MAGNET USER SUMMIT 2024

HONEY, I RANSOMWARED THE KIDS

Building a Home or Small Office Lab For DFIR and Malware Analysis

Doug Metz, Senior Security Forensics Specialist
Magnet Forensics

MAGNET USER SUMMIT 2024

MAGNET USER SUMMIT 2024

MAGNET USER SUMMIT 2024

Honey, I Ransomwared the Kids: Building a Home Lab For DFIR and Malware Analysis

Doug Metz, Senior Security Forensics Specialist, Magnet Forensics

Monday, Apr 15 | 4:30 PM - 5:30 PM CDT

MAGNET FORENSICS®

The **Aux**tera Project

BAKER STREET FORENSICS

D . F . I . R .

HTCIA

Delaware Valley - Philadelphia

MAGNET USER SUMMIT 2024

NASHVILLE | MAGNETUSERSUMMIT.COM | #MUS2024

Abstract

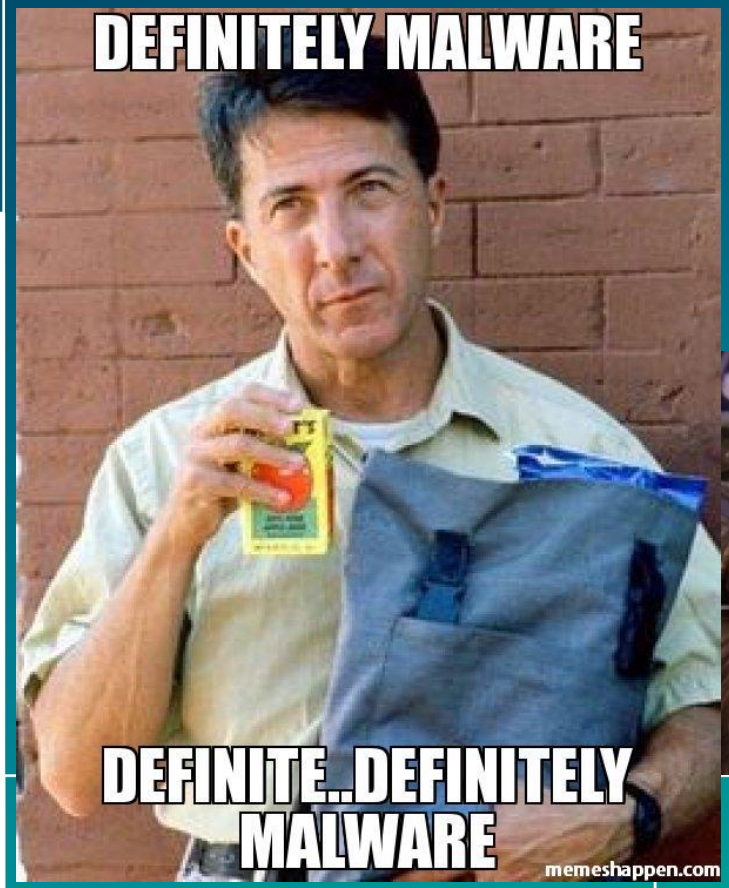
This session will review hardware and software recommendations for building a home or small office lab for DFIR and Malware analysis, and how not to compromise yourself or your loved ones in the process.

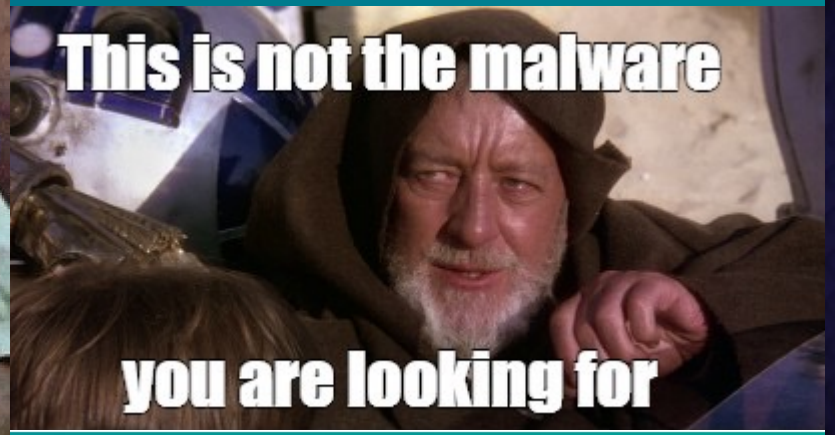
Please be sure to handle all malware with caution. Only you can prevent forest fires. Knowing is half the battle.

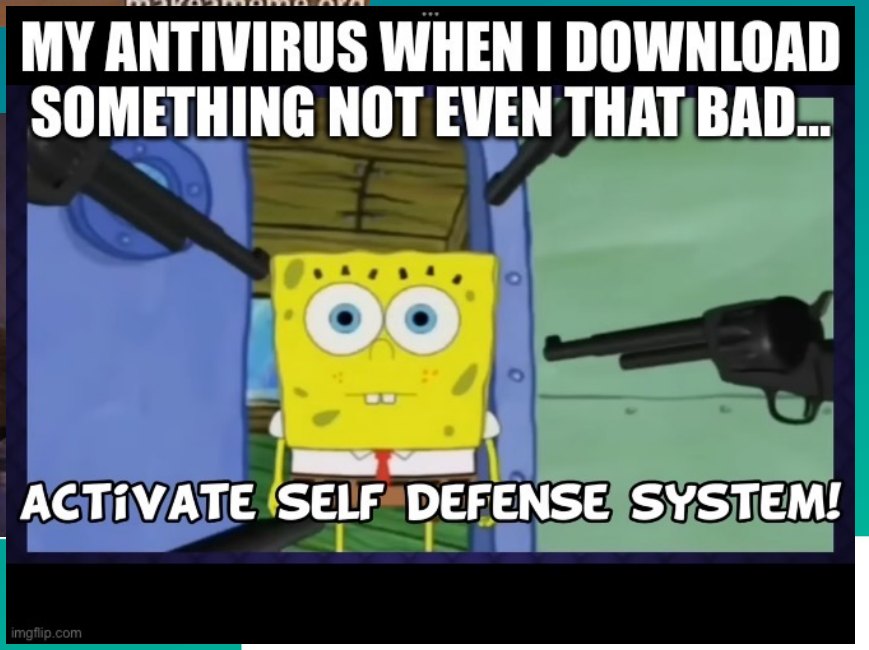

OOOOHH. MALWARE!
DOES IT COME IN A SET?


MALWARE
MALWARE EVERYWHERE


YO QUERO
RANSOMWARE?
imgflip.com


DEFINITELY MALWARE
DEFINITE..DEFINITELY MALWARE
memeshappen.com


This is not the malware
you are looking for


MY ANTIVIRUS WHEN I DOWNLOAD SOMETHING NOT EVEN THAT BAD...
ACTIVATE SELF DEFENSE SYSTEM!
imgflip.com

Topics

- Minimum hardware for SOHO Malware Lab
- Platform: ESXI v8
- Setting up an isolated network
- Virtual machines for analysis
- Internet access for compromised systems
- PowerShell utilities for basic malware analysis
- Goodware vs. Malware and how to get them

Hardware

Manufacturer	Intel(R) Client Systems
Model	NUC11PAHi7
CPU	4 CPUs x 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz
Memory	63.63 GB

Manufacturer	Synology
Model	DS920+
CPU	INTEL Celeron J4125 - 2GHZ (4 Cores)
Memory	4096 MB RAM
HDD:	4x Seagate IronWolf 16TB NAS Internal Hard Drive HDD - CMR 3.5 Inch SATA 6GB/S 7200 RPM 256MB Cache for Raid Network Attached Storage (ST16000VN001)

USB Network:	Amazon Basics USB 3.0 to 10/100/1000 Gigabit Ethernet Internet Adapter, Black

LTE Internet:	NETGEAR 4G LTE Broadband Modem (LM1200)

< $4,000 USD

The Lack Rack

Platform: ESXi v8

vmware by Broadcom | Multi-Cloud Services | Products | Solutions | Partners | Resources | GET STARTED

Home / Evaluate VMware Products / VMware vSphere Hypervisor 8

Product Evaluation Center for VMware vSphere Hypervisor 8

This download center features technical documentation and installation guides to make your use of vSphere Hypervisor a success.

Top vSphere Hypervisor Resources

- VMware Hardware Compatibility Guide

Installation & Configuration | License & Download | Troubleshooting & Support | Upgrade

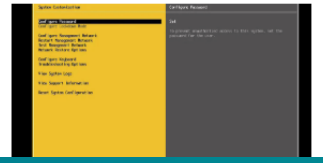
vSphere Hypervisor – Install & Configure

Thank you for downloading vSphere Hypervisor

Introductory Resources

Installing, Deploying and Using vSphere Hypervisor

Videos
Installing, Deploying and Using vSphere Hypervisor



- vSphere Hypervisor - Installation & Configuration
- vSphere Hypervisor - License Overview
- vSphere Hypervisor - vSphere Client Installation
- vSphere Hypervisor - Installing and Importing VM

vmware CUSTOMER CONNECT | Products and Accounts | Support | Knowledge | Communities | Success | Learning | DM

Home / VMware vSphere

Download VMware vSphere

Select Version: 8.0

Customers who have purchased vSphere 8 can download their relevant installation package from the product download tab below. Looking to upgrade from vSphere 7.0? Visit the vSphere Upgrade Center.

Get Your vSphere License Key

Read More

Product Resources
- View My Download History
- Product Information
- Documentation
- vSphere Community
- Support Resources
- Download Free Trial

Product Downloads | Drivers & Tools | Open Source | Custom ISOs | OEM Addons

Product	Release Date	
Essentials		
VMware vSphere Hypervisor (ESXi) 8.0U2	2023-09-21	GO TO DOWNLOADS
VMware vCenter Server 8.0U2a	2023-10-26	GO TO DOWNLOADS
VMware NSX 4.1.2.1 For vShield Endpoint	2023-11-07	GO TO DOWNLOADS
VMware Tools 12.3.5	2023-10-26	GO TO DOWNLOADS
Essentials Plus		
VMware vSphere Hypervisor (ESXi) 8.0U2	2023-09-21	GO TO DOWNLOADS
VMware vCenter Server 8.0U2a	2023-10-26	GO TO DOWNLOADS
VMware vSphere Replication 8.8.0.2	2023-11-21	GO TO DOWNLOADS
VMware NSX 4.1.2.1 For vShield Endpoint	2023-11-07	GO TO DOWNLOADS

Download: link in resource slide

What the Fling?

- ESXi 8.0 **finally** has a native driver for the NUC's NIC, which saves us the trouble of creating a custom install ISO or manually installing the community VIB (VMWare Installation Bundle) later.

VMWare Remote Console

MacOS: Download from **Apple app store**

Linux and Windows: Download from **VMWare Customer Connect**

Management & Internet Networks

- Before creating the dedicated malware network ensure that the VMs can reach the internet
- Pull down any available updates for operating system or tooling
- Check ping connectivity between VM assets

Primary VM Network - Internet

Virtual Machines for Analysis

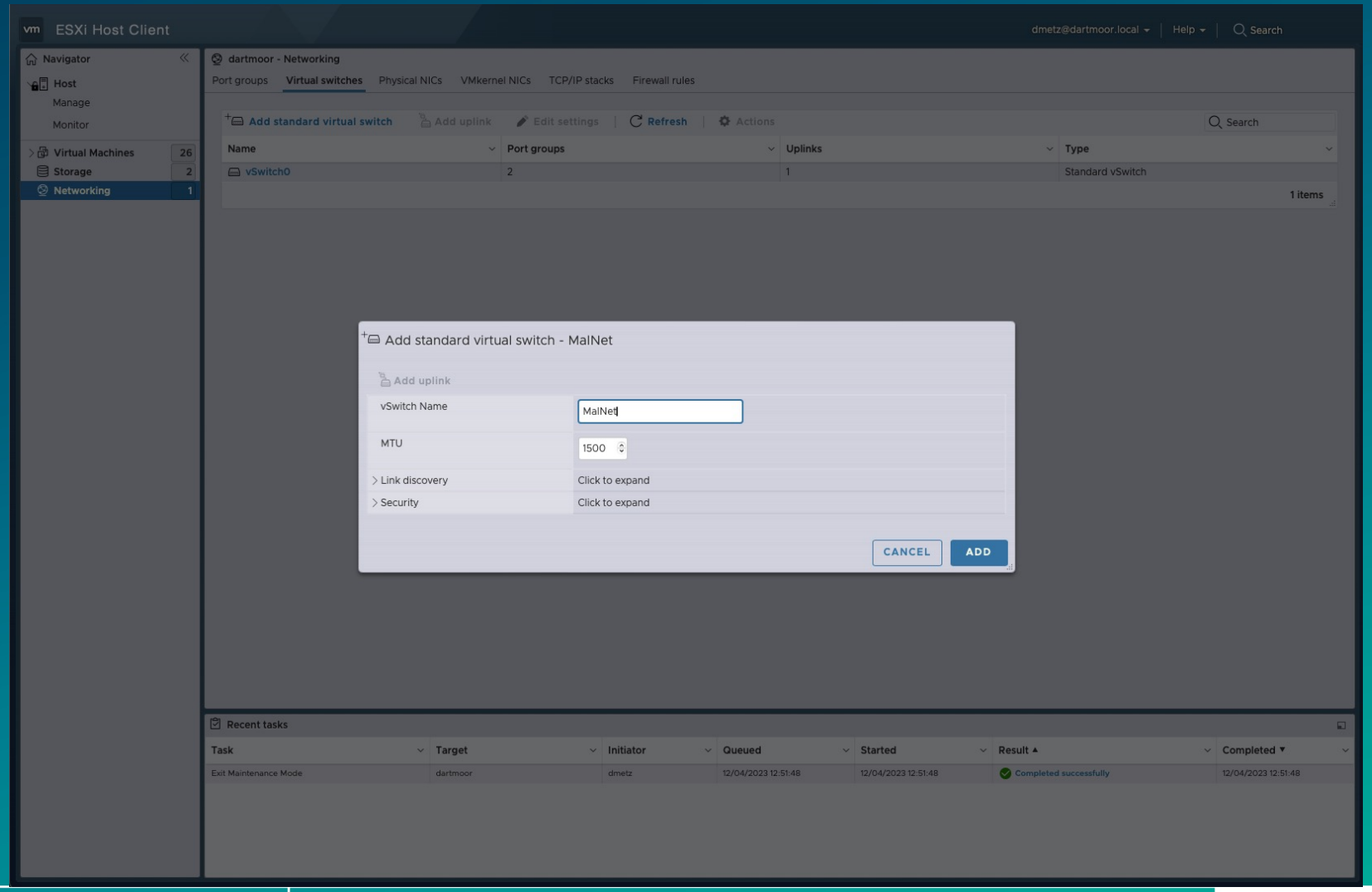
REMnux

FLARE

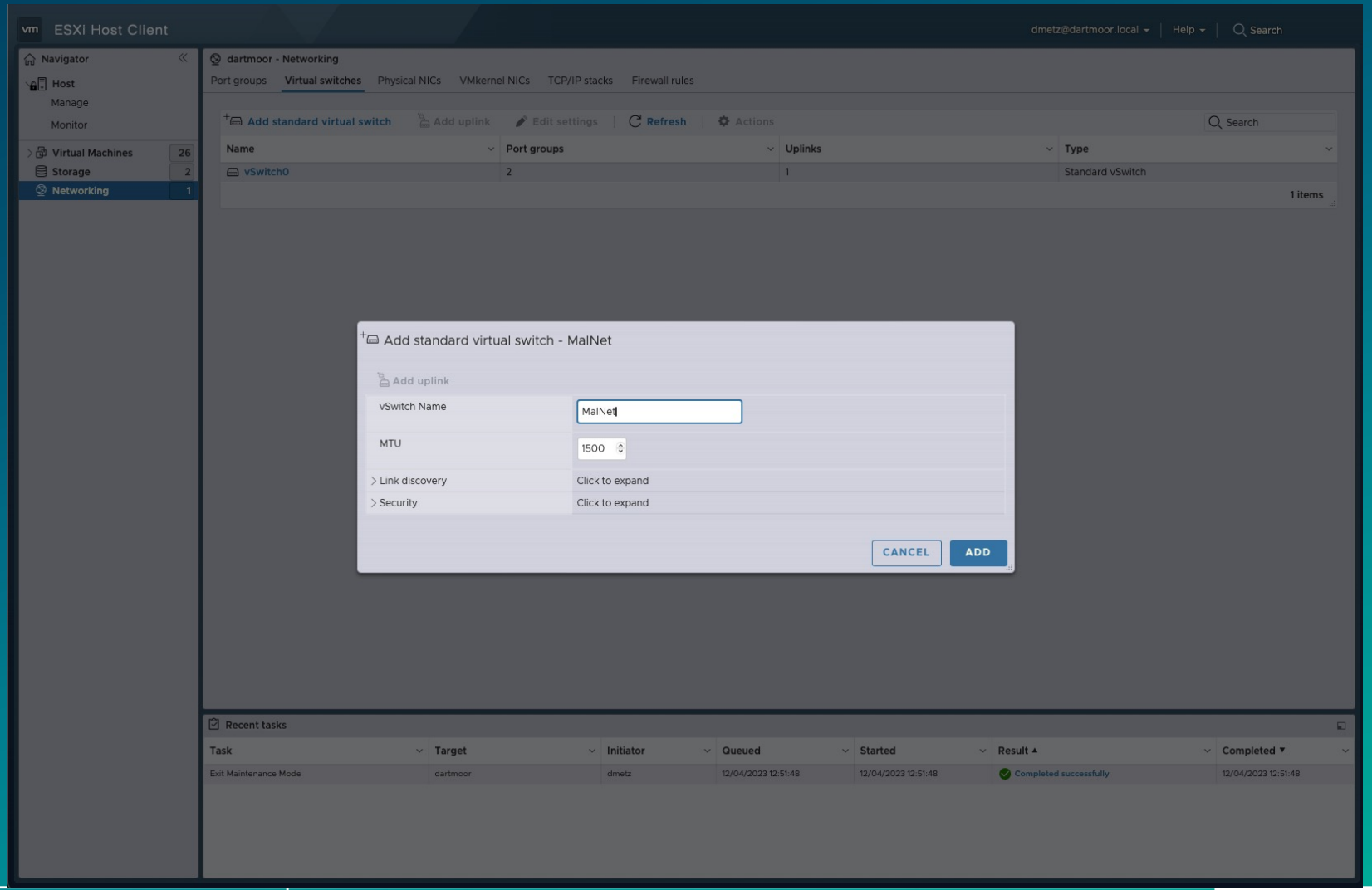
Windows10/11

Creating the Malware Network

Add a virtual switch

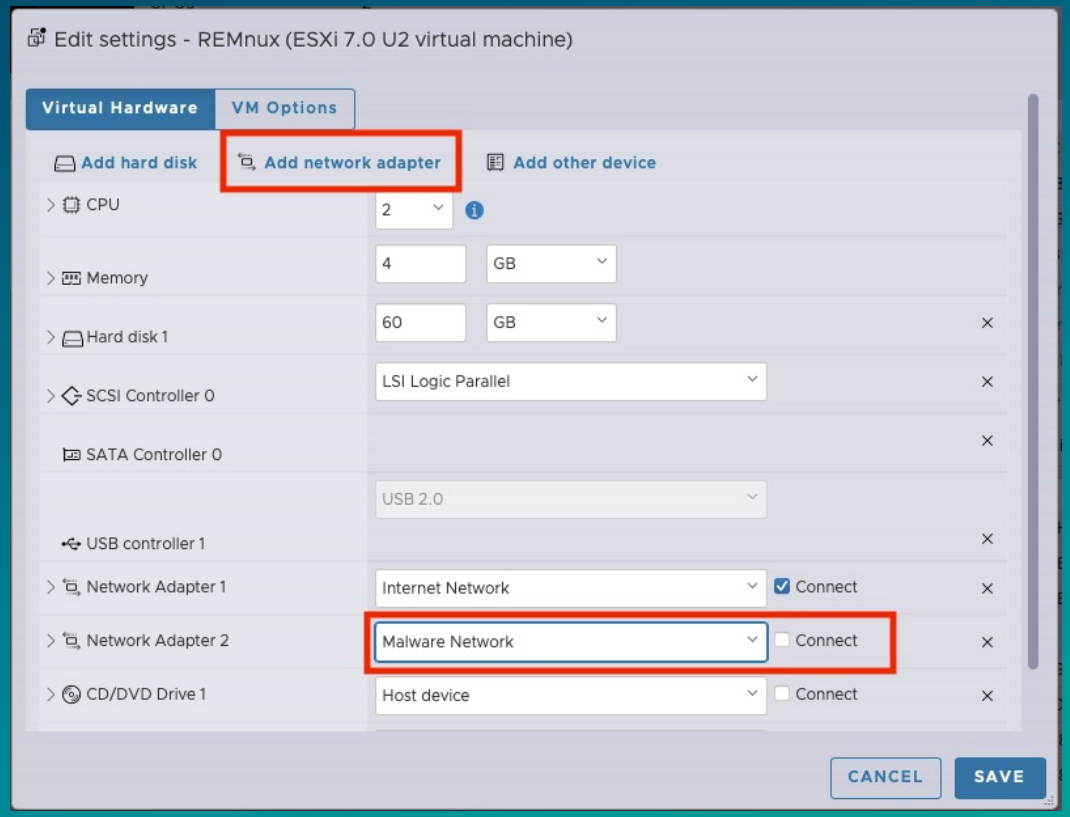


Add a port group



Add a Malware Network Adapter

Add a 2nd network adapter to the configuration of any *malware* assets

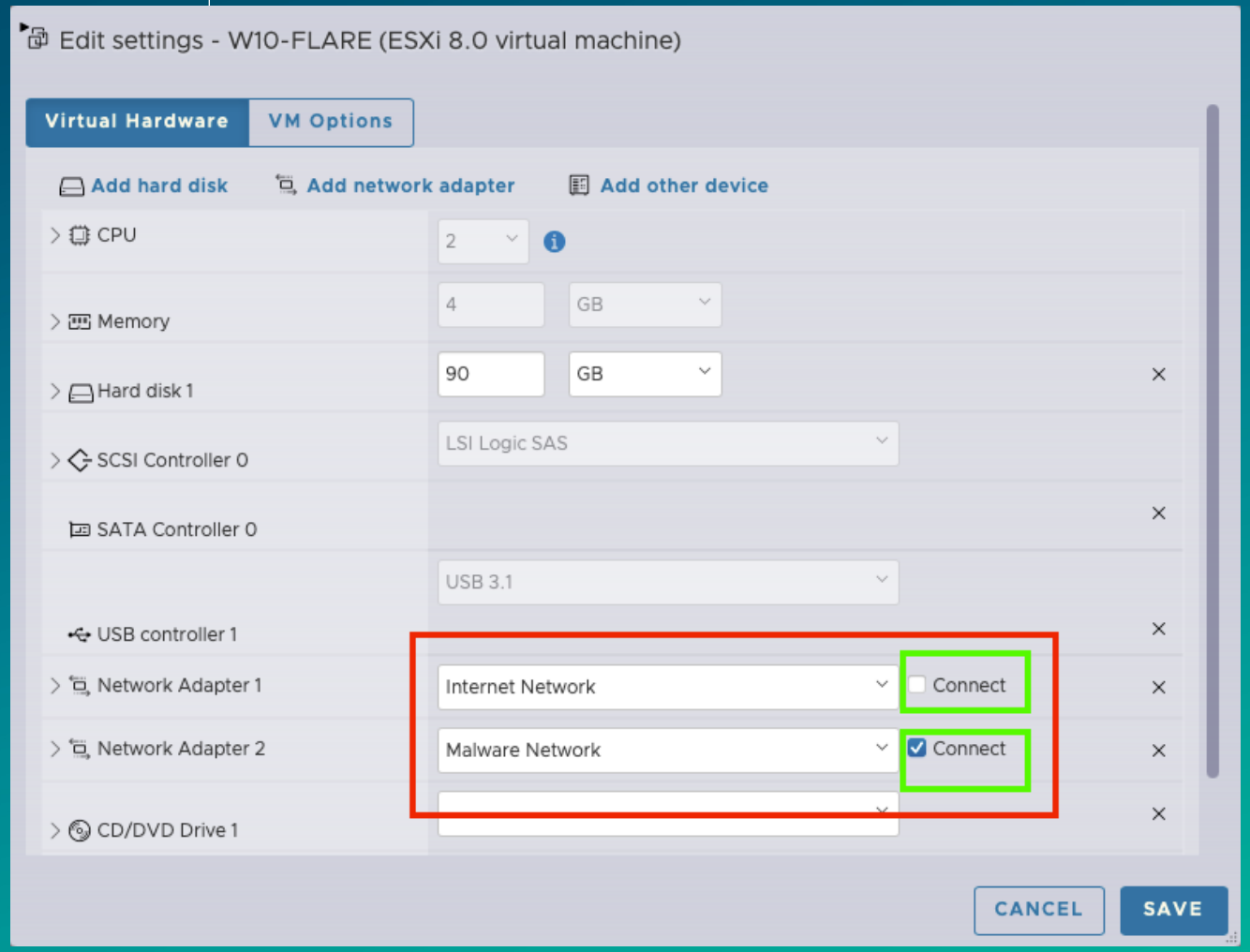


Primary Network - Malware Network - Internet

The Malware Network - Isolated

- Disconnect the Internet network adapter(s)
- Connect the Malware network adapter(s)
- Enable static IPs on the malware asset(s)
- Ping between malware assets ✅
- Ping 8.8.8.8 ❌

Primary Network - Malware Assets - Internet

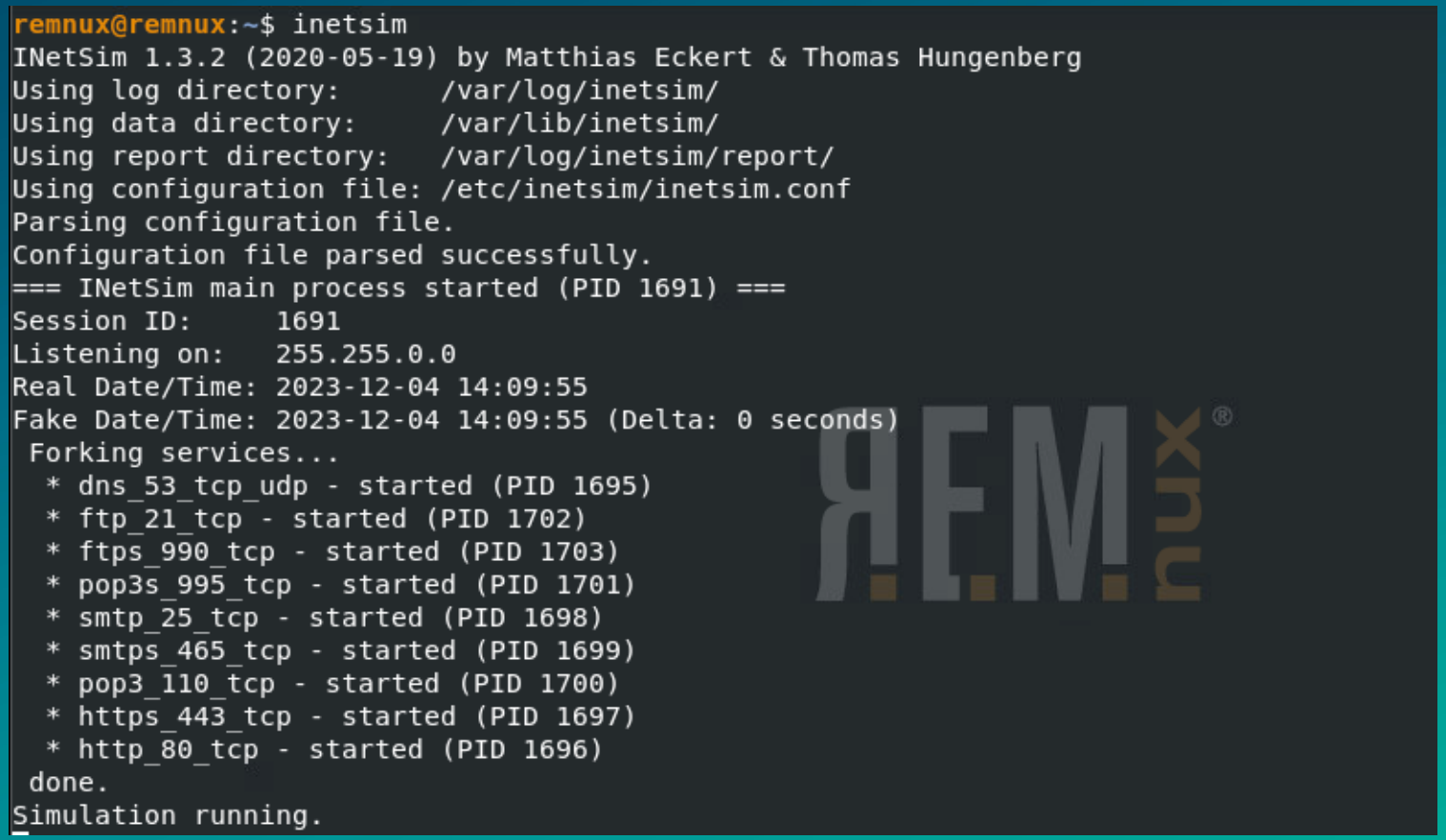


The Malware Network - Inetsim

Enable Inetsim on REMnux to emulate network services, including DNS, HTTP, and FTP

Edit /etc/inetsim/inetsim.conf with:

```
start_service dns
service_bind_address <REMNUX_IP>
dns_default_ip <REMNUX_IP>
```



Windows Guest > Inetsim

Ping REMnux ✅

NSLookup (DNS) – any query returns REMnux IP ✅

Ping External ❌

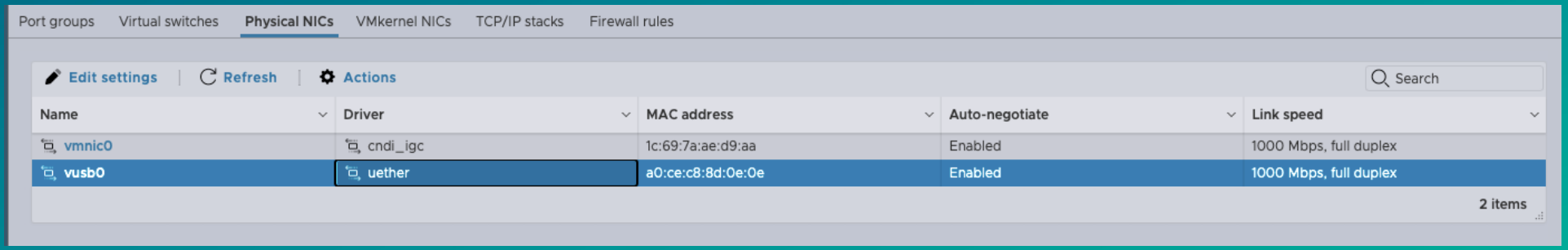
Primary Network - Malware Network – (Simulated) Internet

```
PS C:\Users\Admin> ping 10.0.1.1

Pinging 10.0.1.1 with 32 bytes of data:
Reply from 10.0.1.1: bytes=32 time<1ms TTL=64
Reply from 10.0.1.1: bytes=32 time<1ms TTL=64
Reply from 10.0.1.1: bytes=32 time<1ms TTL=64
Reply from 10.0.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 10.0.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\Admin> nslookup
Default Server:  www.inetsim.org
Address:  10.0.1.1

> www.suspiciousserver.net
Server:  www.inetsim.org
Address:  10.0.1.1

Name:    www.suspiciousserver.net
Address:  10.0.1.1

>
PS C:\Users\Admin> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% l
PS C:\Users\Admin>
```

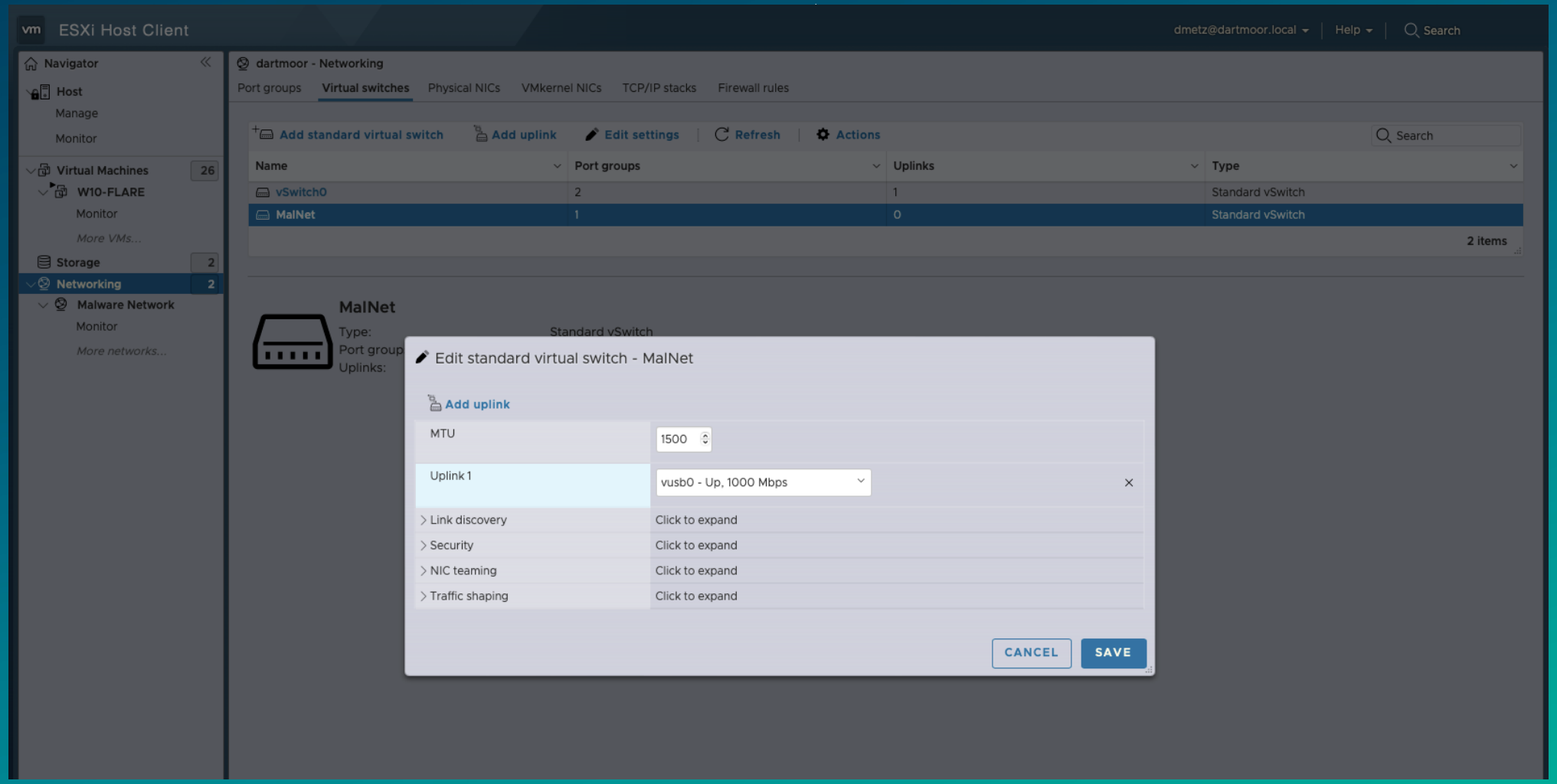
Connecting the Malware Network to the Internet

LTE Hotspot & USB Network Adapter

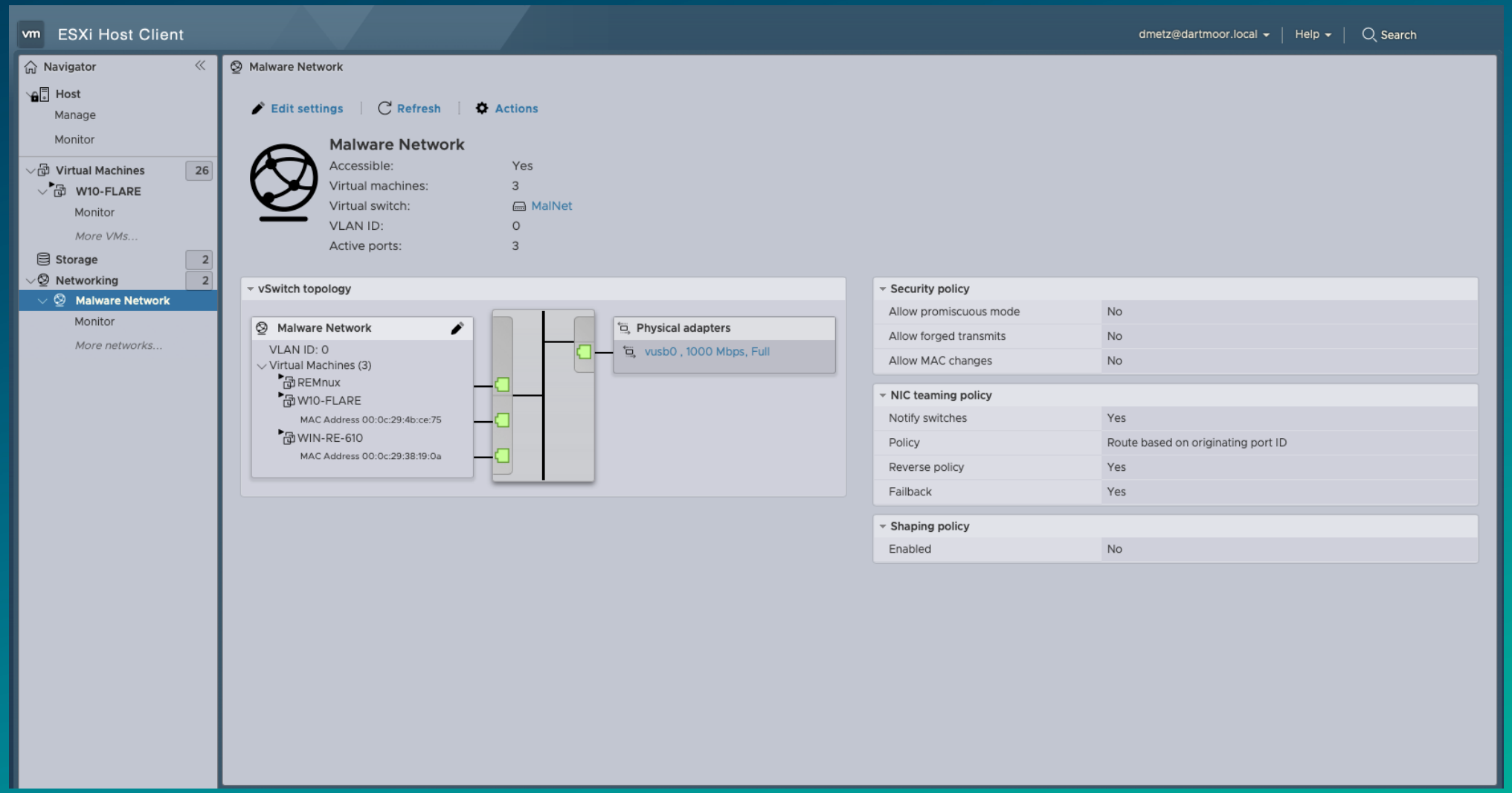
- Insert SIM card in hotspot
- Connect laptop to hotspot – verify connectivity; it's *easier to troubleshoot single connection.*
- Once LTE verified and distributing IP/Internet then connect to VMWare.
  - Attach USB adapter to NUC
  - Connect network cable from hotspot to USB adapter
  - "Hey Siri, turn on the Malware Network" (power on hotspot)



Virtual Switch – Add Uplink



Verify Uplink



Switch to DHCP

- For any of the malware assets that you want to be able to communicate with the internet, set the network adapters to DHCP
- The devices will get their IP and DNS information from the Hotspot

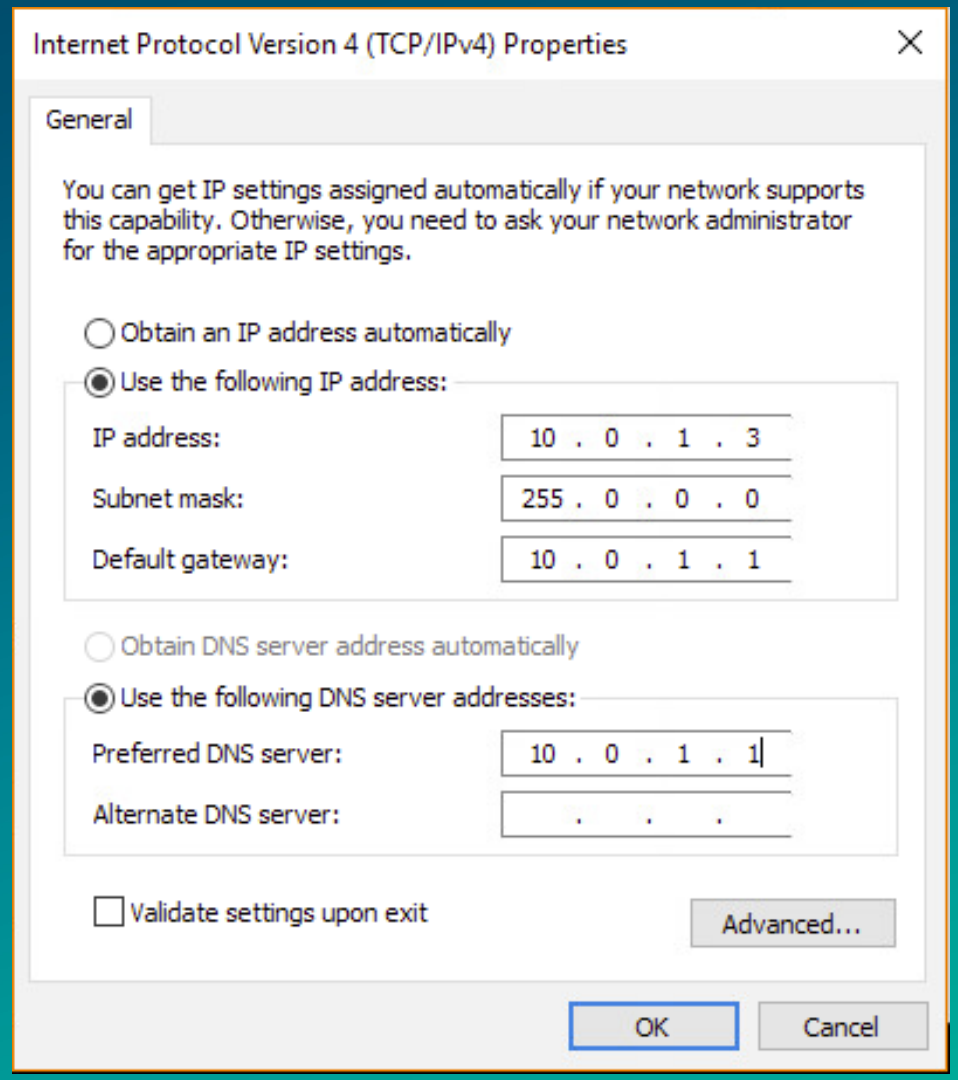
Primary Network - Malware Network - Internet

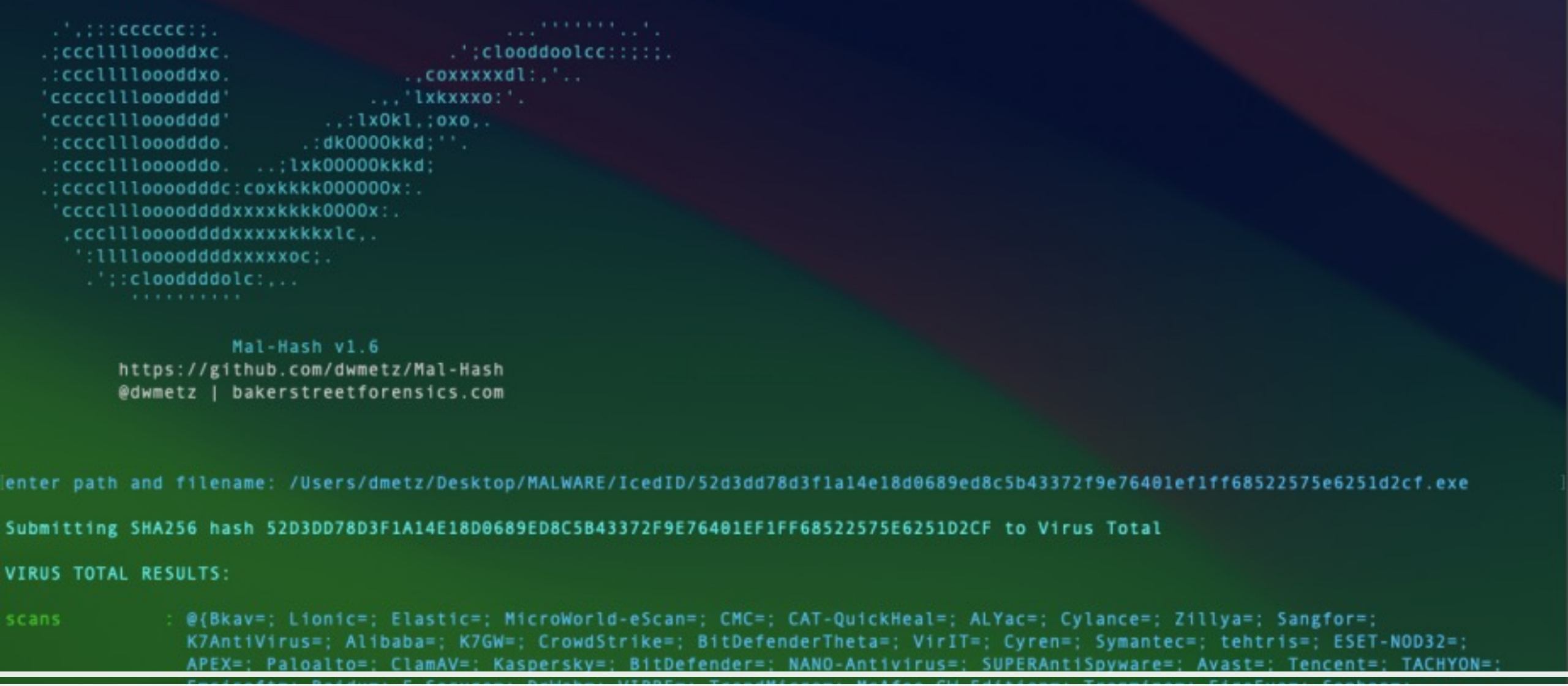
```
PS C:\Users\Admin> ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:
Request timed out.

Ping statistics for 192.168.4.1:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
Control-C
PS C:\Users\Admin> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=47ms TTL=54
Reply from 8.8.8.8: bytes=32 time=45ms TTL=54

Ping statistics for 8.8.8.8:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 47ms, Average = 46ms
Control-C
PS C:\Users\Admin> ping www.google.com

Pinging www.google.com [2607:f8b0:4006:821::2004] with 32 bytes of data:
Reply from 2607:f8b0:4006:821::2004: time=51ms
Reply from 2607:f8b0:4006:821::2004: time=55ms
Reply from 2607:f8b0:4006:821::2004: time=49ms

Ping statistics for 2607:f8b0:4006:821::2004:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```

Back to Manual

- To return the assets to the (non-Internet) malware network, set the IP addresses back to manual.
- Turn of hotspot
- Inetsim (optional)

Primary Network - Malware Network - Internet





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.*

Capturing Malware Evidence with detonaRE

detonaRE – from Latin-ish, *to detonate*

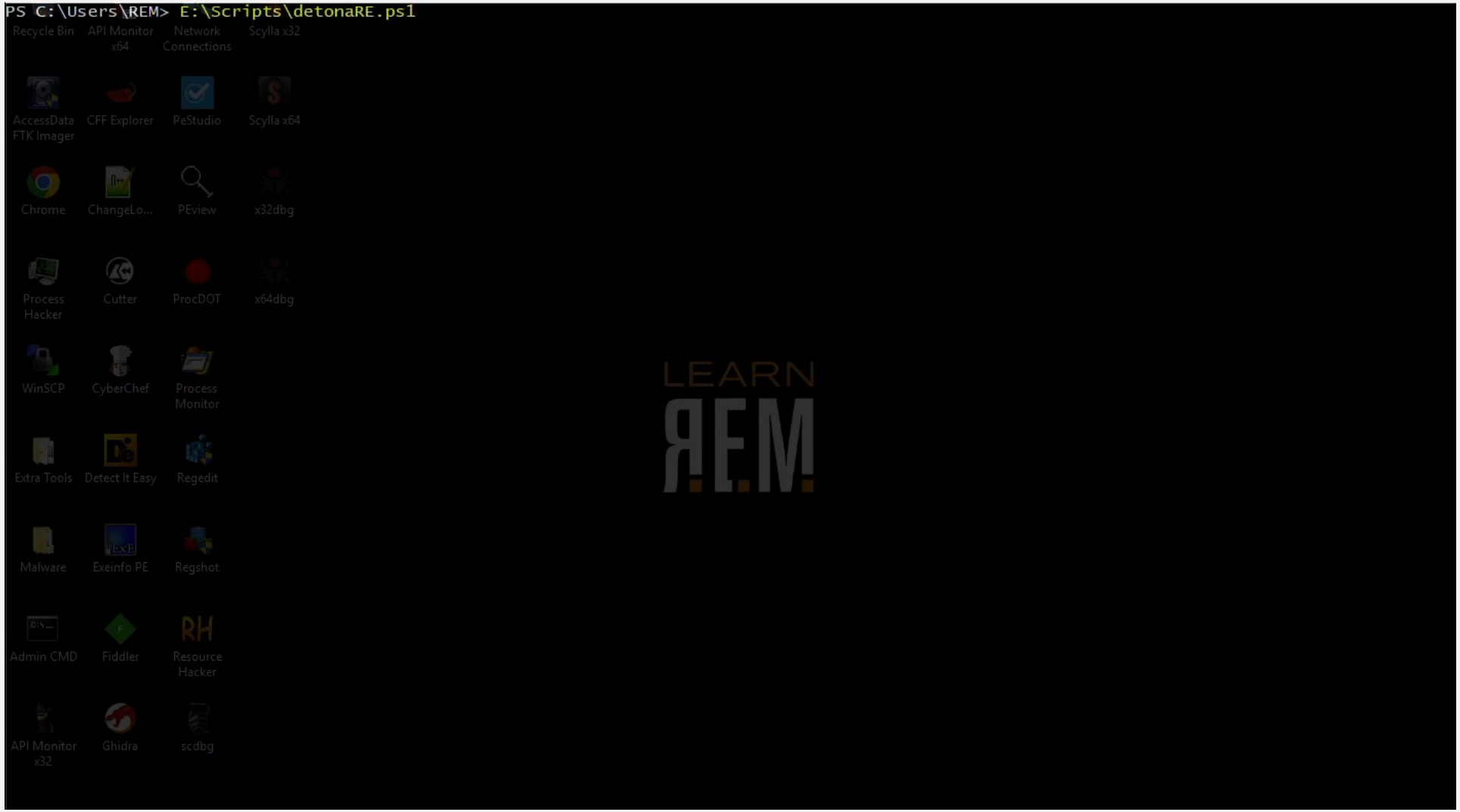
- initiates packet capture
- launches malware sample
- terminates packet capture after specified time interval
- initiates evidence collection with **Magnet RESPONSE** (Memory, Process, and Triage capture) *
- converts collected .etl file (network capture) to .pcap with **etl2pcapng**.
    - Alternate: Volatile, Memory, Pagefile, Process

detonaRE – configuration

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” ## location of MagnetRESPONSE and etl2pcapng exe’s
```

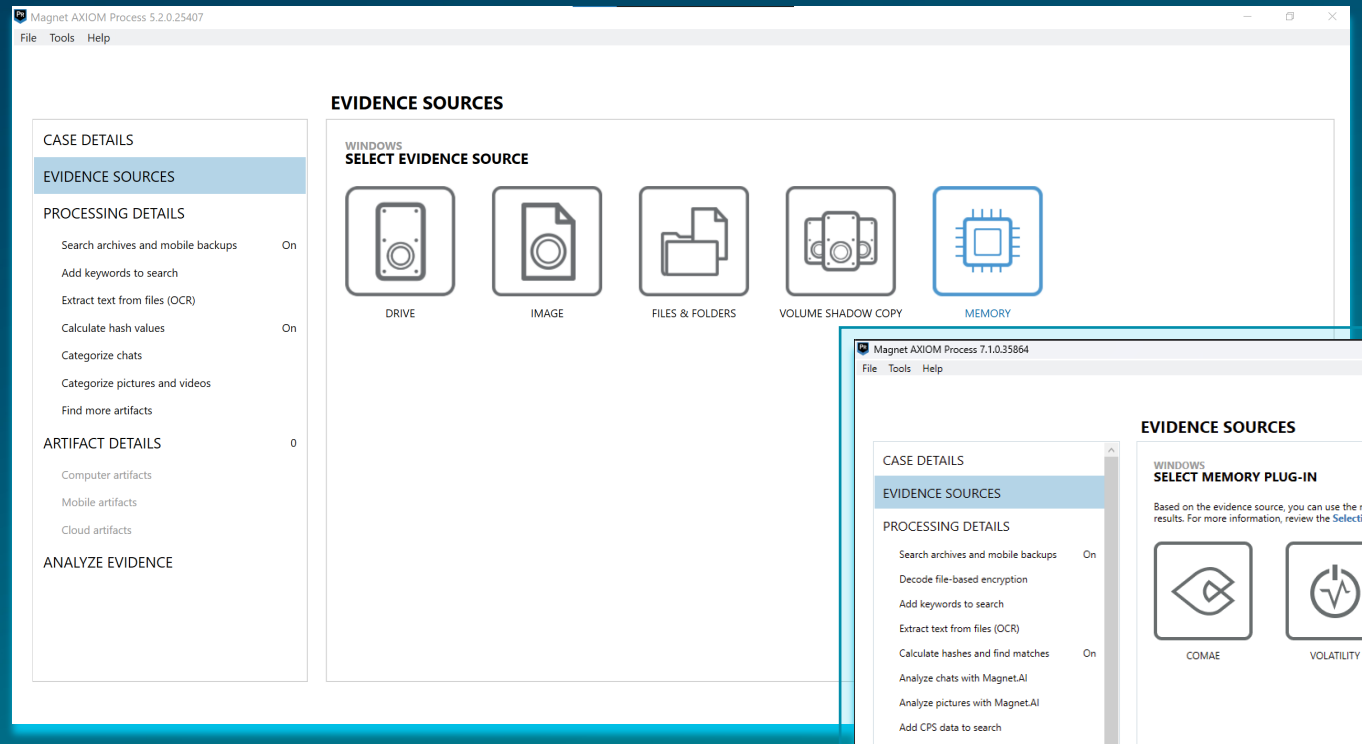
detonaRE – demo

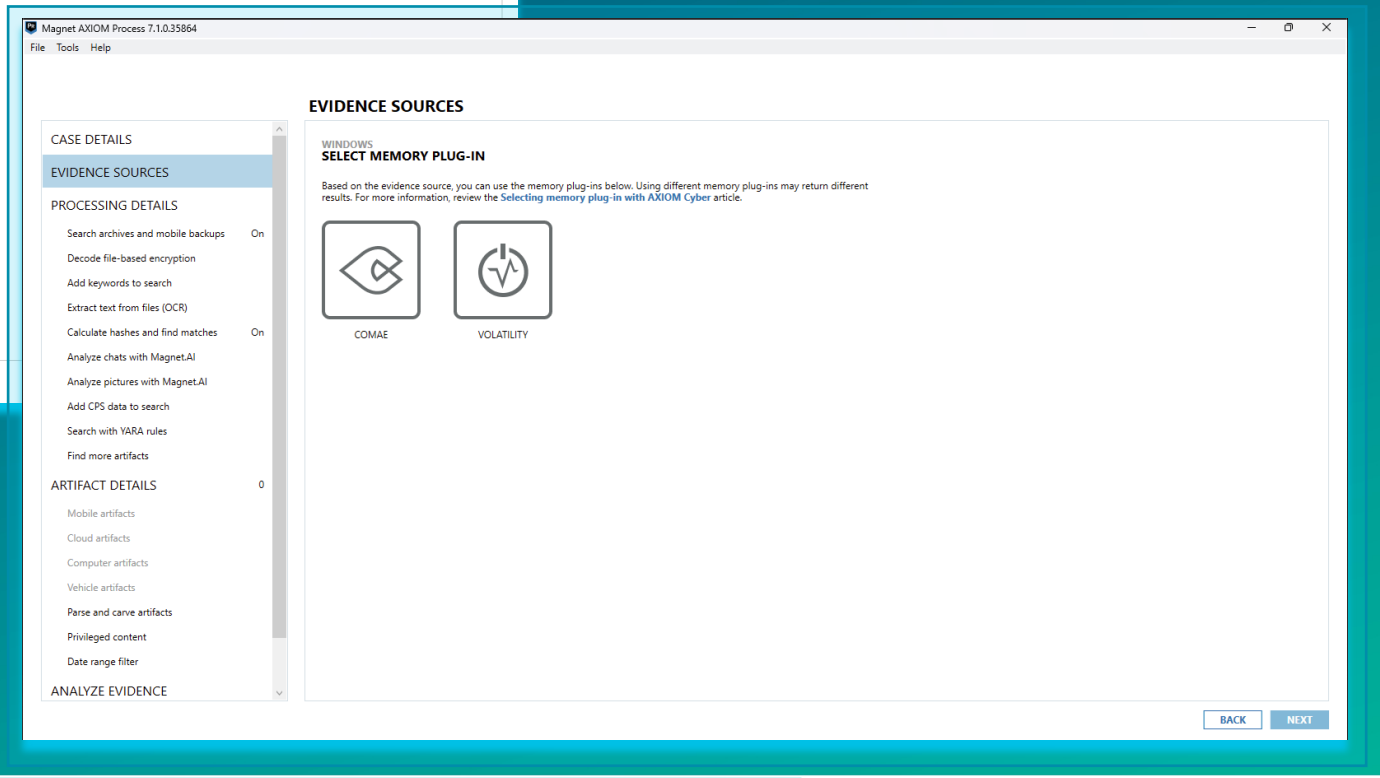


Processing Malware Evidence with

MAGNET AXIOM™ CYBER

Comae Memory Processing

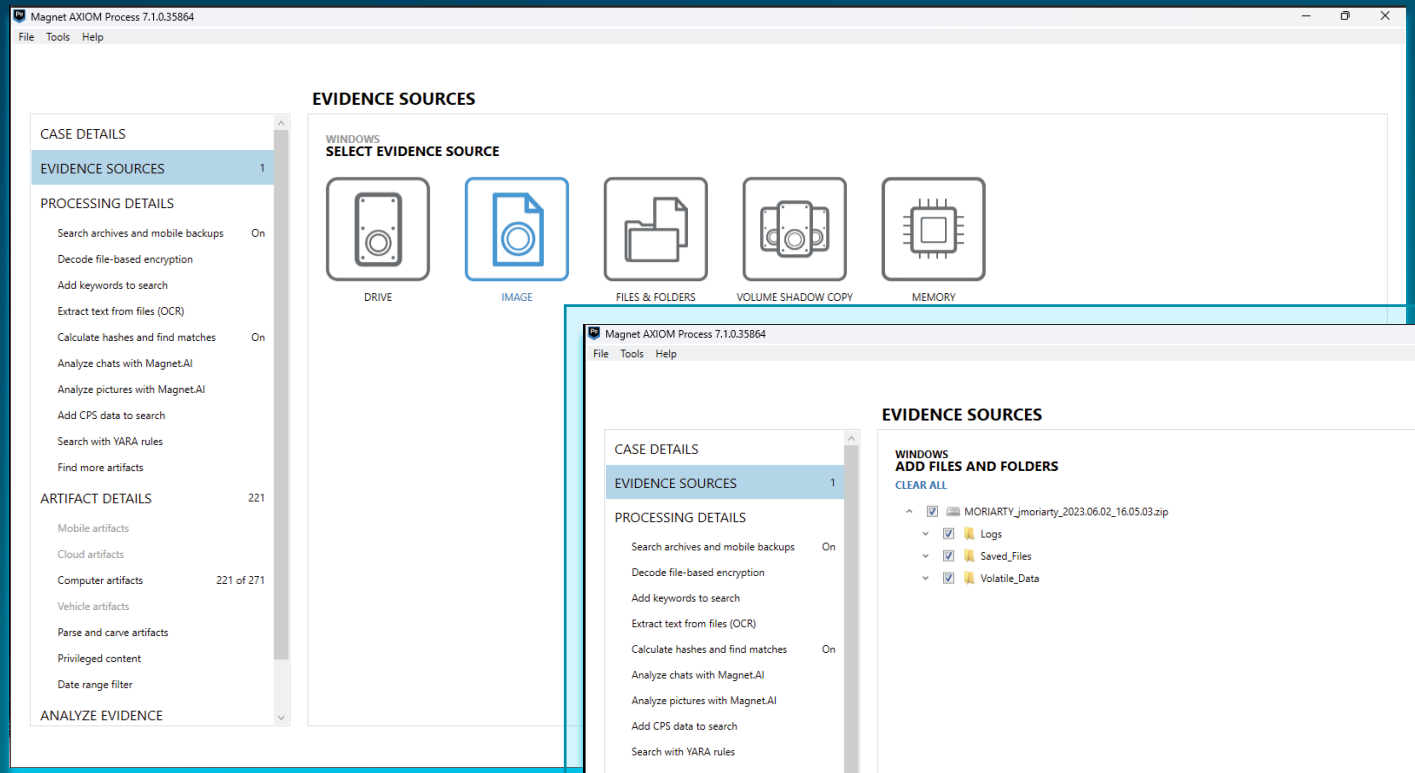


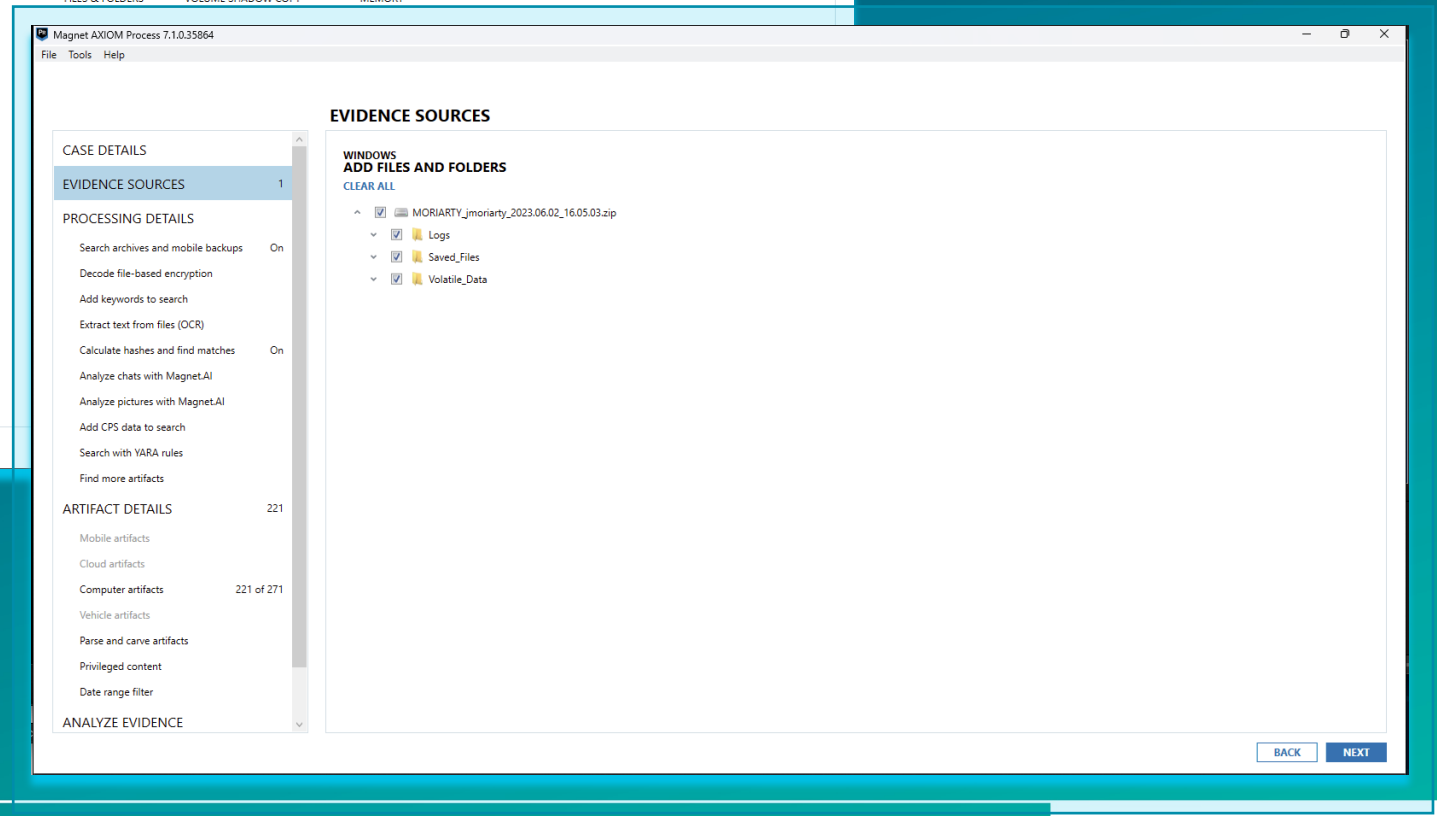


Computer > Windows > Load Evidence > Memory

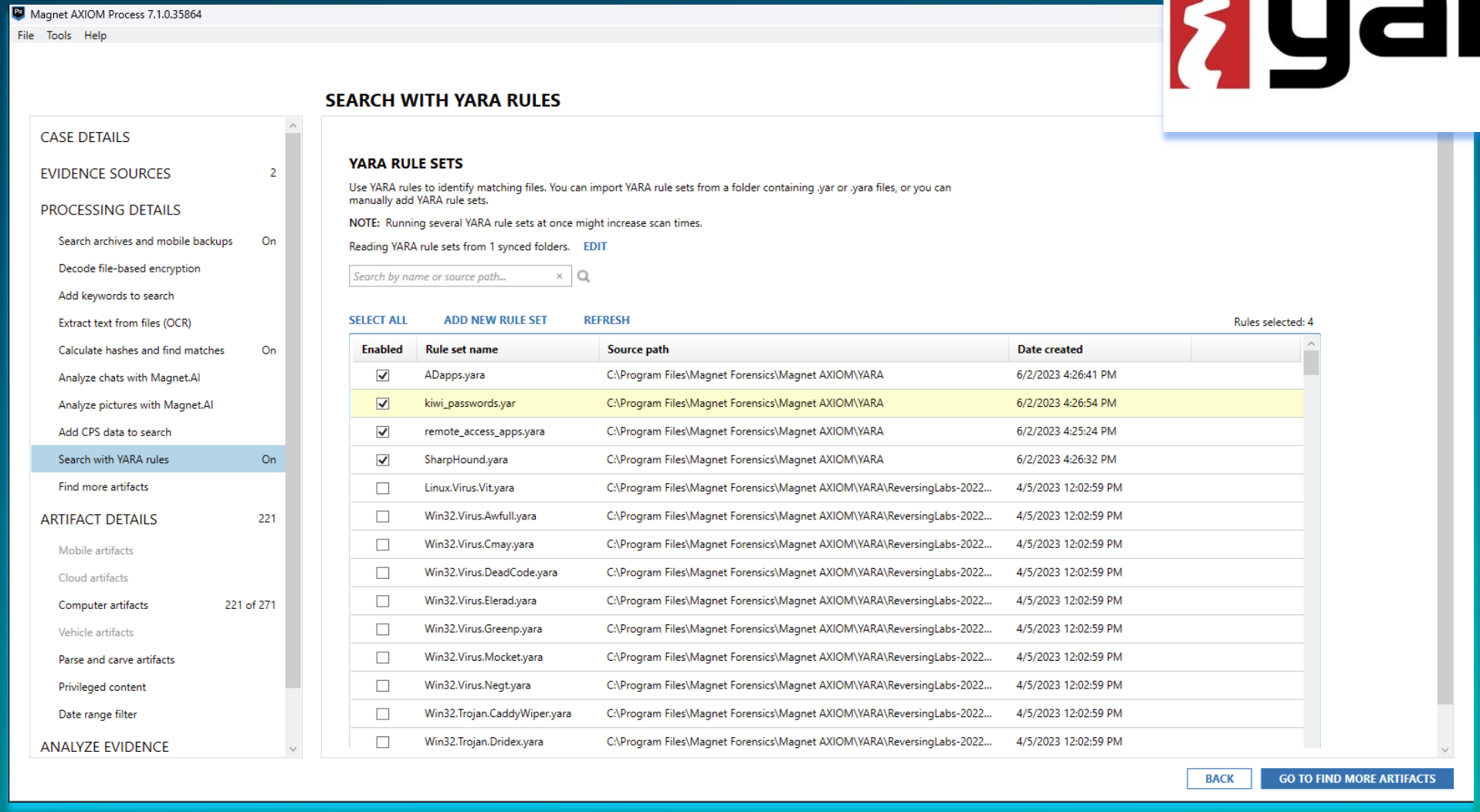
Triage Processing

Computer > Windows > Load Evidence > IMAGE

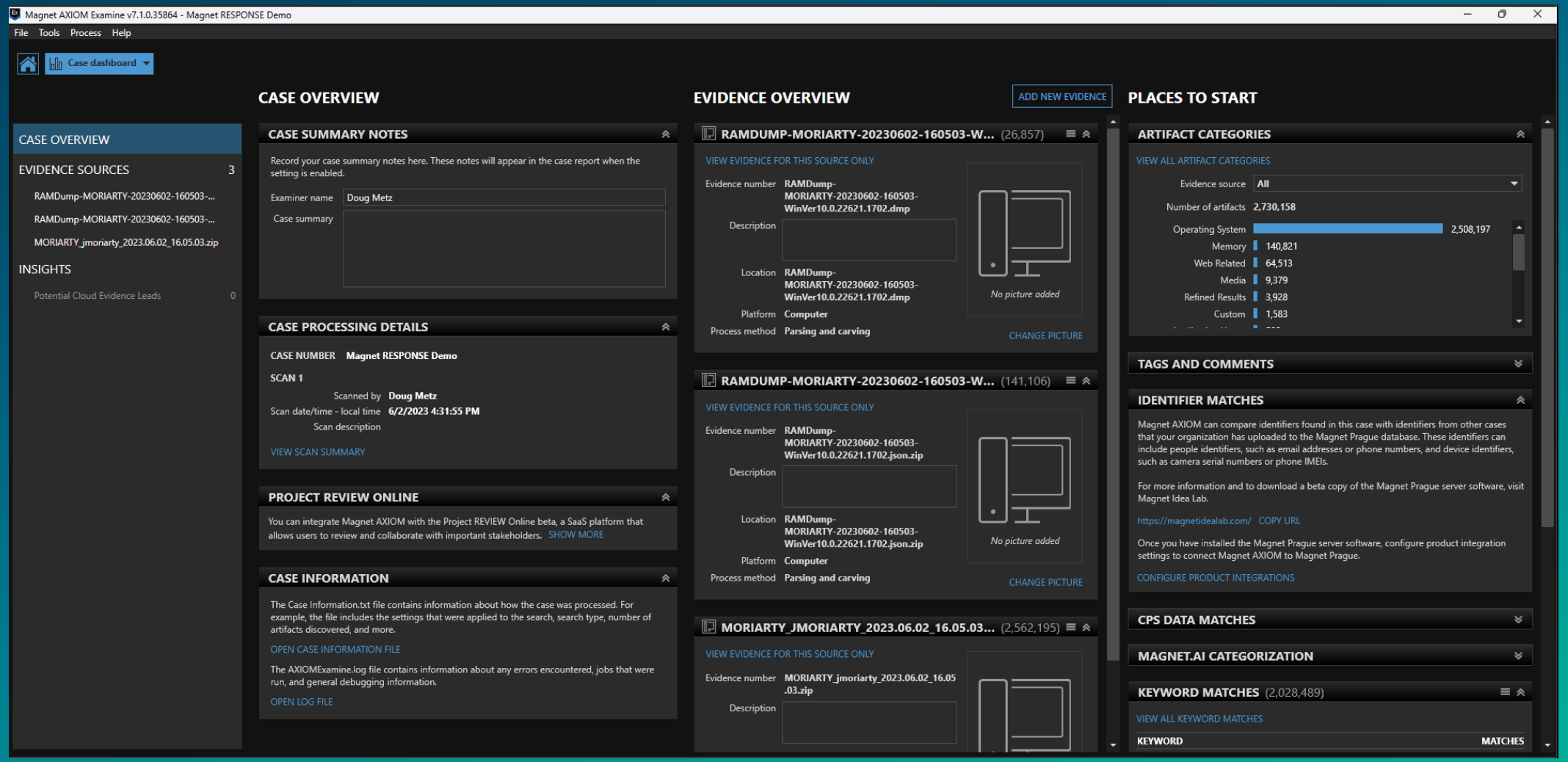




YARA


Magnet AXIOM Process 7.1.0.35864
File Tools Help
SEARCH WITH YARA RULES
CASE DETAILS
EVIDENCE SOURCES 2
PROCESSING DETAILS
Search archives and mobile backups On
Decode file-based encryption
Add keywords to search
Extract text from files (OCR)
Calculate hashes and find matches On
Analyze chats with Magnet.AI
Analyze pictures with Magnet.AI
Add CPS data to search
Search with YARA rules On
Find more artifacts
ARTIFACT DETAILS 221
Mobile artifacts
Cloud artifacts
Computer artifacts 221 of 271
Vehicle artifacts
Parse and carve artifacts
Privileged content
Date range filter
ANALYZE EVIDENCE
YARA RULE SETS
Use YARA rules to identify matching files. You can import YARA rule sets from a folder containing .yar or .yara files, or you can manually add YARA rule sets.
NOTE: Running several YARA rule sets at once might increase scan times.
Reading YARA rule sets from 1 synced folders. EDIT
Search by name or source path...
SELECT ALL ADD NEW RULE SET REFRESH
Rules selected: 4
Enabled | Rule set name | Source path | Date created
ADapps.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA | 6/2/2023 4:26:41 PM
kiwi_passwords.yar | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA | 6/2/2023 4:26:54 PM
remote_access_apps.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA | 6/2/2023 4:25:24 PM
SharpHound.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA | 6/2/2023 4:26:32 PM
Linux.Virus.Vit.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Virus.Awfull.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Virus.Cmay.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Virus.DeadCode.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Virus.Elerad.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Virus.Greenp.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Virus.Mocket.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Virus.Negt.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Trojan.CaddyWiper.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
Win32.Trojan.Dridex.yara | C:\Program Files\Magnet Forensics\Magnet AXIOM\YARA\ReversingLabs-2022... | 4/5/2023 12:02:59 PM
BACK
GO TO FIND MORE ARTIFACTS

Artifacts from RESPONSE Triage



Curating a Goodware & Malware Corpus

Malware Sources

- VX Underground
- Hybrid Analysis
- Malware Bazaar
- VirusShare
- The Zoo
- Recorded Future Triage

Registration may be required

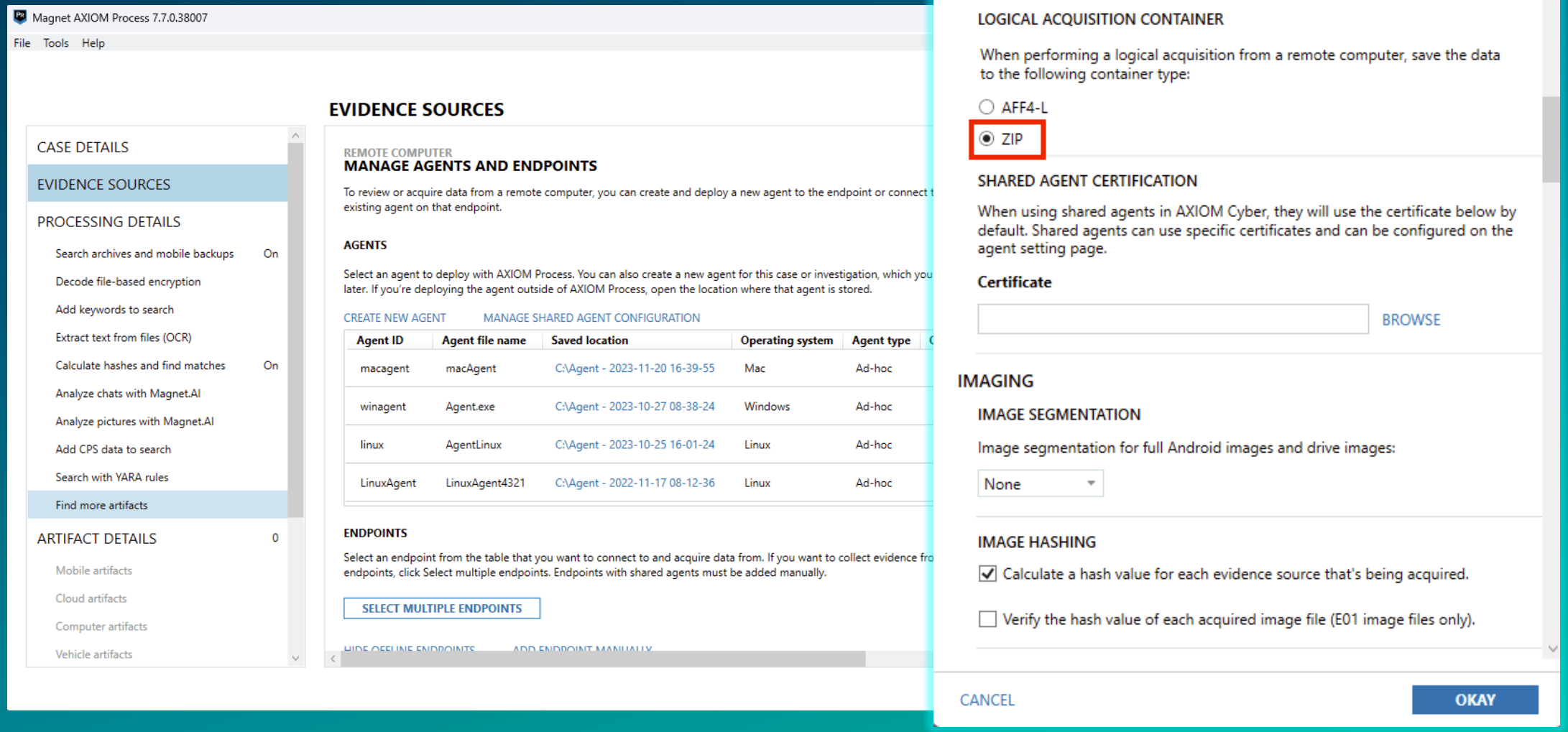
Goodware Sources



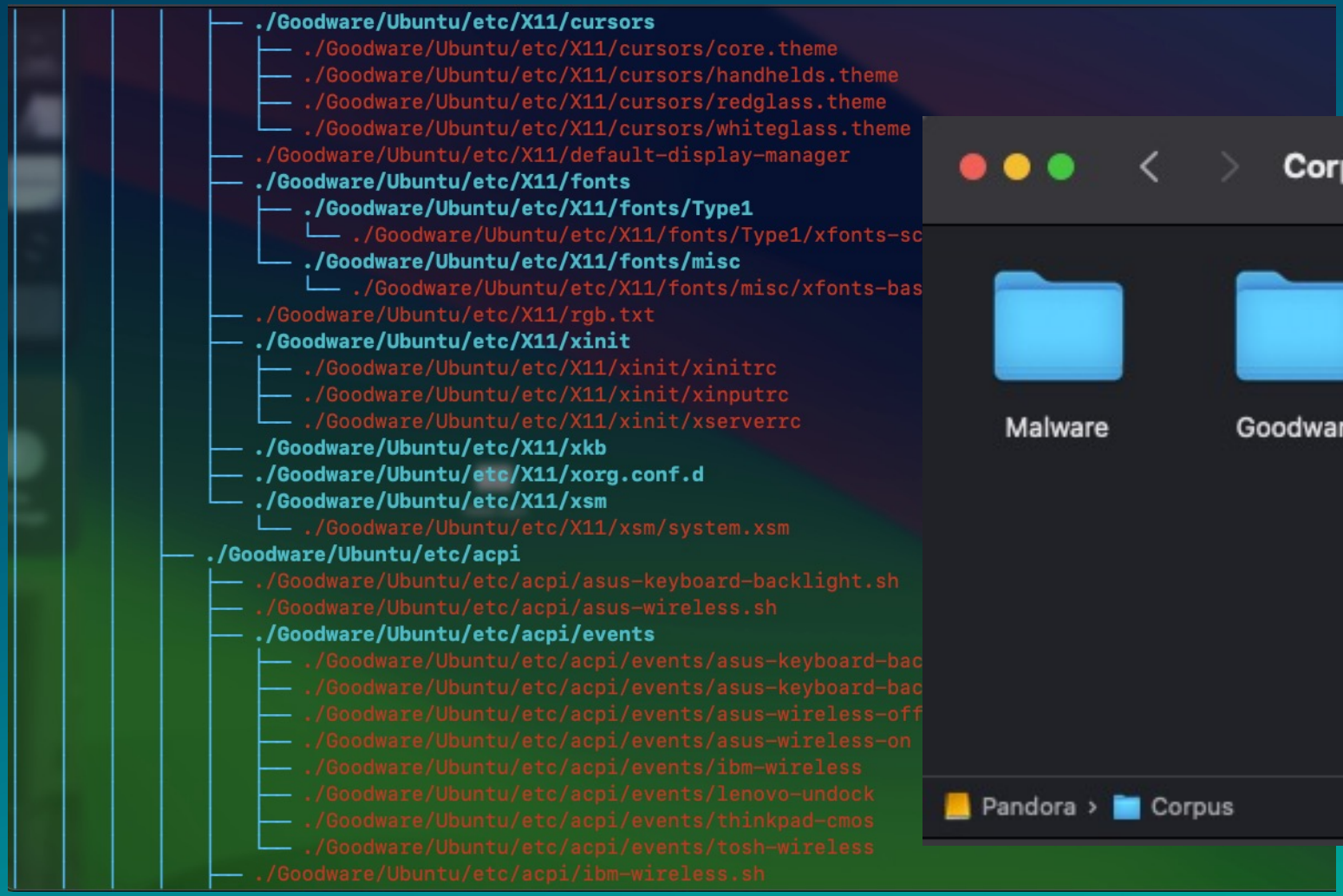


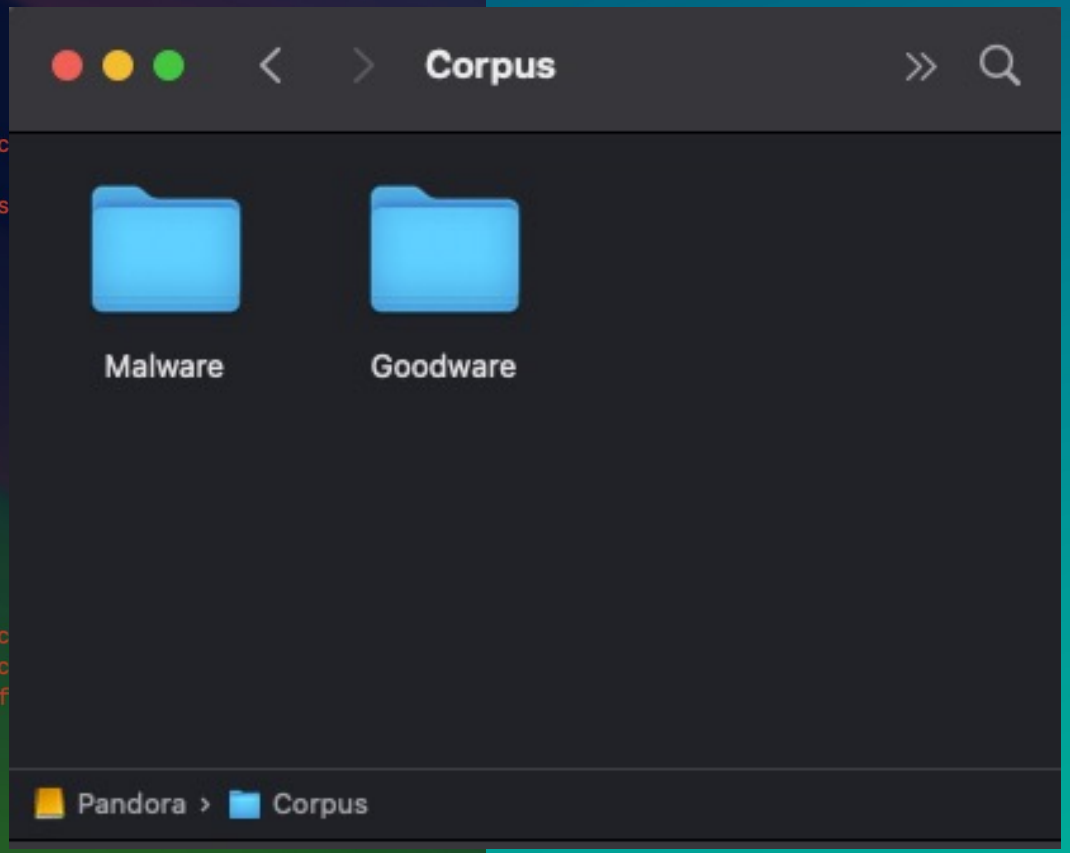

Sample files from trusted sources of benign files or applications.

Goodware Collection



Goodware & Malware Corpus





Resources

Auxtera Project https://theauxteraproject.com

Baker Street Forensics https://bakerstreetforensics.com

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

FLARE https://github.com/mandiant/flare-vm

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

Hybrid Analysis https://www.hybrid-analysis.com

IKEA Lack Table https://www.ikea.com/us/en/p/lack-side-table-black-brown-80104268/#content

Etl2pcapng https://github.com/microsoft/etl2pcapng

Inetsim https://www.inetsim.org

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

Magnet Forensics Free Tools (Magnet RESPONSE, DumpIt) http://magnetforensics.com/free-tools

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

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

Malware Bazaar https://bazaar.abuse.ch

Recorded Future Triage https://tria.ge

REMnux https://remnux.org

The Zoo https://thezoo.morirt.com

VirusShare https://virusshare.com

Virus Total https://www.virustotal.com

VMWare ESXi v8 https://customerconnect.vmware.com/en/evalcenter?p=free-esxi8

VMWare Remote Console (Mac) https://apps.apple.com/us/app/vmware-remote-console/

VX Underground https://www.vx-underground.org/malware.html

Windows 10/11 https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/

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~~