



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



MUS

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 Auxtera Project



BAKER STREET FORENSICS

D . F . I . R .



HTCIA

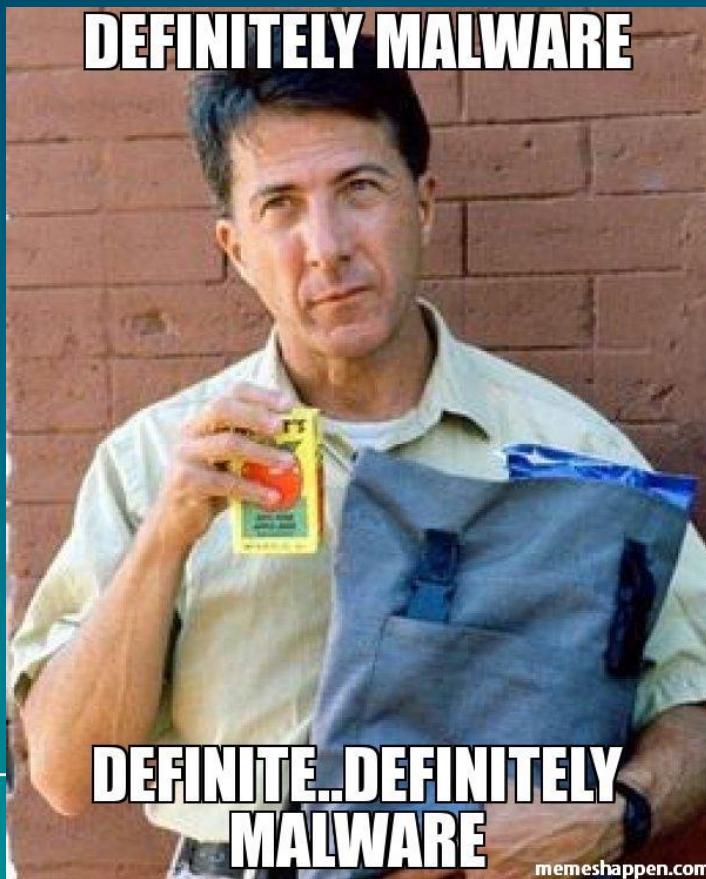
Delaware Valley - Philadelphia



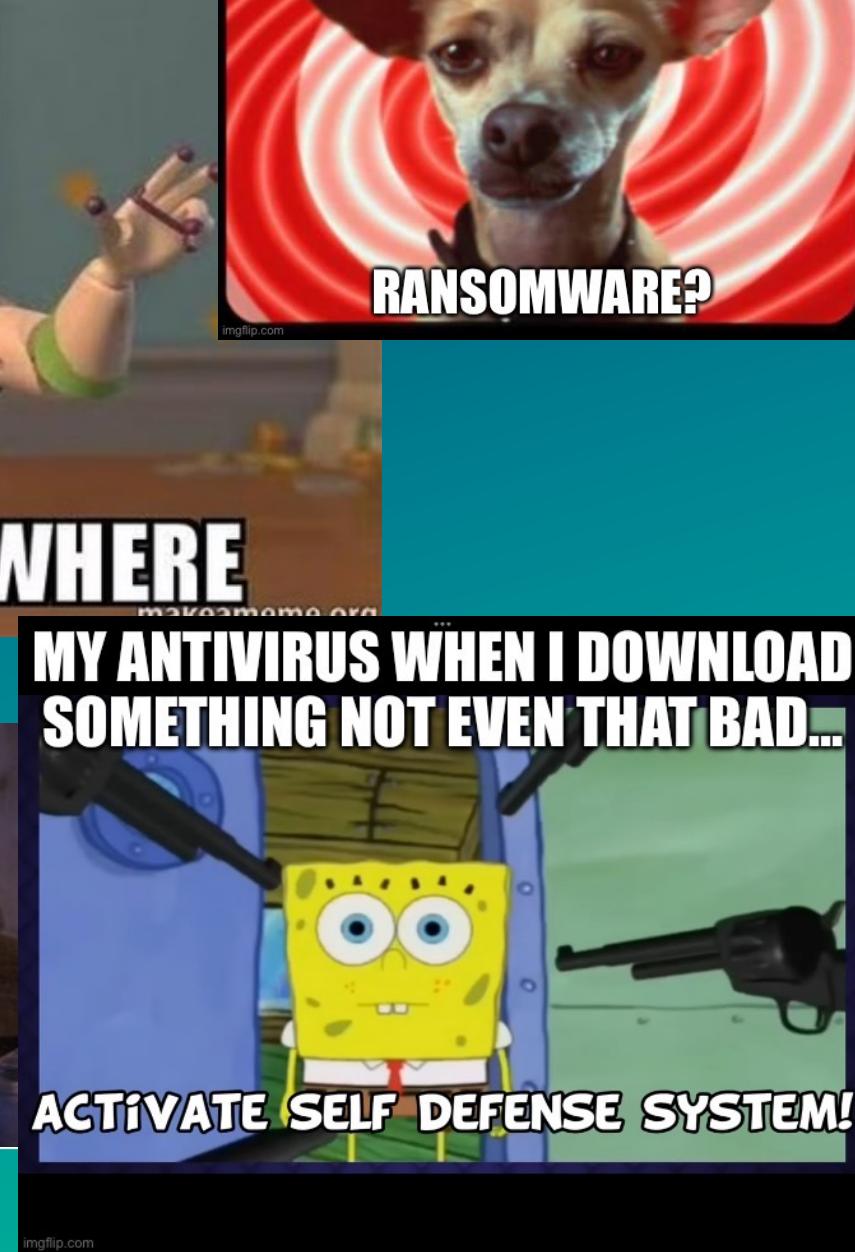
Abstract

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.



MAGNETUSERSUMMIT.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)



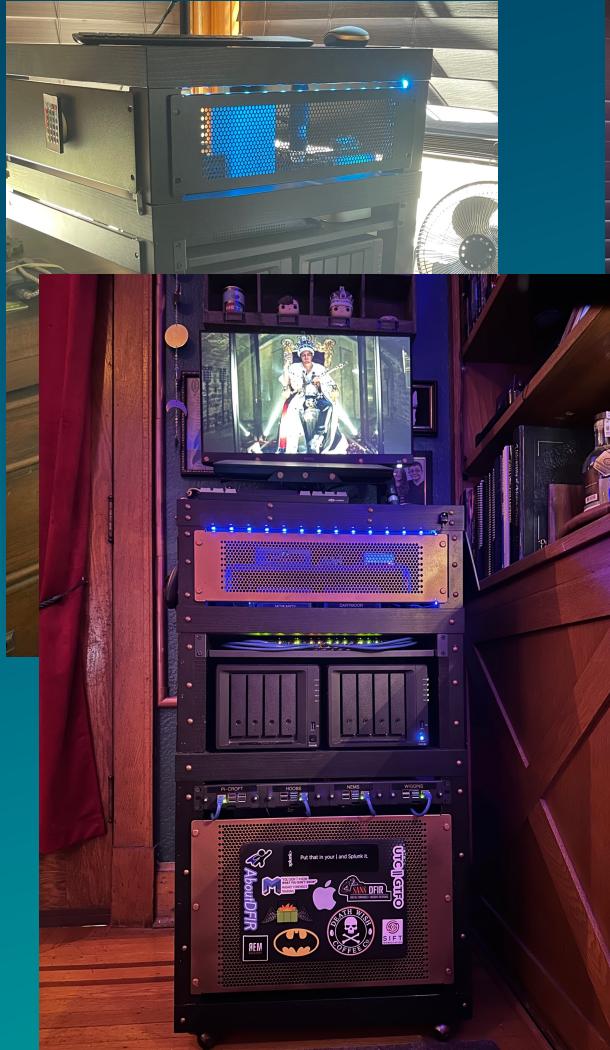
USB Network:	Amazon Basics USB 3.0 to 10/100/1000 Gigabit Ethernet Internet Adapter, Black
--------------	---



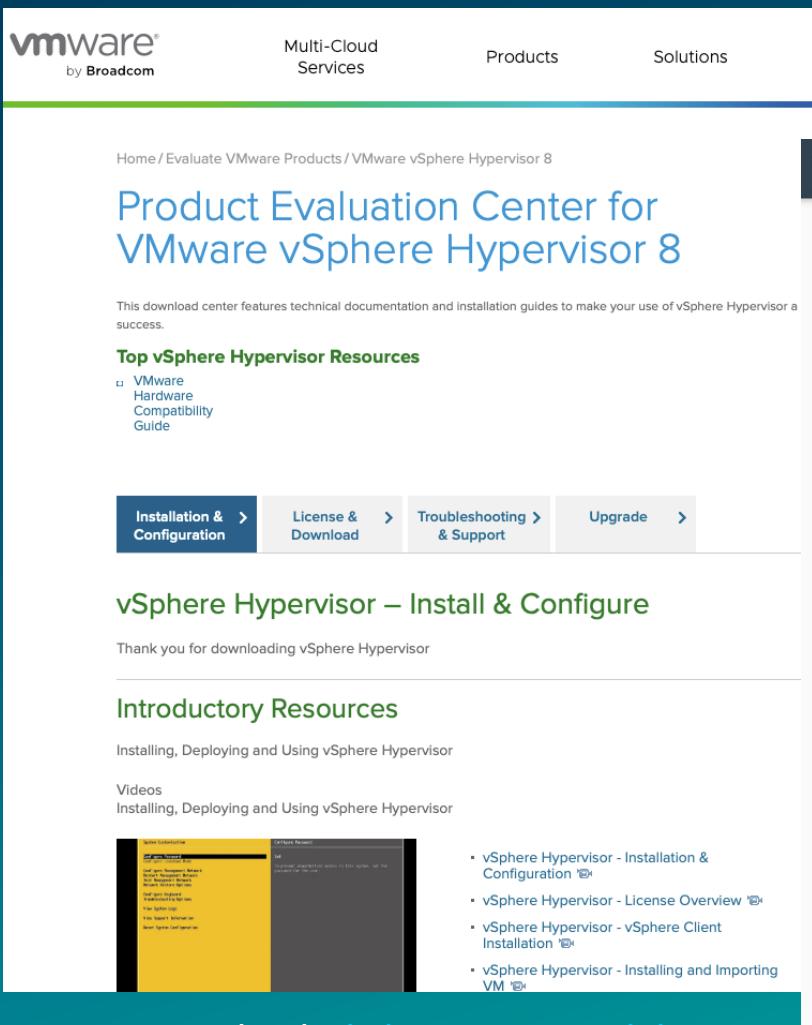
LTE Internet:	NETGEAR 4G LTE Broadband Modem (LM1200)
---------------	---

< \$4,000 USD

The Lack Rack



Platform: ESXi v8



This screenshot shows the VMware Product Evaluation Center for vSphere Hypervisor 8. It features a navigation bar with links for Multi-Cloud Services, Products, Solutions, Partners, Resources, and a search bar. A prominent "GET STARTED" button is also present. Below the navigation, a breadcrumb trail indicates the current page: Home / Evaluate VMware Products / VMware vSphere Hypervisor 8. The main content area is titled "Product Evaluation Center for VMware vSphere Hypervisor 8". It includes a section for "Top vSphere Hypervisor Resources" with links to VMware, Hardware Compatibility Guide, and compatibility matrices. Below this are tabs for "Installation & Configuration", "License & Download", "Troubleshooting & Support", and "Upgrade". A "vSphere Hypervisor – Install & Configure" section follows, containing introductory resources, videos, and a screenshot of the vSphere Hypervisor installation interface.

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

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

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 Downloads	Drivers & Tools	Open Source	Custom ISOs	OEM Addons																																	
<table border="1"> <thead> <tr> <th>Product</th> <th>Release Date</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Essentials</td> <td></td> <td></td> </tr> <tr> <td>VMware vSphere Hypervisor (ESXi) 8.0U2</td> <td>2023-09-21</td> <td>GO TO DOWNLOADS</td> </tr> <tr> <td>VMware vCenter Server 8.0U2a</td> <td>2023-10-26</td> <td>GO TO DOWNLOADS</td> </tr> <tr> <td>VMware NSX 4.1.2.1 For vShield Endpoint</td> <td>2023-11-07</td> <td>GO TO DOWNLOADS</td> </tr> <tr> <td>VMware Tools 12.3.5</td> <td>2023-10-26</td> <td>GO TO DOWNLOADS</td> </tr> <tr> <td>Essentials Plus</td> <td></td> <td></td> </tr> <tr> <td>VMware vSphere Hypervisor (ESXi) 8.0U2</td> <td>2023-09-21</td> <td>GO TO DOWNLOADS</td> </tr> <tr> <td>VMware vCenter Server 8.0U2a</td> <td>2023-10-26</td> <td>GO TO DOWNLOADS</td> </tr> <tr> <td>VMware vSphere Replication 8.8.0.2</td> <td>2023-11-21</td> <td>GO TO DOWNLOADS</td> </tr> <tr> <td>VMware NSX 4.1.2.1 For vShield Endpoint</td> <td>2023-11-07</td> <td>GO TO DOWNLOADS</td> </tr> </tbody> </table>					Product	Release Date	Action	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
Product	Release Date	Action																																			
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																																			

Product Resources

- [View My Download History](#)
- [Product Information](#)
- [Documentation](#)
- [vSphere Community](#)
- [Support Resources](#)
- [Download Free Trial](#)

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

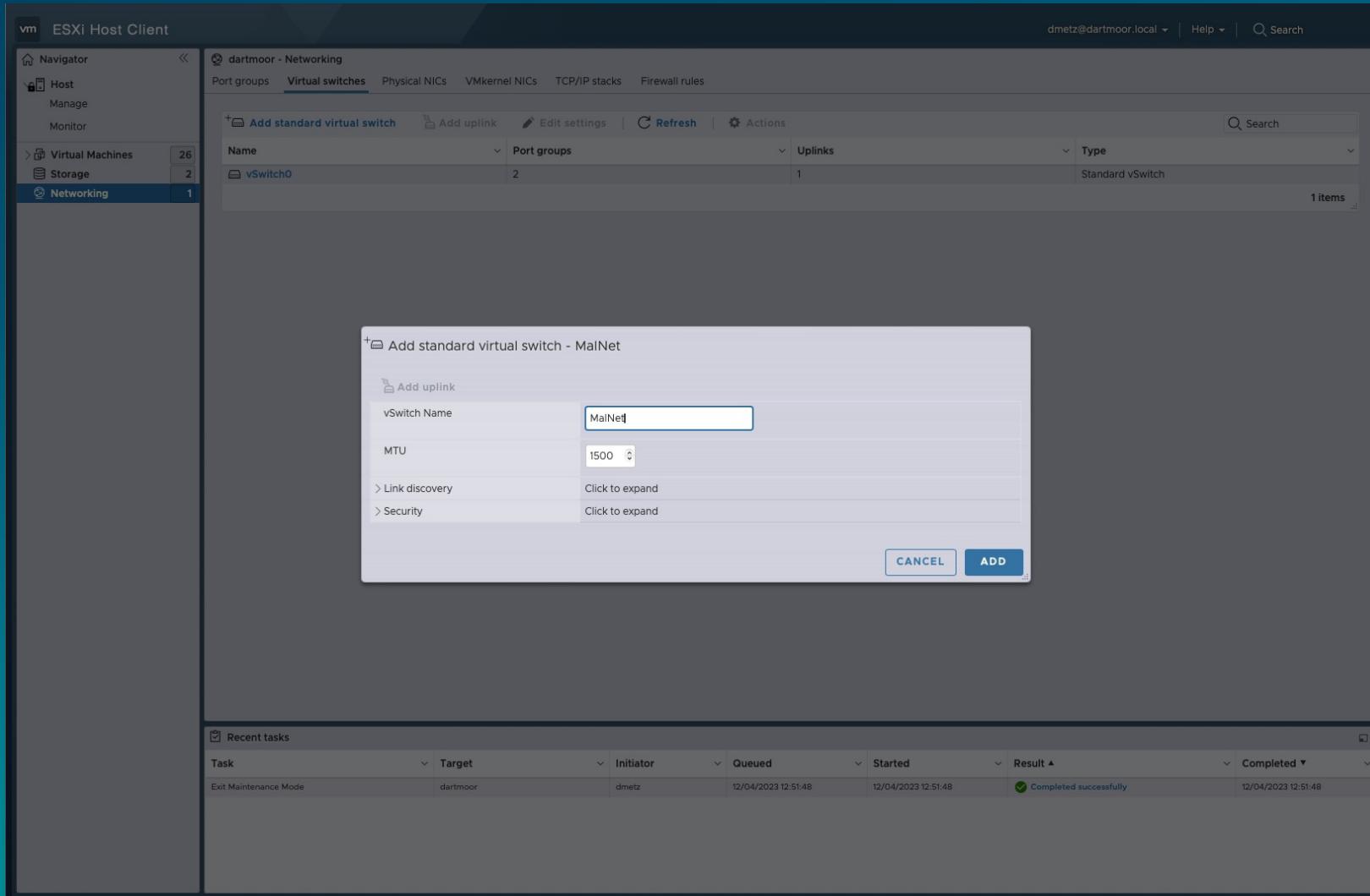


Windows10/11

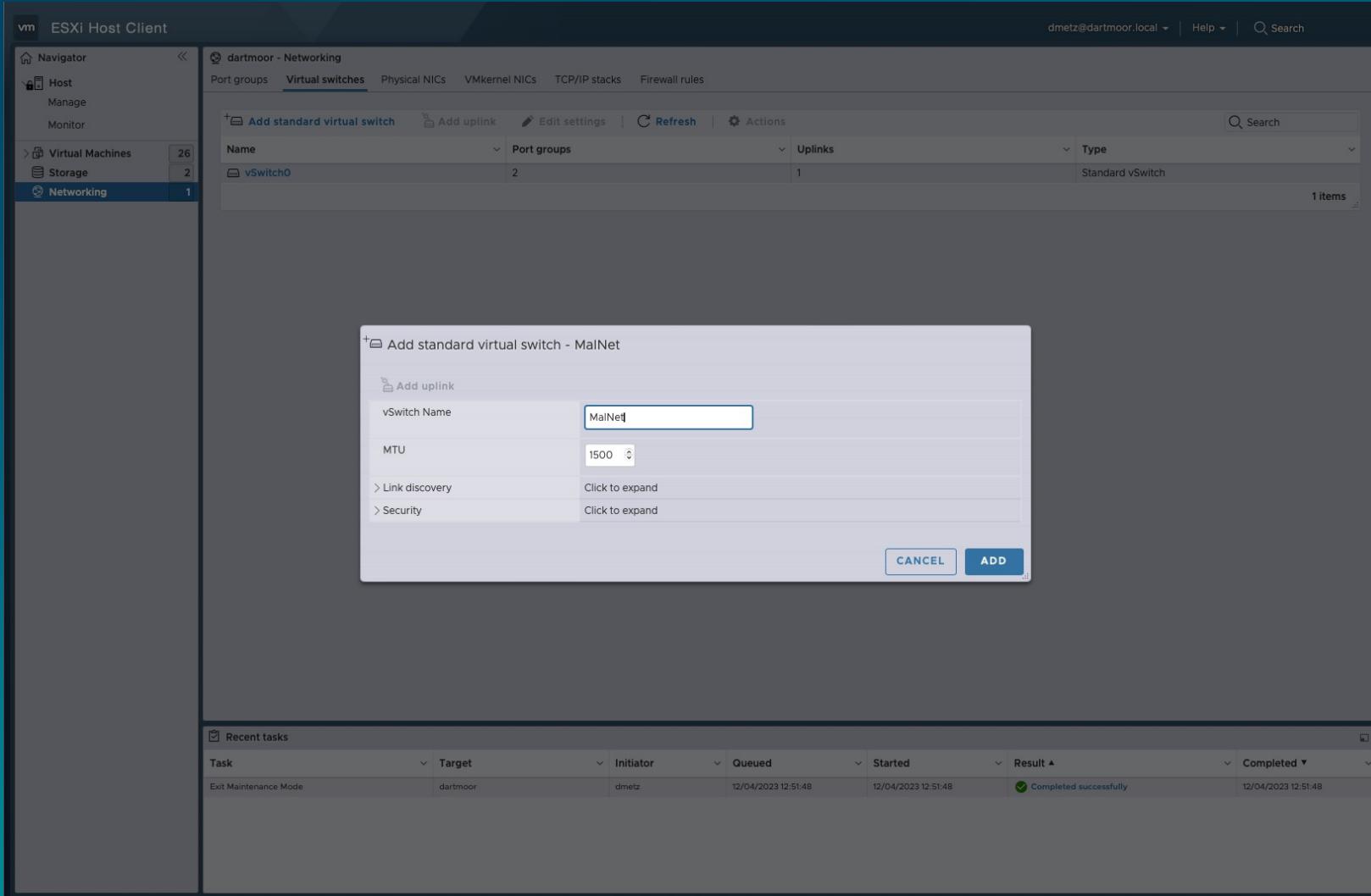


Creating the Malware Network

Add a virtual switch

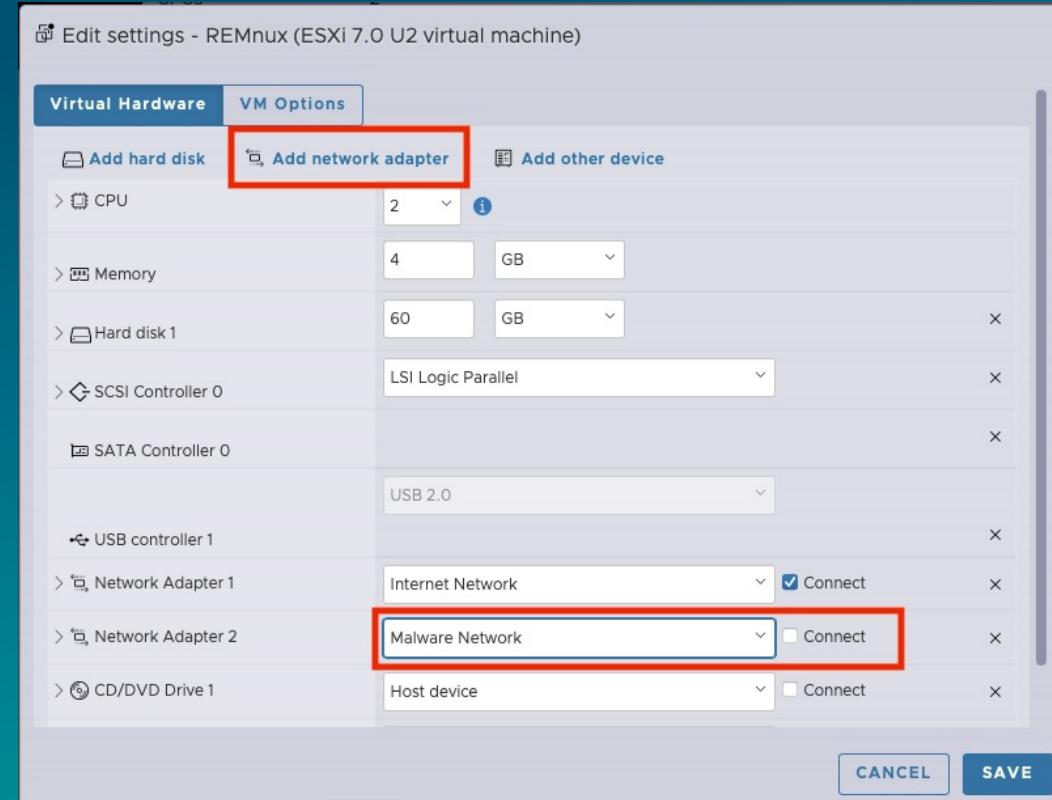


Add a port group



Add a Malware Network Adapter

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

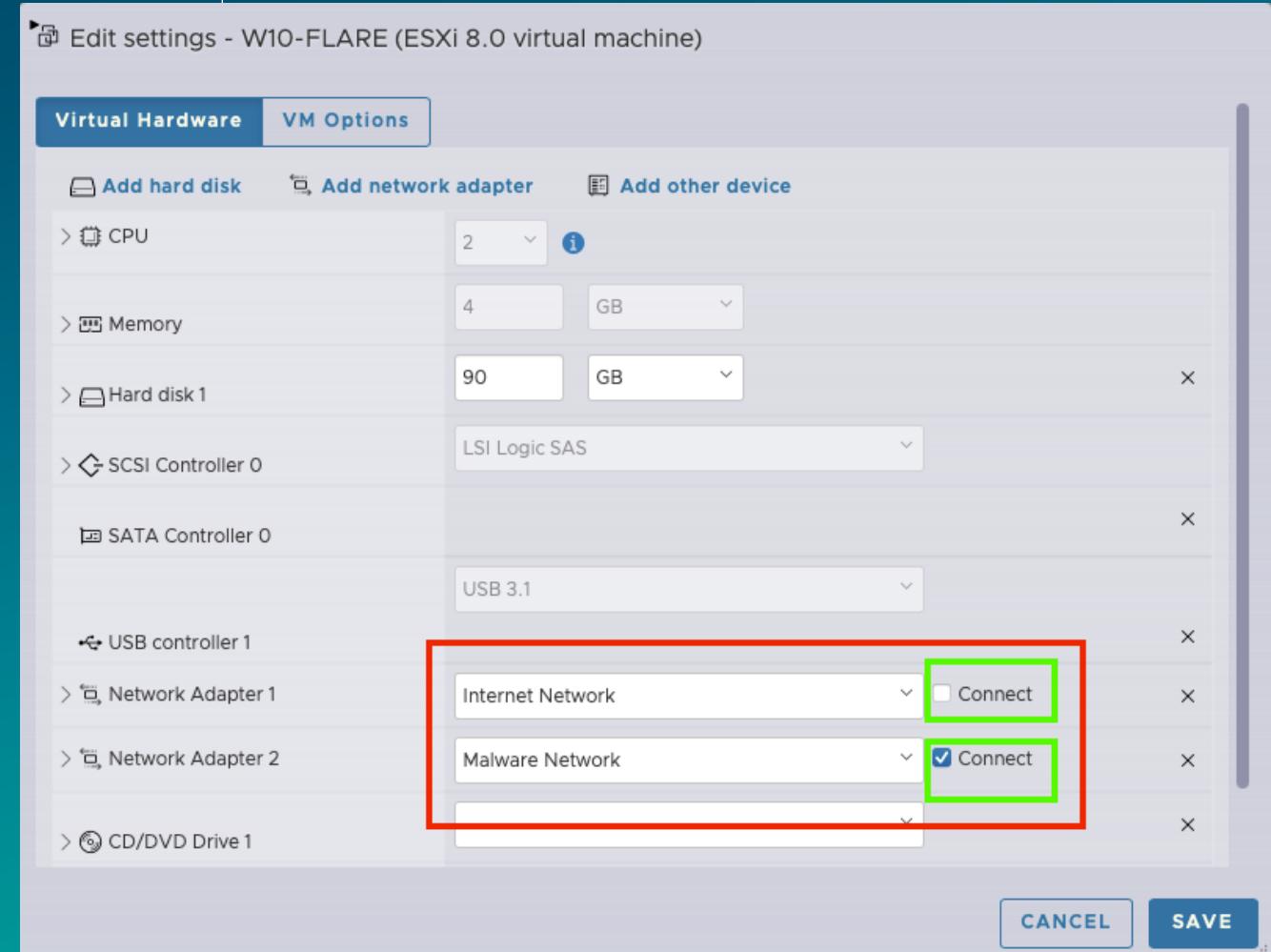


Primary Network - Malware Network - Internet

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>
```

```
remnux@remnux:~$ inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:     /var/lib/inetsim/
Using report directory:   /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 1691) ===
Session ID:      1691
Listening on:    255.255.0.0
Real Date/Time: 2023-12-04 14:09:55
Fake Date/Time: 2023-12-04 14:09:55 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 1695)
* ftp_21_tcp - started (PID 1702)
* ftpts_990_tcp - started (PID 1703)
* pop3s_995_tcp - started (PID 1701)
* smtp_25_tcp - started (PID 1698)
* smtpts_465_tcp - started (PID 1699)
* pop3_110_tcp - started (PID 1700)
* https_443_tcp - started (PID 1697)
* http_80_tcp - started (PID 1696)
done.
Simulation running.
```



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.
```

```
Ping statistics for 8.8.8.8:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

```
PS C:\Users\Admin> |
```

WARNING

THIS ZONE IS UNDER STRICT



QUARANTINE

INFECTIONOUS VIRUS AREA



BAKER STREET FORENSICS

Connecting the Malware Network to the Internet

D . F . I . N .

IRREGULARS ARE PART OF

LTE Hotspot & USB Network Adapter

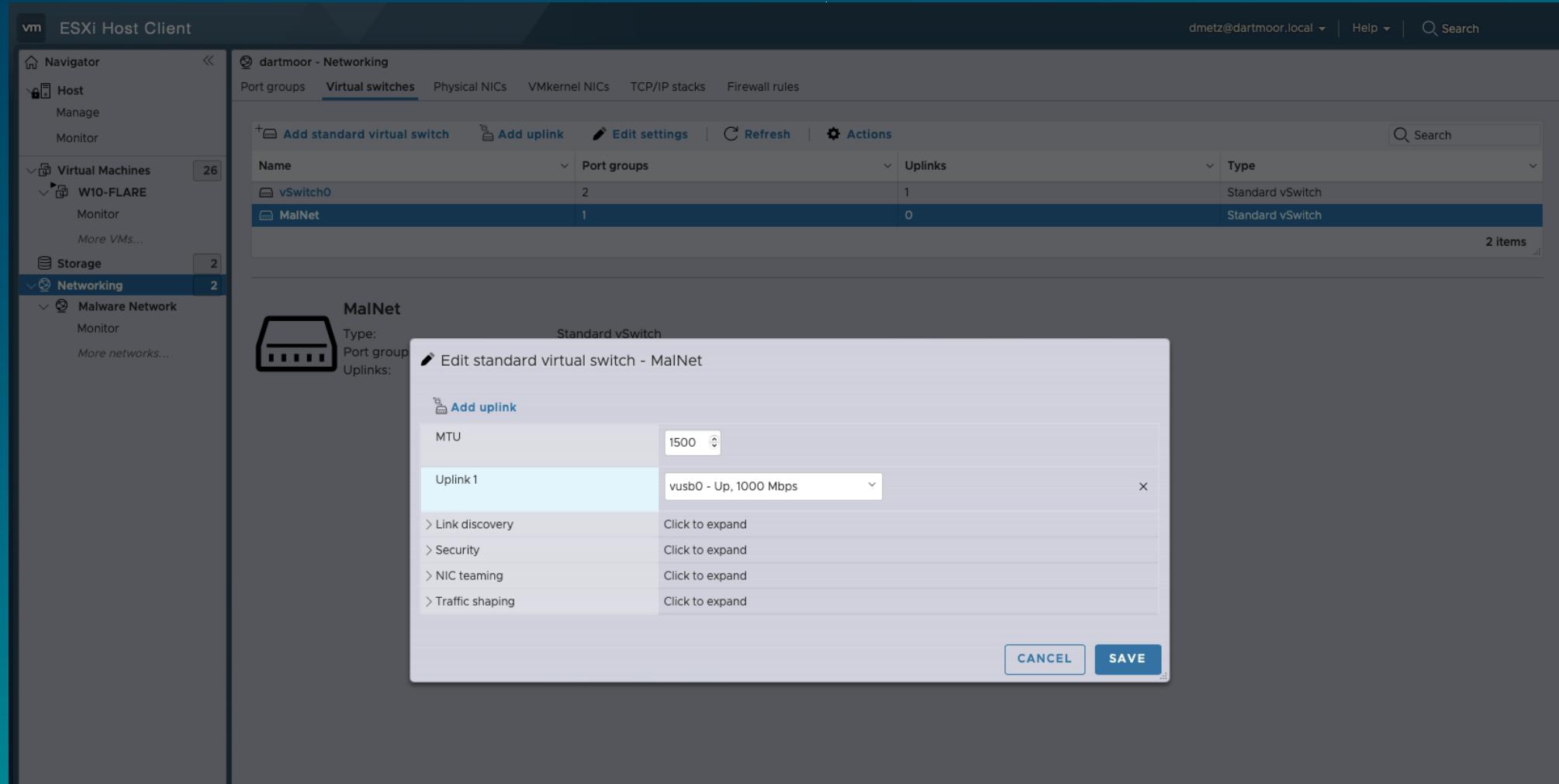
- Insert SIM card in hotspot
- Connect laptop to hotspot – verify connectivity; it's *easier to troubleshoot single connection.*
- Once LTE verified and distributing IP/Internet then connect to VMWare.
 - Attach USB adapter to NUC
 - Connect network cable from hotspot to USB adapter
 - "Hey Siri, turn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



The screenshot shows the vSphere interface under the 'Physical NICs' tab. It displays two network interfaces: 'vmnic0' and 'vusb0'. The 'vmnic0' row is grayed out, while 'vusb0' is selected, indicated by a blue background. The table columns include Name, Driver, MAC address, Auto-negotiate, and Link speed. The 'vusb0' row shows the driver 'ueether', MAC address 'a0:ce:c8:8d:0e:0e', Auto-negotiate as Enabled, and Link speed as 1000 Mbps, full duplex. A search bar and a '2 items' indicator are also visible.

Name	Driver	MAC address	Auto-negotiate	Link speed
vmnic0	cndi_igc	1c:69:7a:ae:d9:aa	Enabled	1000 Mbps, full duplex
vusb0	ueether	a0:ce:c8:8d:0e:0e	Enabled	1000 Mbps, full duplex

Virtual Switch – Add Uplink



Verify Uplink

ESXi Host Client

Navigator

- Host
- Manage
- Monitor
- Virtual Machines (26)
 - W10-FLARE (Monitor, More VMs...)
- Storage (2)
- Networking (2)
 - Malware Network (Monitor, More networks...)

Malware Network

Edit settings | Refresh | Actions

Malware Network

Accessible: Yes

Virtual machines: 3

Virtual switch: MailNet

VLAN ID: 0

Active ports: 3

vSwitch topology

Malware Network (VLAN ID: 0)
Virtual Machines (3): REMnux, W10-FLARE, WIN-RE-610
MAC Address 00:0c:29:4b:ce:75, MAC Address 00:0c:29:38:19:0a

Physical adapters: vusb0, 1000 Mbps, Full

Security policy

- Allow promiscuous mode: No
- Allow forged transmits: No
- Allow MAC changes: No

NIC teaming policy

- Notify switches: Yes
- Policy: Route based on originating port ID
- Reverse policy: Yes
- Fallback: Yes

Shaping policy

- Enabled: No

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

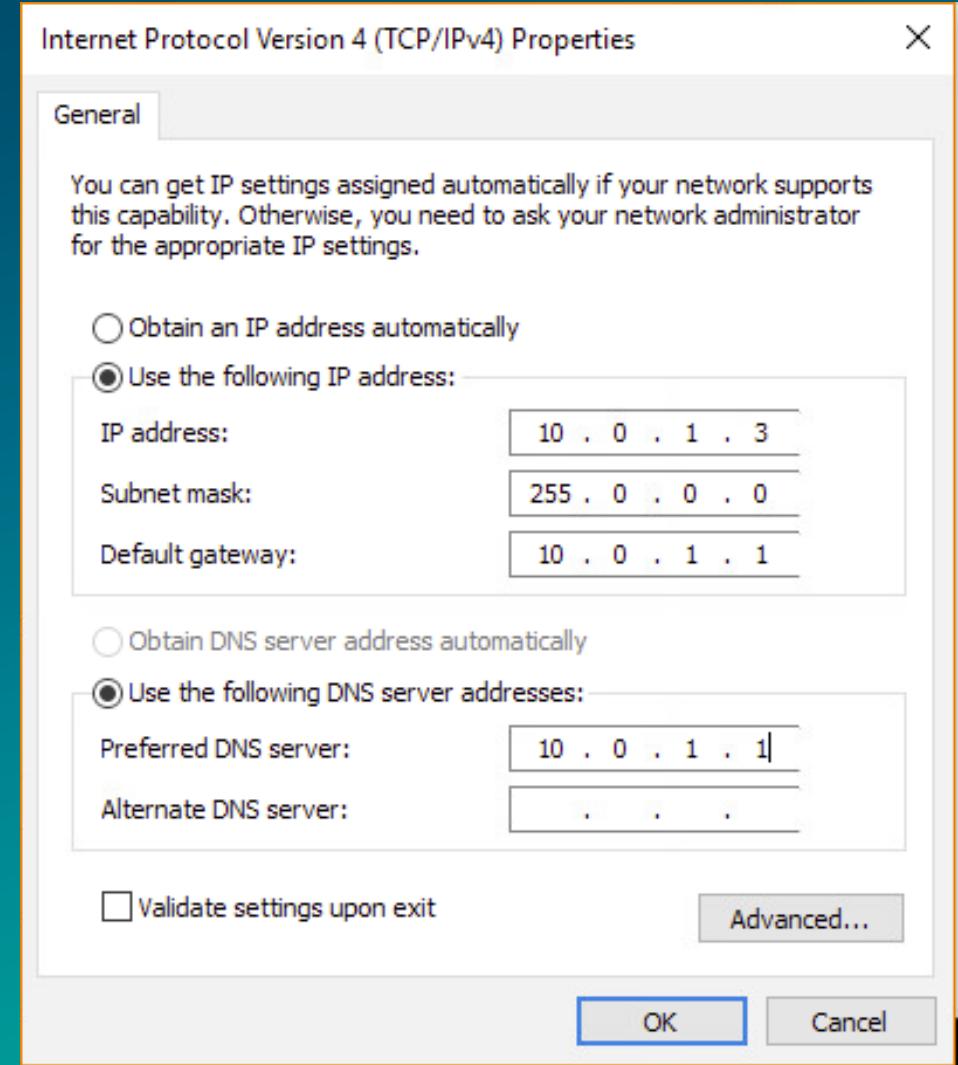
Pinging www.google.com [2607:f8b0:4006:821::2004] with 32 bytes of data:
Reply from 2607:f8b0:4006:821::2004: time=51ms
Reply from 2607:f8b0:4006:821::2004: time=55ms
Reply from 2607:f8b0:4006:821::2004: time=49ms

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 off hotspot
- Inetsim (optional)

Primary Network - Malware Network - Internet



```
.':::::cccccc:;.
.:cccclllooooddxo.          .';clooddooolcc:;;;;.
.:cccllloooodxo.          .:coxxxxxdl:,'.
'ccccclllooooddd'          .,,lxkxxxo:'.
'ccccclllooooddd'          .,:lxOkL,:oxo..
':ccccclllooooddo.        .:dk0000kkd;''.
.:ccccclllooooddo.  ...;lxk00000kkkd;
.:ccccclllooooddc:coxkkkk000000x:.
'cccccllloooodddxxxxxkkk0000x:.
'.ccccllloooodddxxxxxkkkxlc..
':llllooooodddxxxxxoc;.
.'';:clooddddolc:...
.....
```

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=; BitDefender=; NANO-Antivirus=; SUPERAntiSpyware=; Avast=; Tencent=; TACHYON=;
Emsisoft=; DrWeb=; F-Secure=; DECTECH=; VIPRE=; TrendMicro=; McAfee=; CM-Security=; TrendMicro-FAT=; F-Secure-Sophos=
Ikarus=; Jiang=; ZoneAlarm=; G DATA=; TrendMicro-hou=; Emsisoft-Eraser=; Emsisoft-AntiR=; Emsisoft-Arcabit=; ViRobot=;
ZoneAlarm=; Zoner=; ZoneAlarm=; DeepInstinct=}
```

VirusTotal Queries with PowerShell

```
scan_id : 52d3dd78d3f1a14e18d0689ed8c5b43372f9e76401ef1ff68522575e6251d2cf
sha1 : 704b84d525eefca6fa7eeb1cf8c94f861310c224
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.*

Recycle Bin API Monitor Network Scylla x32
x64 Connections



Capture. Detonate. Collect.

version 1.2 | @dwmetz | ©2023 bakerstreetforensics.com

Process Hacker Cutter ProcDOT x64dbg

Collection directory E:\Collections\WIN-RE-610-202308151019

Initiating Process Monitor

Initiating PCAP collection
Monitor

LEARN
REM

Capturing Malware Evidence with detonaRE

detonaRE – from Latin-ish, *to detonate*

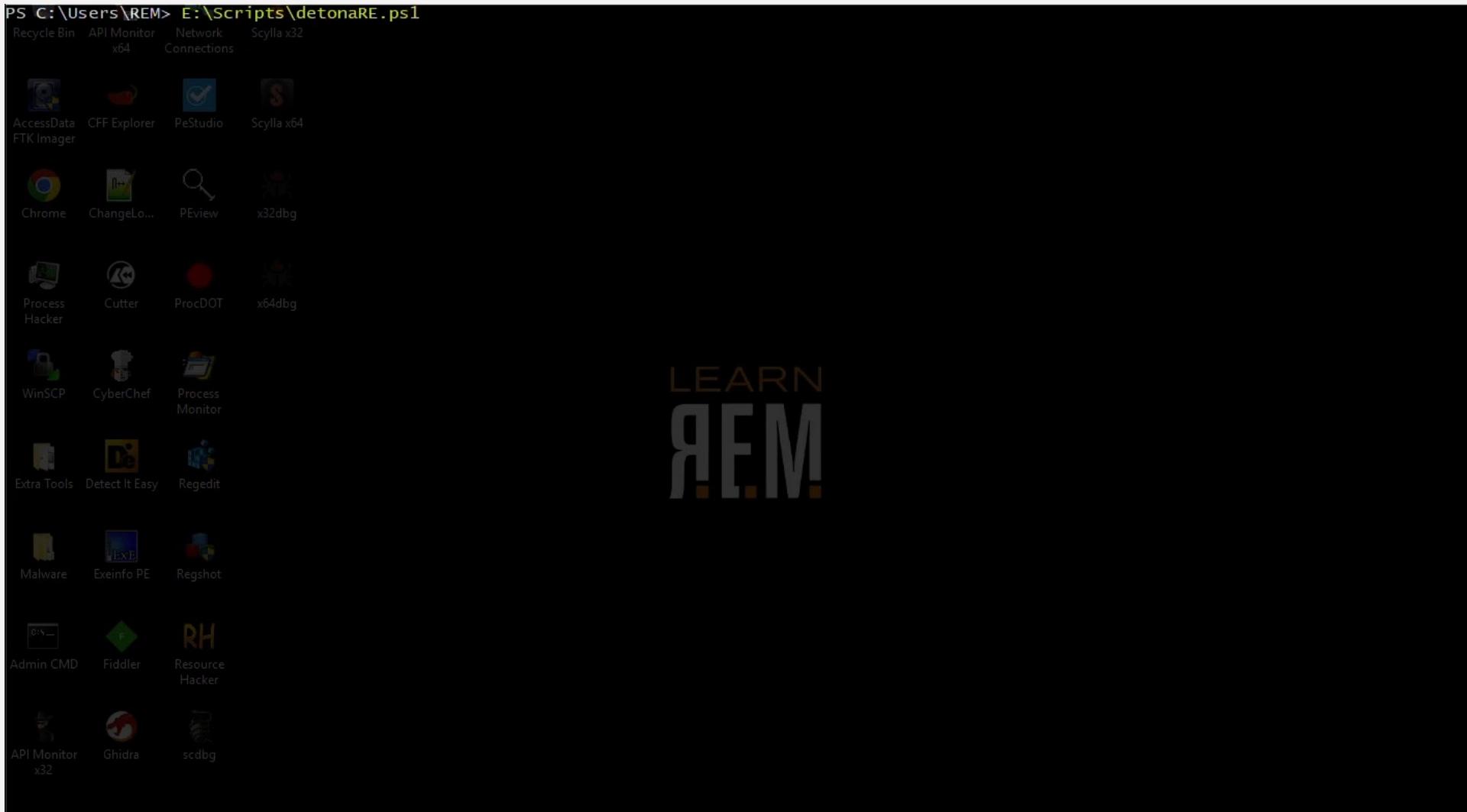
- initiates packet capture
- launches malware sample
- terminates packet capture after specified time interval
- initiates evidence collection with **Magnet RESPONSE** (Memory, Process, and Triage capture) *
- converts collected .etl file (network capture) to .pcap with **etl2pcapng**.
 - Alternate: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

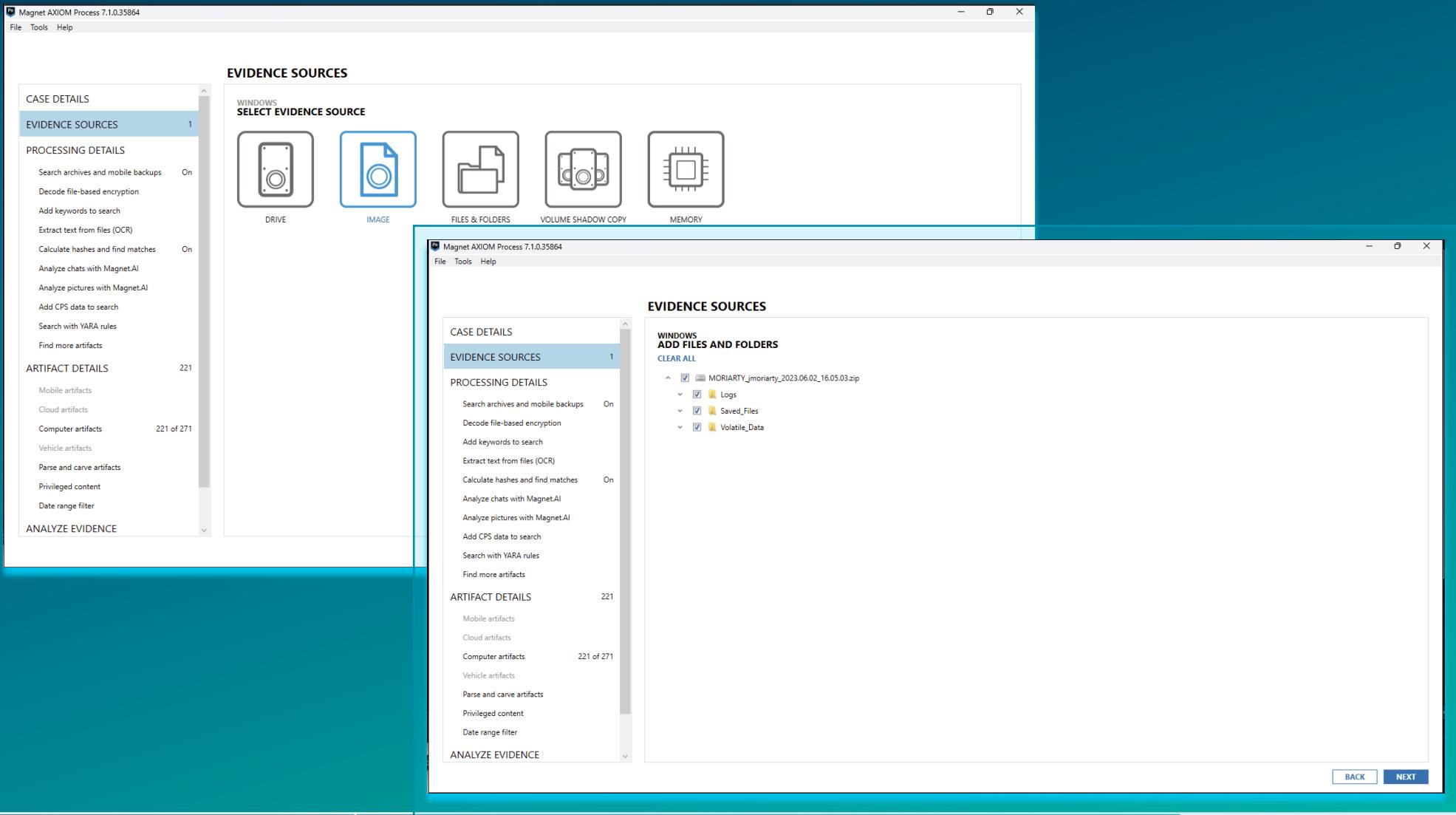
The screenshot displays two windows of the Magnet AXIOM Process software interface:

- Top Window (Version 5.2.0.25407):** Shows the "EVIDENCE SOURCES" screen. On the left, under "CASE DETAILS", "EVIDENCE SOURCES" is selected. Under "PROCESSING DETAILS", "Search archives and mobile backups" and "Calculate hash values" are set to "On". Under "ARTIFACT DETAILS", there are 0 artifacts. On the right, the "SELECT EVIDENCE SOURCE" panel shows icons for DRIVE, IMAGE, FILES & FOLDERS, VOLUME SHADOW COPY, and MEMORY. The MEMORY icon is highlighted.
- Bottom Window (Version 7.1.0.35864):** Shows the "SELECT MEMORY PLUG-IN" screen. It has a similar layout with "CASE DETAILS", "EVIDENCE SOURCES" selected, and "PROCESSING DETAILS" showing various options like "Search archives and mobile backups" and "Calculate hashes and find matches". The "ARTIFACT DETAILS" section shows 0 artifacts. On the right, the "SELECT MEMORY PLUG-IN" panel lists "COMAE" and "VOLATILITY" as available plug-ins. At the bottom right are "BACK" and "NEXT" buttons.

Computer > Windows > Load Evidence > Memory

Triage Processing

Computer > Windows > Load Evidence > IMAGE



MUS YARA

Magnet AXIOM Process 7.1.0.35864

File Tools Help

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
- 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

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 folders. [EDIT](#)

Search by name or source path...

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

Rules selected: 4

[BACK](#) [GO TO FIND MORE ARTIFACTS](#)



Artifacts from RESPONSE Triage

The screenshot displays the Magnet AXIOM Examine software interface, specifically the Magnet RESPONSE Demo version. The window is titled "Magnet AXIOM Examine v7.1.0.35864 - Magnet RESPONSE Demo".

CASE OVERVIEW

- EVIDENCE SOURCES:** RAMDump-MORIARTY-20230602-160503..., RAMDump-MORIARTY-20230602-160503..., MORIARTY_jmoriarty_2023.06.02_16.05.03.zip
- INSIGHTS:** Potential Cloud Evidence Leads 0

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 AXIOMEexamine.log file contains information about any errors encountered, jobs that were run, and general debugging information. [OPEN LOG FILE](#).

EVIDENCE OVERVIEW

EVIDENCE NUMBER: RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.dmp (26,857)

EVIDENCE SOURCE: RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.dmp

LOCATION: RAMDump-MORIARTY-20230602-160503-WinVer10.0.22621.1702.dmp

PLATFORM: Computer

PROCESS METHOD: Parsing and carving

ARTIFACT CATEGORIES

Evidence source: All

Number of artifacts: 2,730,158

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

PLACES TO START

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://magneteidealab.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



Curating a Goodware & Malware Corpus

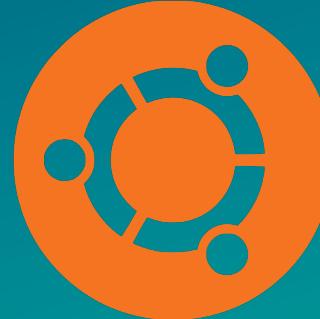
Malware Sources

- 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

Magnet AXIOM Process 7.7.0.38007

File Tools Help

EVIDENCE SOURCES

REMOTE COMPUTER
MANAGE AGENTS AND ENDPOINTS

To review or acquire data from a remote computer, you can create and deploy a new agent to the endpoint or connect to an existing agent on that endpoint.

AGENTS

Select an agent to deploy with AXIOM Process. You can also create a new agent for this case or investigation, which you can later use. If you're deploying the agent outside of AXIOM Process, open the location where that agent is stored.

CREATE NEW AGENT		MANAGE SHARED AGENT CONFIGURATION		
Agent ID	Agent file name	Saved location	Operating system	Agent type
macagent	macAgent	C:\Agent - 2023-11-20 16-39-55	Mac	Ad-hoc
winagent	Agent.exe	C:\Agent - 2023-10-27 08-38-24	Windows	Ad-hoc
linux	AgentLinux	C:\Agent - 2023-10-25 16-01-24	Linux	Ad-hoc
LinuxAgent	LinuxAgent4321	C:\Agent - 2022-11-17 08-12-36	Linux	Ad-hoc

ENDPOINTS

Select an endpoint from the table that you want to connect to and acquire data from. If you want to collect evidence from multiple endpoints, click Select multiple endpoints. Endpoints with shared agents must be added manually.

SELECT MULTIPLE ENDPOINTS

HIDE OFFLINE ENDPOINTS **ADD ENDPOINT MANUALLY**

Settings

LOGICAL ACQUISITION CONTAINER

When performing a logical acquisition from a remote computer, save the data to the following container type:

AFF4-L
 ZIP

SHARED AGENT CERTIFICATION

When using shared agents in AXIOM Cyber, they will use the certificate below by default. Shared agents can use specific certificates and can be configured on the agent setting page.

Certificate

BROWSE

IMAGING

IMAGE SEGMENTATION

Image segmentation for full Android images and drive images:

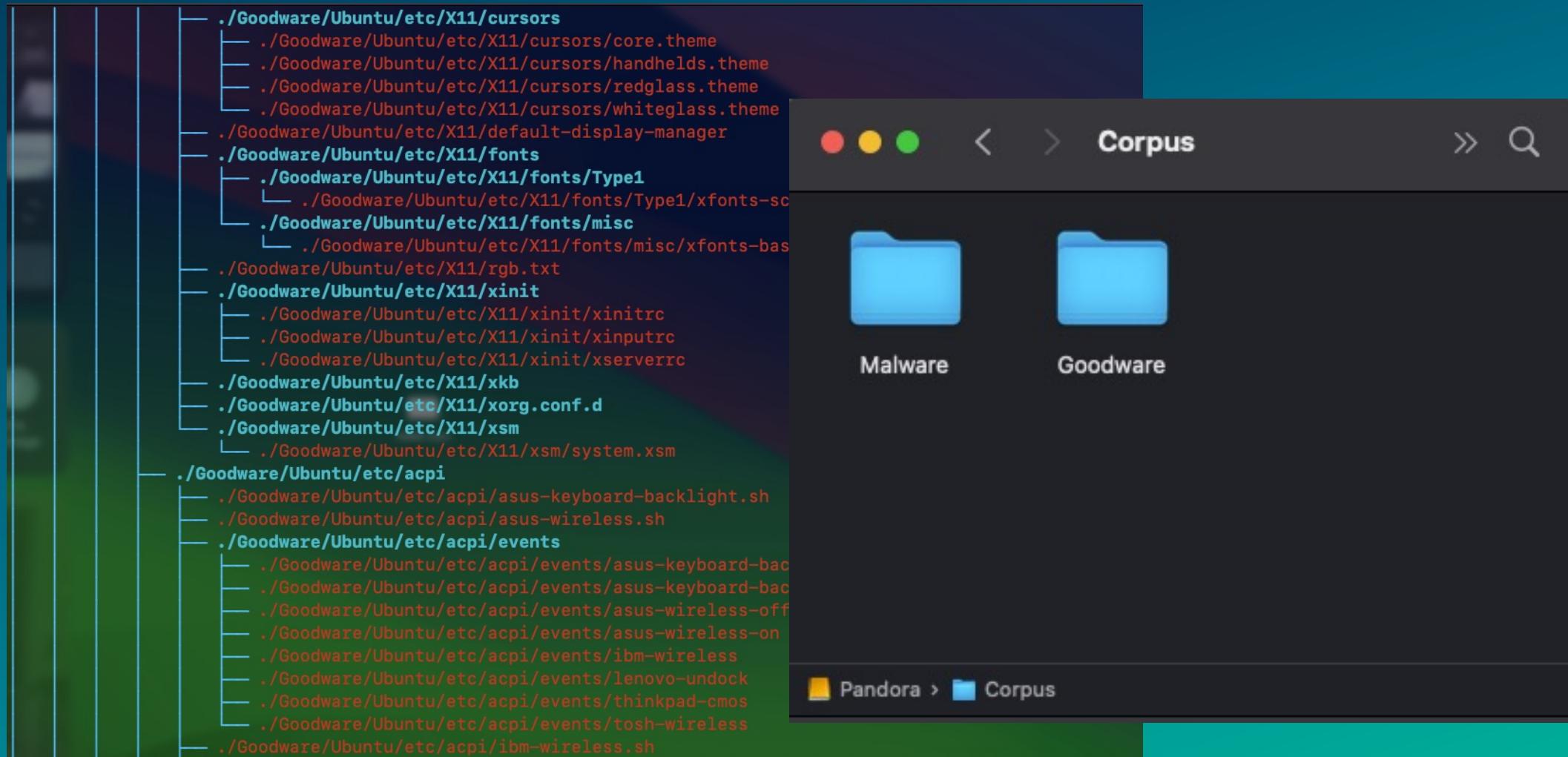
None

IMAGE HASHING

Calculate a hash value for each evidence source that's being acquired.
 Verify the hash value of each acquired image file (E01 image files only).

CANCEL **OKAY**

Goodware & Malware Corpus



Honey, I Ransomwared the Kids

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://triage>

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-](https://www.vx-underground.org/malware.html)

[underground.org/malware.html](https://www.vx-underground.org/malware.html)

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

[us/windows/downloads/virtual-machines/](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

