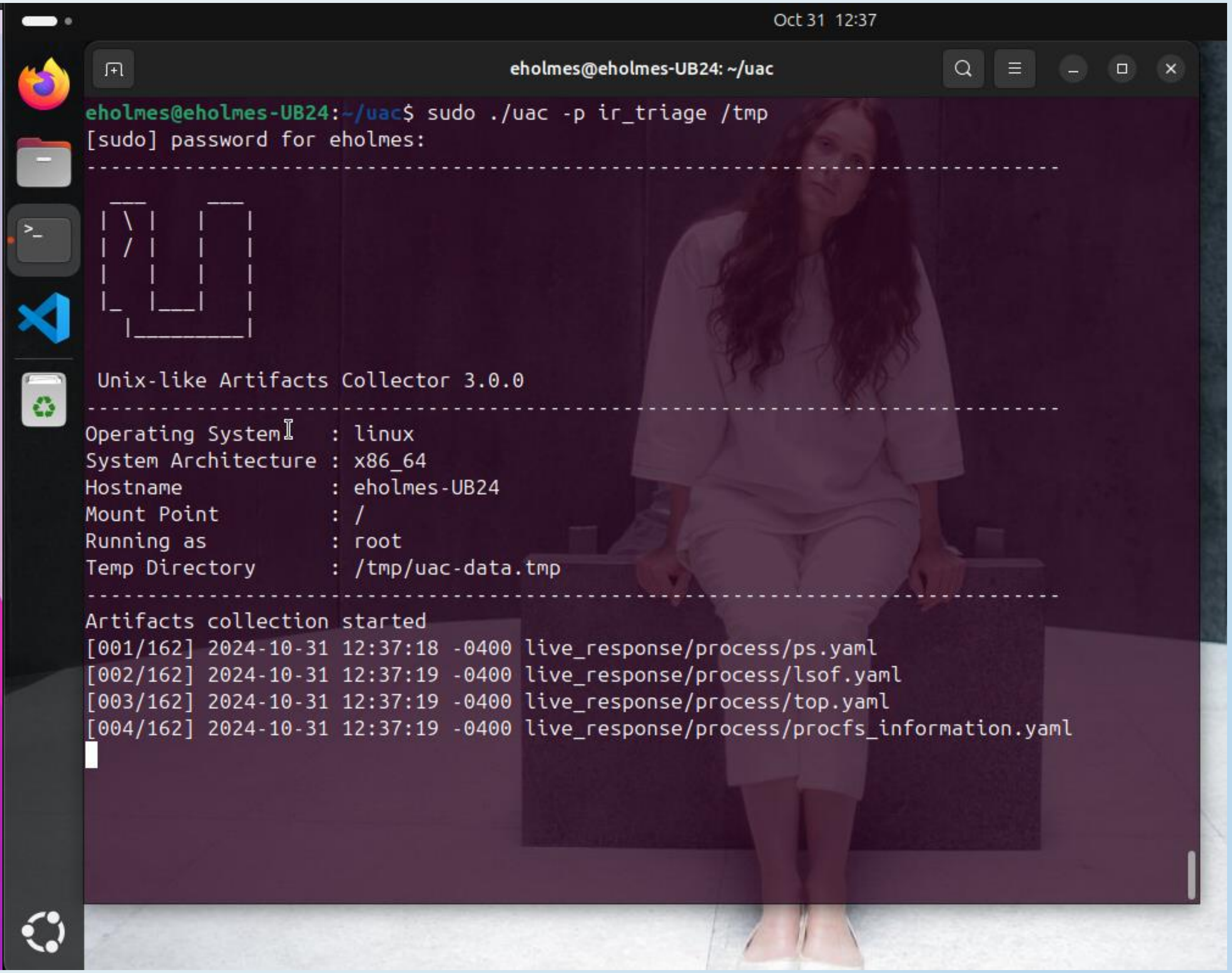
```
# ./uac -p ir_triage /tmp
```

- Triage Collection
- CLI
- Open-Source
- Actively maintained
- Linux, Mac, ESXi, OpenBSD, Solaris…+
- Extensible via YAML files

UAC (Unix-like Artifacts Collector)



```
jwatson@watson uac % sudo ./uac -p ir_triage /tmp
Password:
--------------------------------------------------------------------------------

  ___    ___
 | \ |  |   |
 | / |  |   |
 |   |  |   |
 |_  |__|   |
   |________|

 Unix-like Artifacts Collector 3.0.0
--------------------------------------------------------------------------------
Operating System    : macos
System Architecture : x86_64
Hostname            : watson.local
Mount Point         : /
Running as          : root
Temp Directory      : /tmp/uac-data.tmp
--------------------------------------------------------------------------------
Artifacts collection started
[001/100] 2024-10-31 09:39:04 -0700 live_response/process/ps.yaml
[002/100] 2024-10-31 09:39:05 -0700 live_response/process/lsof.yaml
[003/100] 2024-10-31 09:39:05 -0700 live_response/process/top.yaml
[004/100] 2024-10-31 09:39:06 -0700 live_response/process/procfs_information.yam
```



```
eholmes@eholmes-UB24:~/uac$ sudo ./uac -p ir_triage /tmp
[sudo] password for eholmes:
--------------------------------------------------------------------------------

  ___    ___
 | \ |  |   |
 | / |  |   |
 |   |  |   |
 |_  |__|   |
   |________|

 Unix-like Artifacts Collector 3.0.0
--------------------------------------------------------------------------------
Operating System    : linux
System Architecture : x86_64
Hostname            : eholmes-UB24
Mount Point         : /
Running as          : root
Temp Directory      : /tmp/uac-data.tmp
--------------------------------------------------------------------------------
Artifacts collection started
[001/162] 2024-10-31 12:37:18 -0400 live_response/process/ps.yaml
[002/162] 2024-10-31 12:37:19 -0400 live_response/process/lsof.yaml
[003/162] 2024-10-31 12:37:19 -0400 live_response/process/top.yaml
[004/162] 2024-10-31 12:37:19 -0400 live_response/process/procfs_information.yaml
```

Continue with

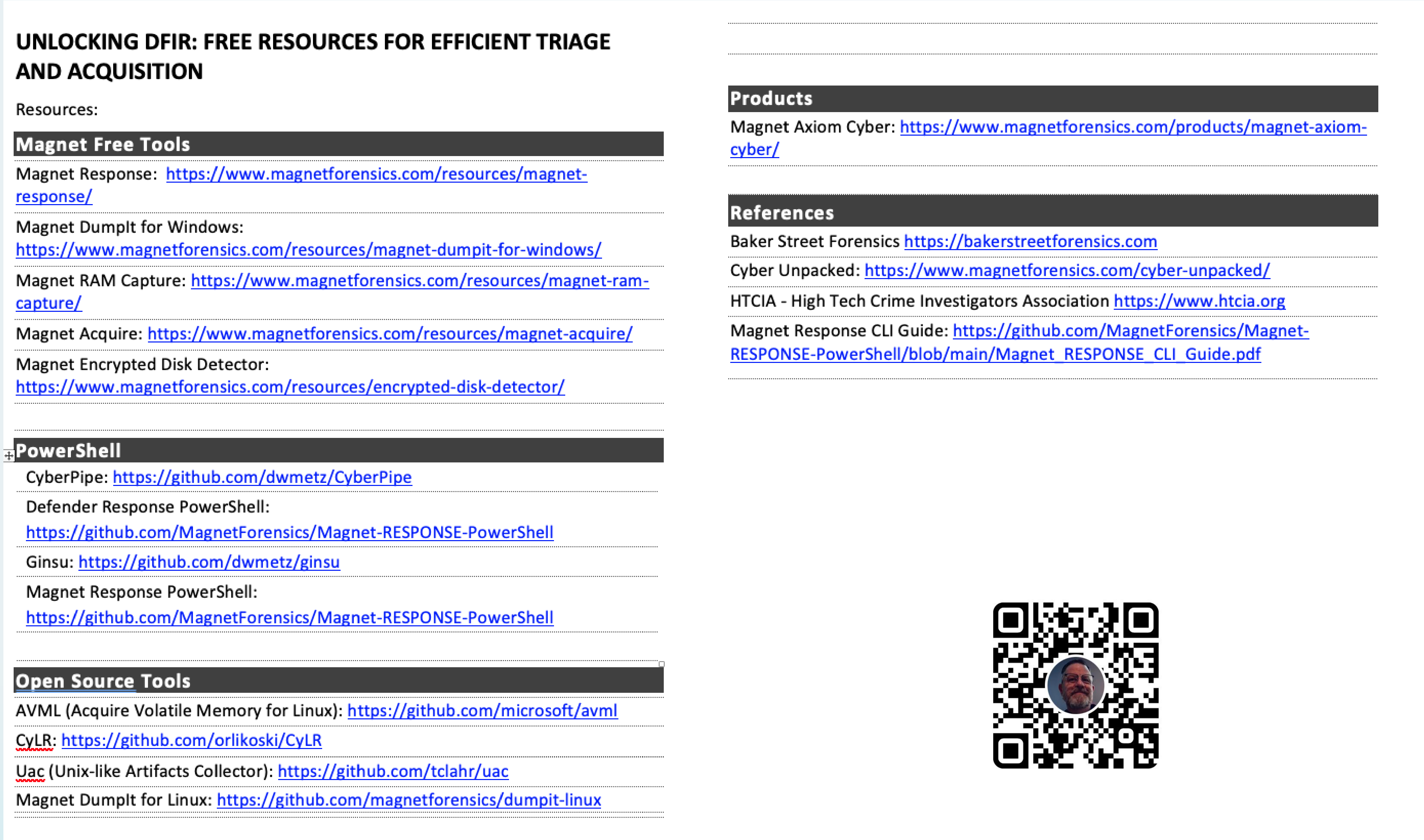
MAGNET AXIOM CYBER™

Sources:

- Magnet Acquire Images (.e01, .raw)
- Magnet RAM Capture Images (.raw)
- Magnet DumpIt for Windows (.dmp, .raw)
- Magnet Response Triage (.zip)
- CyberPipe (.zip, .dmp, .raw)
- CyLR (.zip)
- UAC (.zip)

Enhance the Evidence:

- Magnet.AI
- YARA
- MITRE ATT&CK
- $MFT
- Remote Acquisition
- Cloud Sources
- Co-Pilot



UNLOCKING DFIR: FREE RESOURCES FOR EFFICIENT TRIAGE AND ACQUISITION

Resources:

Magnet Free Tools

Magnet Response: https://www.magnetforensics.com/resources/magnet-response/

Magnet DumpIt for Windows: https://www.magnetforensics.com/resources/magnet-dumpit-for-windows/

Magnet RAM Capture: https://www.magnetforensics.com/resources/magnet-ram-capture/

Magnet Acquire: https://www.magnetforensics.com/resources/magnet-acquire/

Magnet Encrypted Disk Detector: https://www.magnetforensics.com/resources/encrypted-disk-detector/

PowerShell

CyberPipe: https://github.com/dwmetz/CyberPipe

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

Ginsu: https://github.com/dwmetz/ginsu

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

Open Source Tools

AVML (Acquire Volatile Memory for Linux): https://github.com/microsoft/avml

CyLR: https://github.com/orlikoski/CyLR

Uac (Unix-like Artifacts Collector): https://github.com/tclahr/uac

Magnet DumpIt for Linux: https://github.com/magnetforensics/dumpit-linux

Products

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

References

Baker Street Forensics https://bakerstreetforensics.com

Cyber Unpacked: https://www.magnetforensics.com/cyber-unpacked/

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

Magnet Response CLI Guide: https://github.com/MagnetForensics/Magnet-RESPONSE-PowerShell/blob/main/Magnet_RESPONSE_CLI_Guide.pdf

Thank You!

MVS Magnet Virtual Summit 2025

We Want Your Feedback!

Let us know what you thought of this Magnet Virtual Summit session by completing a quick survey. Plus you’ll also be able to earn points towards potential prizes for each survey you complete.

Thank you!