Dive Into WDAG

Yunhai Zhang

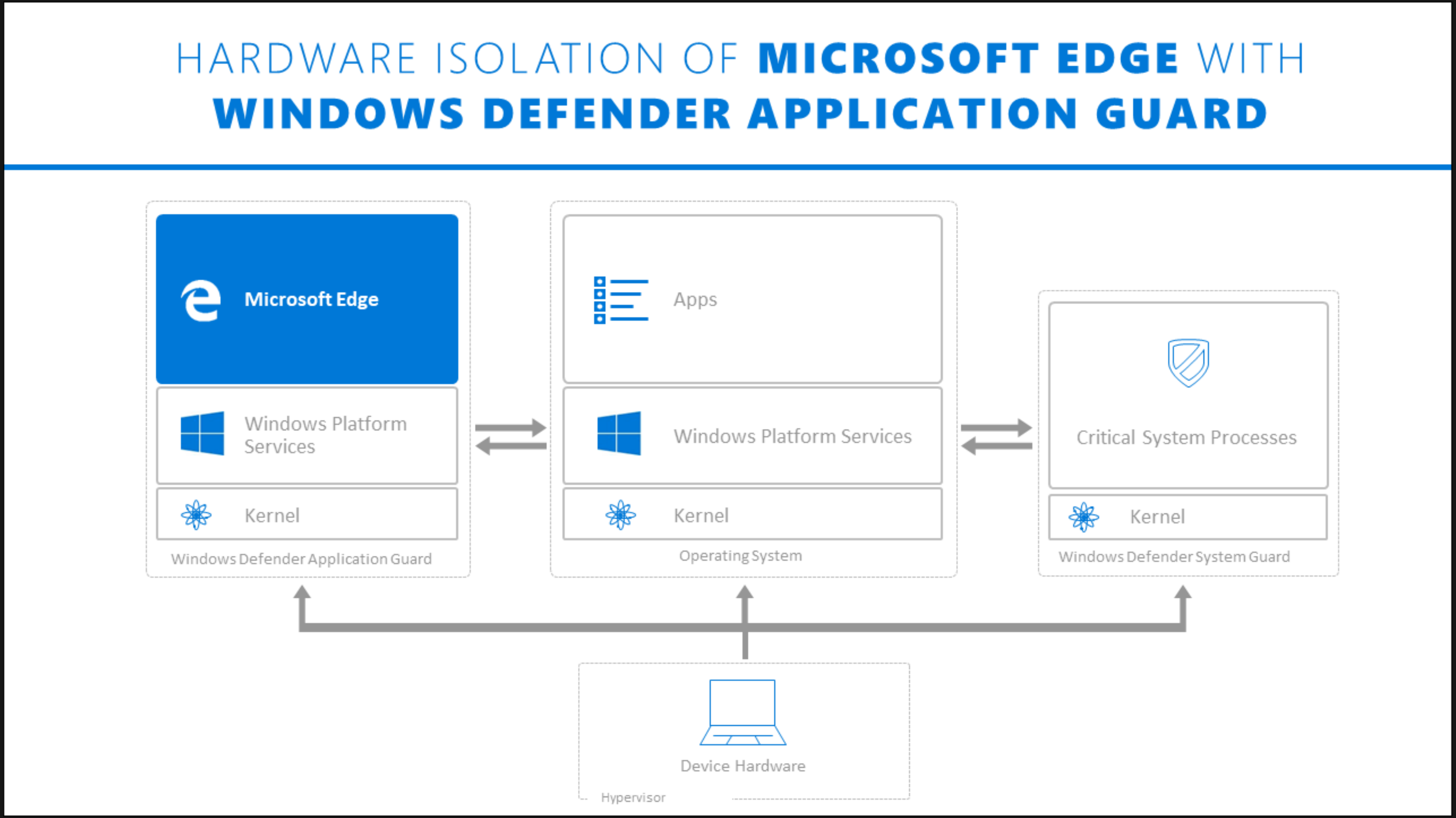
Who am I

- Yunhai Zhang
- Twitter: @_f0rgetting_
- Researcher of NSFOCUS
- Winner of Mitigation Bypass Bounty: 2014 ~ 2018

What is WDAG

- Windows Defender Application Guard
  - A security feature of Windows 10
  - Hardware isolation based on virtualization technology
  - Separate untrusted content from the host operating system
  - Keep the host safe and remove potential malware

What is WDAG

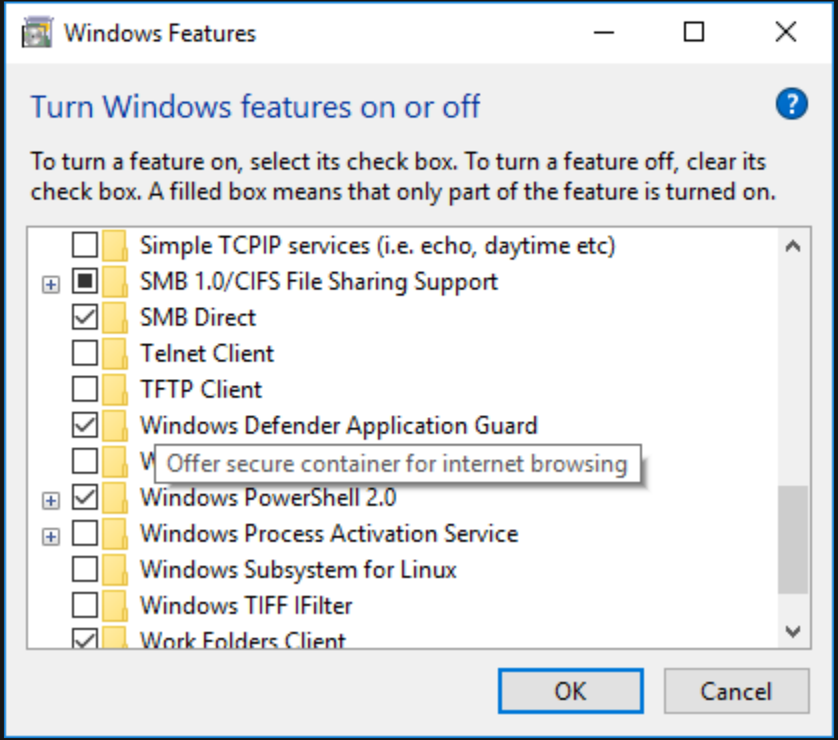


HARDWARE ISOLATION OF **MICROSOFT EDGE** WITH **WINDOWS DEFENDER APPLICATION GUARD**

Microsoft Edge
Windows Platform Services
Kernel
Windows Defender Application Guard
Apps
Windows Platform Services
Kernel
Operating System
Critical System Processes
Kernel
Windows Defender System Guard
Device Hardware
Hypervisor

How to use WDAG

- WDAG is not installed by default
  - System Requirement
    - Support SLAT and VT-x or AMD-V
    - More than 4 CPU cores
    - More than 8GB memory
    - More than 5GB disk space



Windows Features

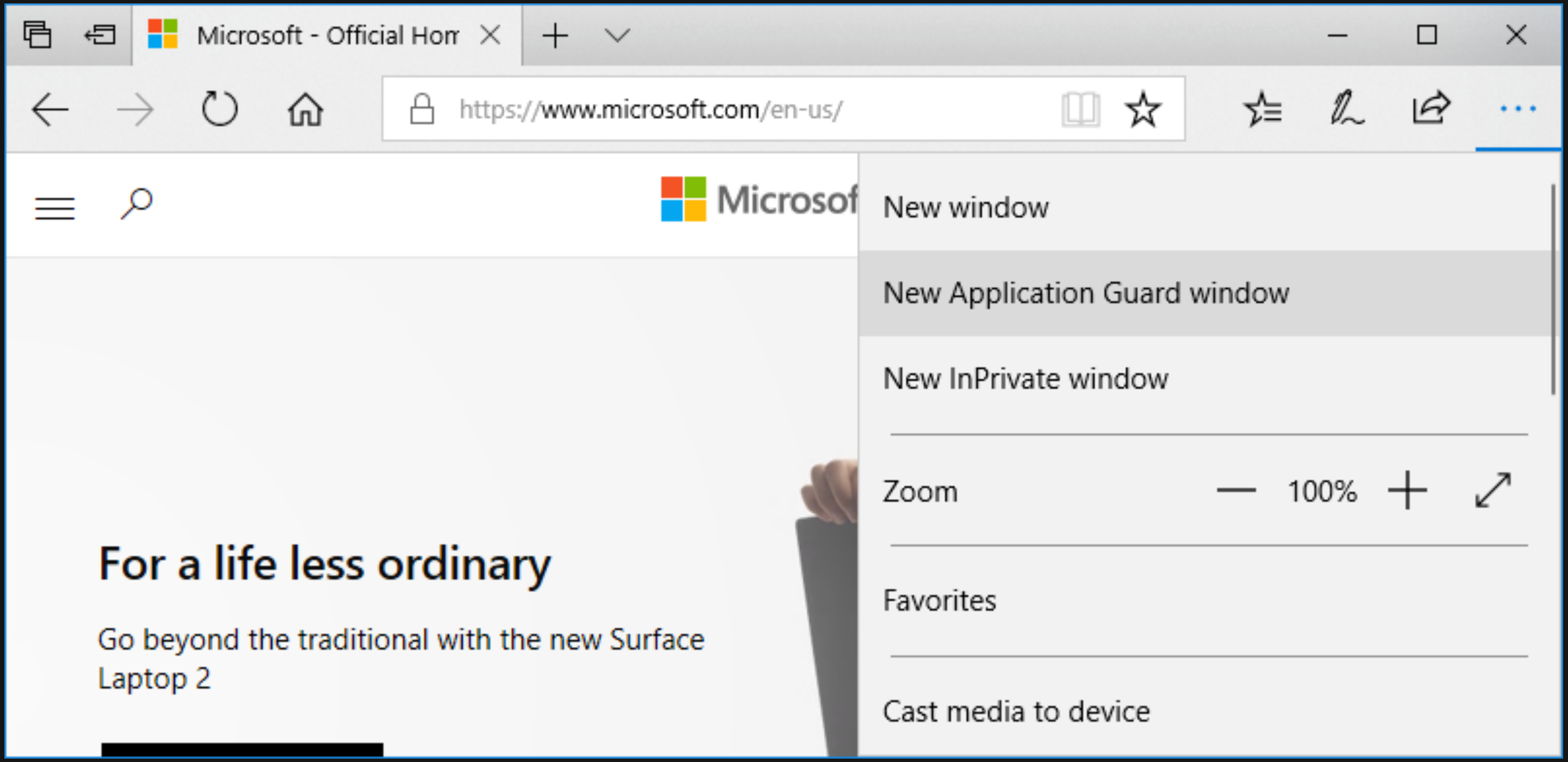
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- □ Simple TCPIP services (i.e. echo, daytime etc)
- ■ SMB 1.0/CIFS File Sharing Support
- ☑ SMB Direct
- □ Telnet Client
- □ TFTP Client
- ☑ Windows Defender Application Guard
- □ W Offer secure container for internet browsing
- ☑ Windows PowerShell 2.0
- □ Windows Process Activation Service
- □ Windows Subsystem for Linux
- □ Windows TIFF IFilter
- ☑ Work Folders Client

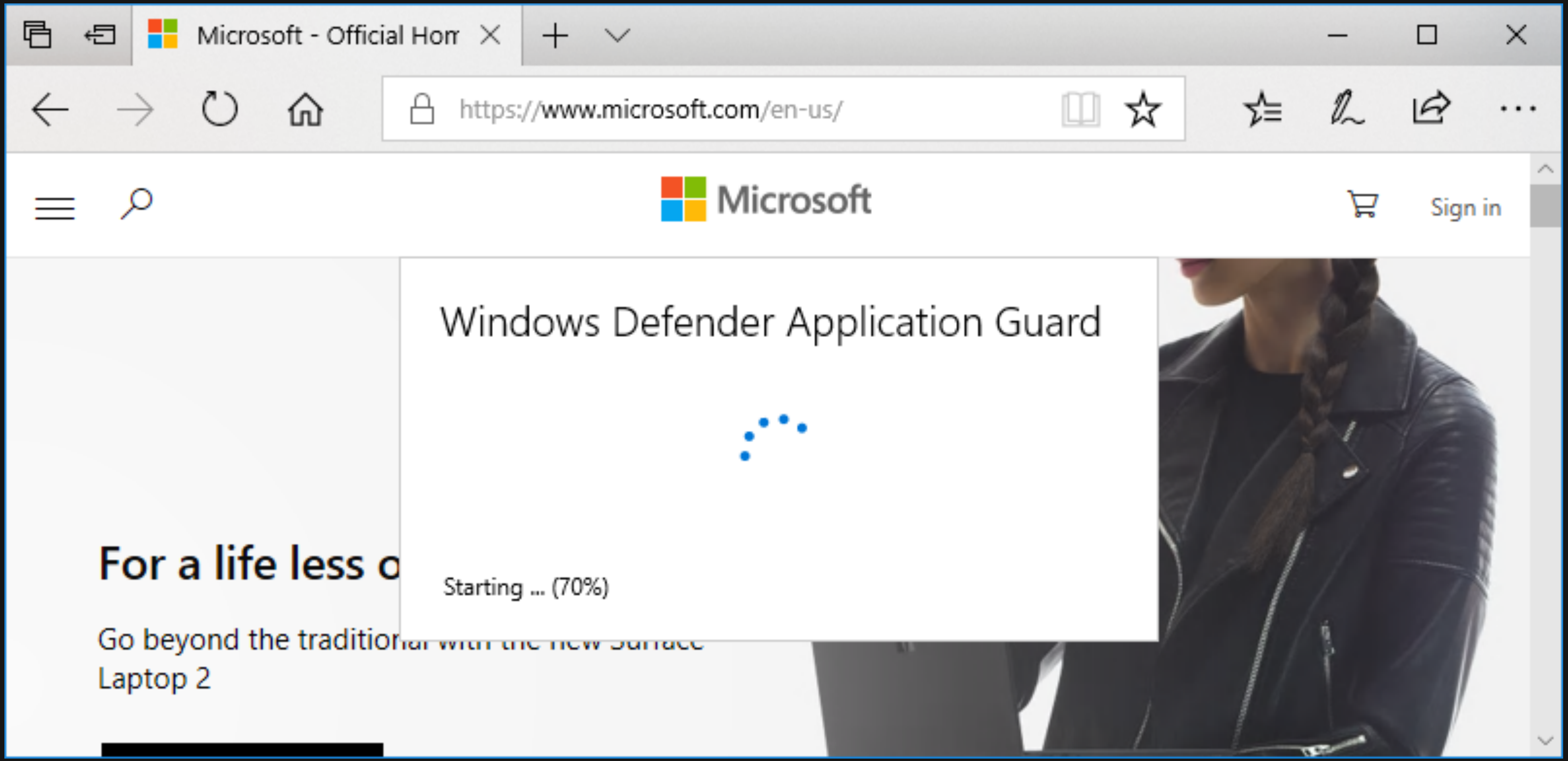
How to use WDAG

- New menu item in Microsoft Edge



How to use WDAG

- Starting WDAG

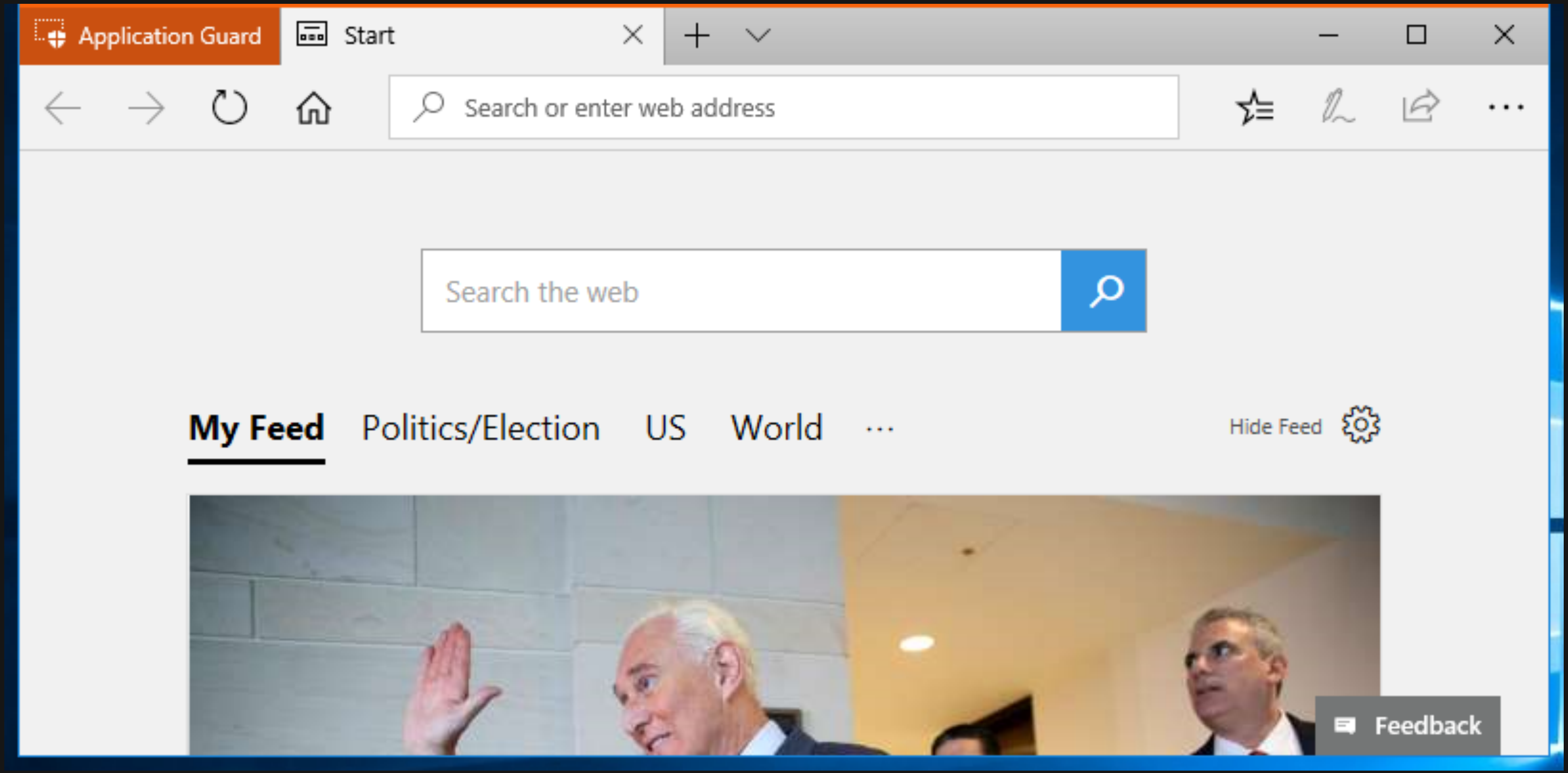

Microsoft - Official Hom
https://www.microsoft.com/en-us/
Microsoft
Sign in
For a life less o
Go beyond the traditional with the new Surface
Laptop 2

Windows Defender Application Guard

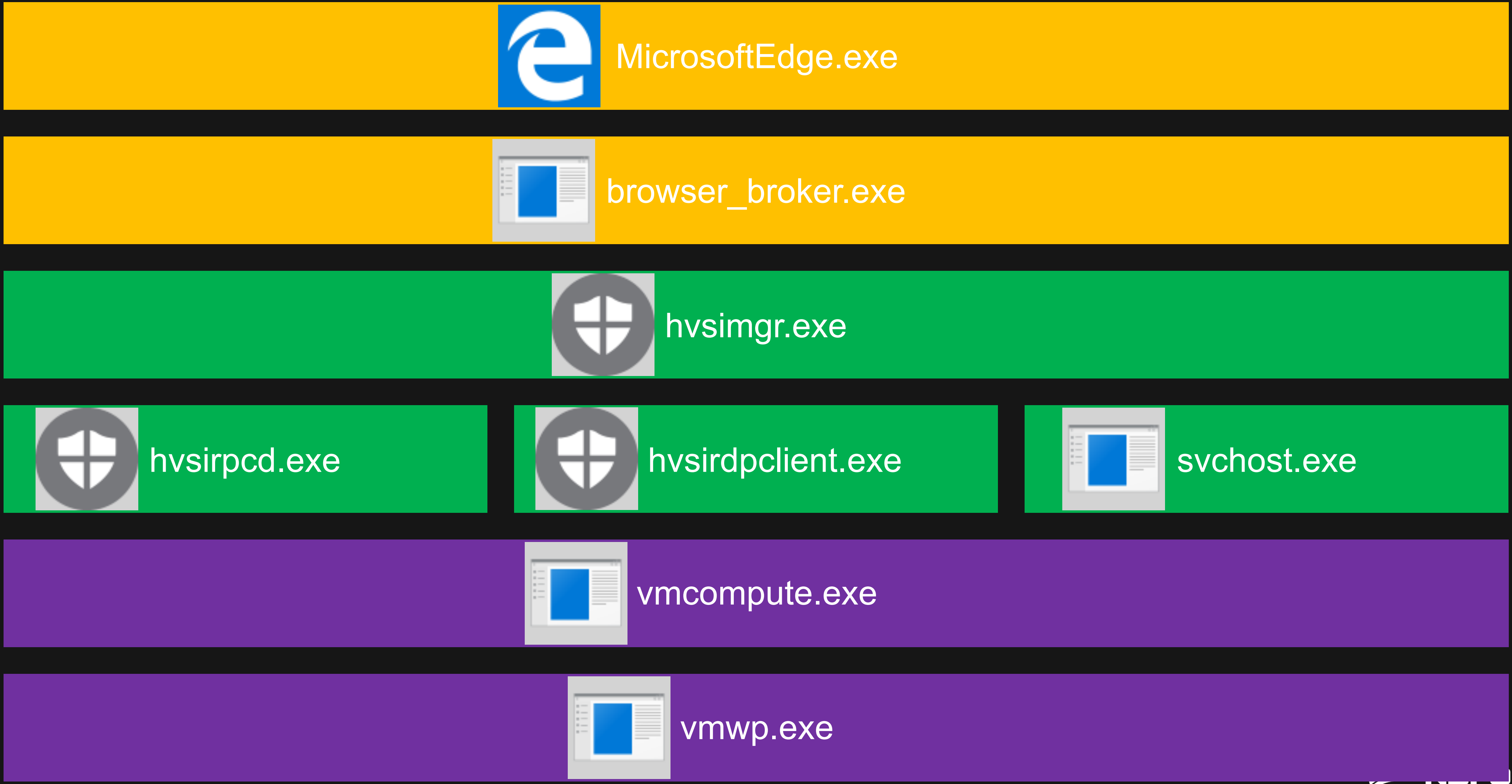
Starting ... (70%)

How to use WDAG

- Microsoft Edge inside WDAG



WDAG Architecture



MicrosoftEdge.exe

browser_broker.exe

hvsimgr.exe

hvsirpcd.exe

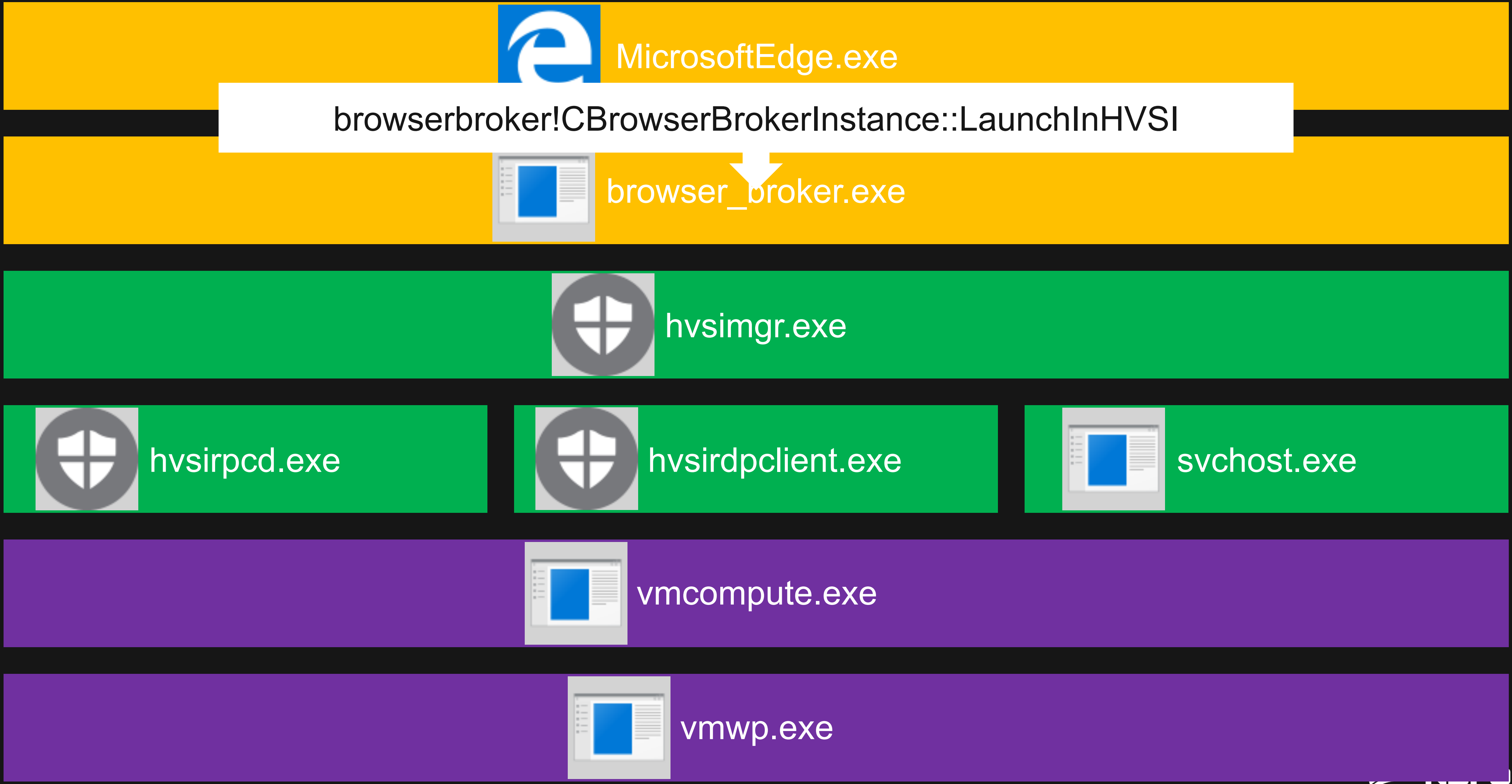
hvsirdpclient.exe

svchost.exe

vmcompute.exe

vmwp.exe

WDAG Architecture



MicrosoftEdge.exe

browserbroker!CBrowserBrokerInstance::LaunchInHVSI

browser_broker.exe

hvsimgr.exe

hvsirpcd.exe

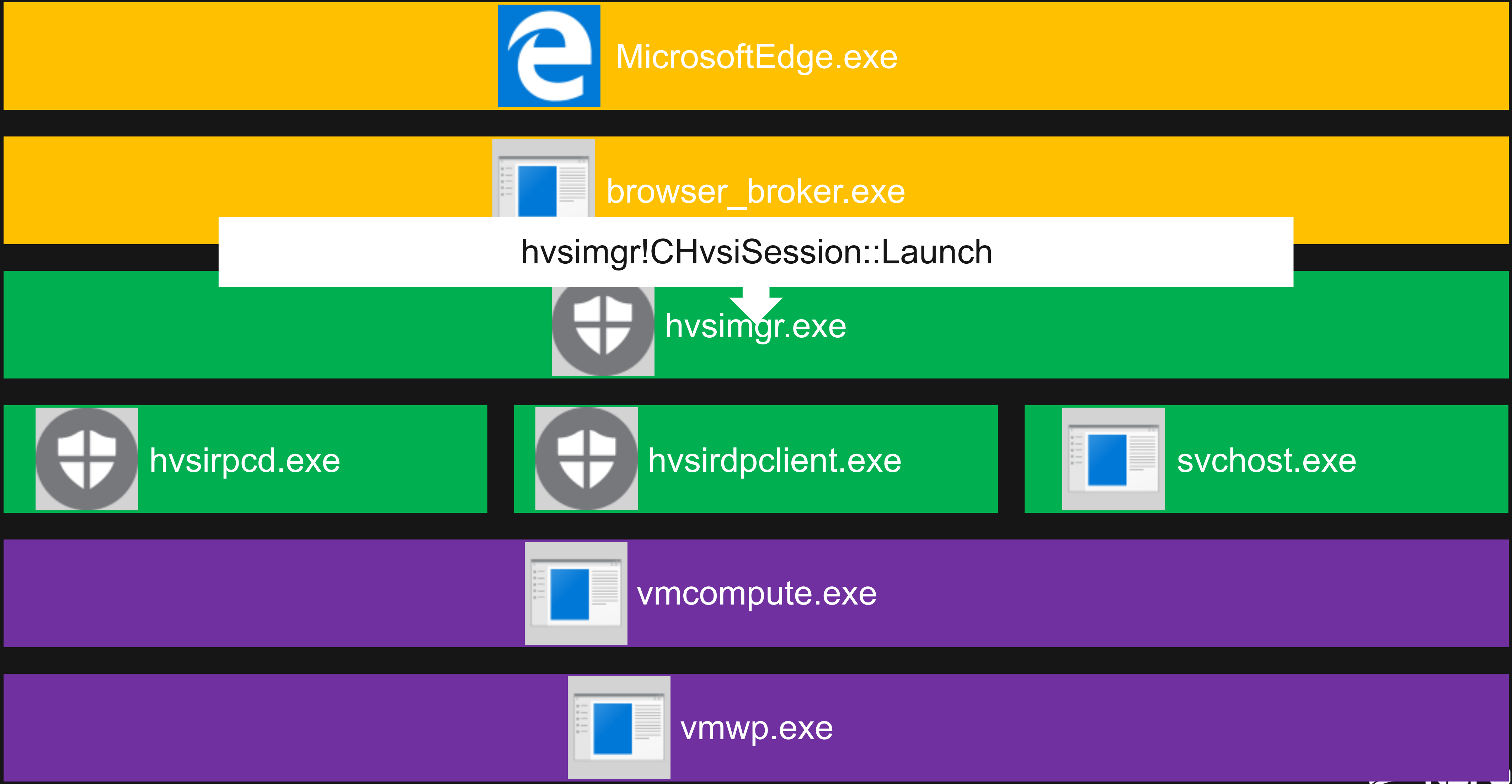
hvsirdpclient.exe

svchost.exe

vmcompute.exe

vmwp.exe

WDAG Architecture



MicrosoftEdge.exe

browser_broker.exe

hvsimgr!CHvsiSession::Launch

hvsimgr.exe

hvsirpcd.exe

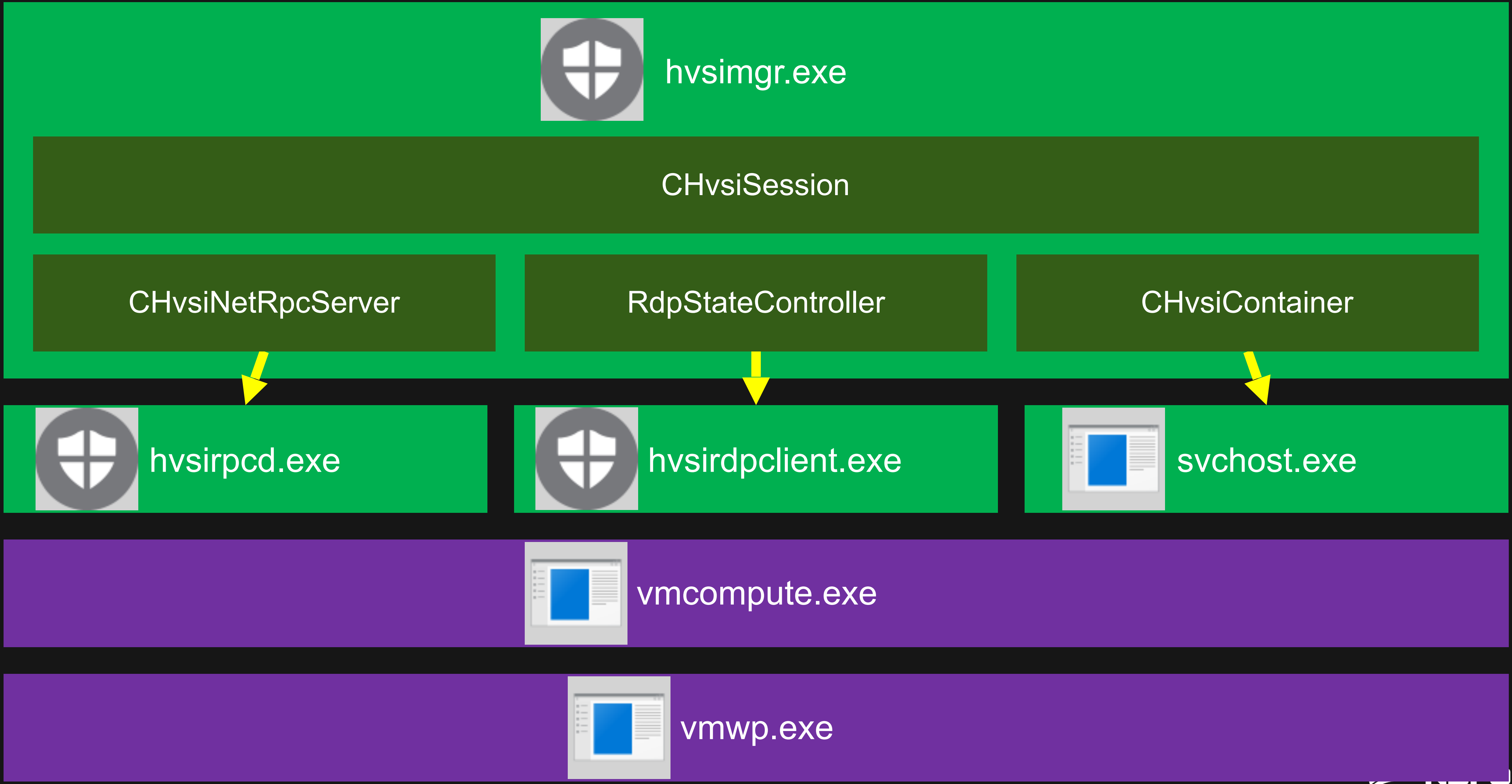
hvsirdpclient.exe

svchost.exe

vmcompute.exe

vmwp.exe

WDAG Architecture



hvsimgr.exe

CHvsiSession

CHvsiNetRpcServer

RdpStateController

CHvsiContainer

hvsirpcd.exe

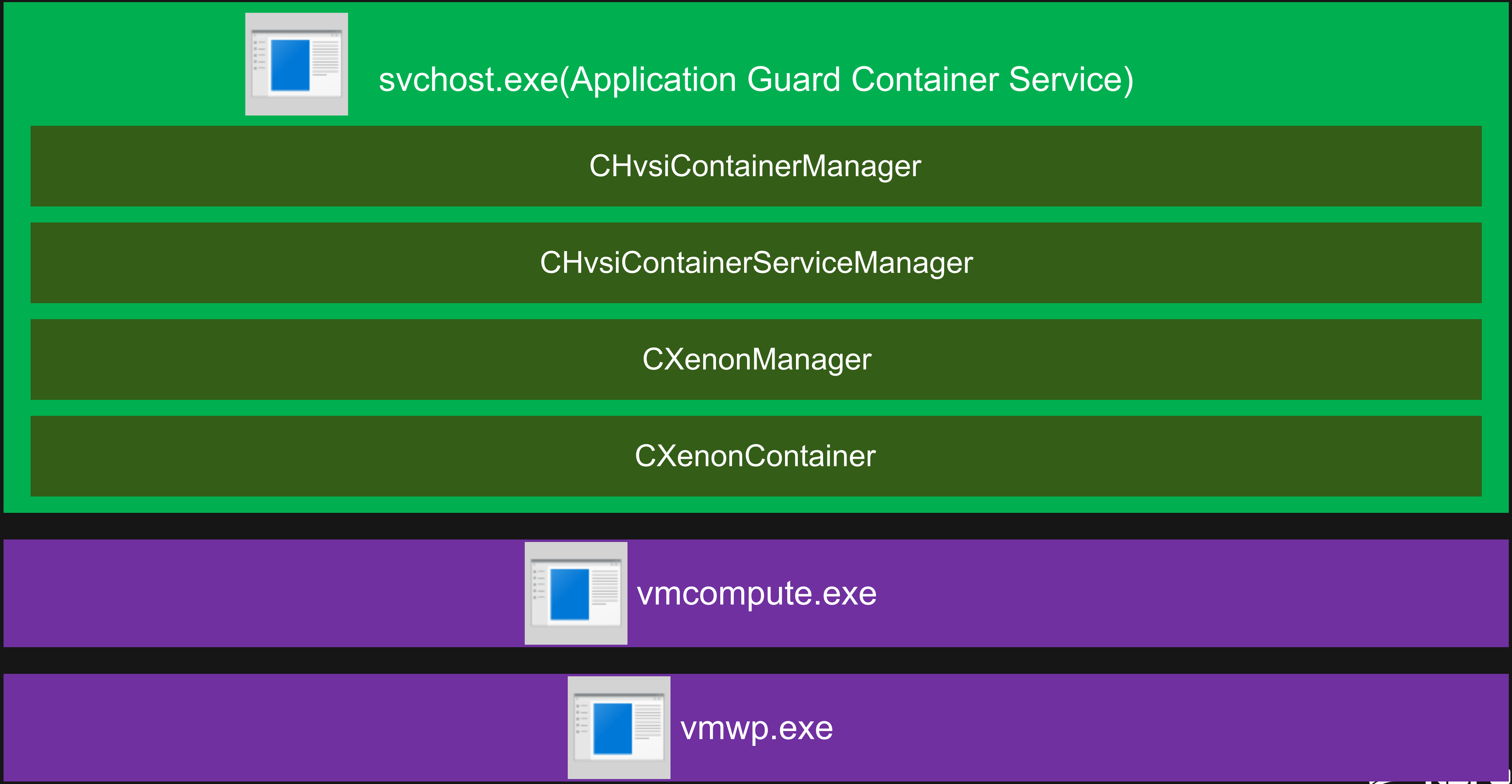
hvsirdpclient.exe

svchost.exe

vmcompute.exe

vmwp.exe

WDAG Architecture



svchost.exe(Application Guard Container Service)

CHvsiContainerManager

CHvsiContainerServiceManager

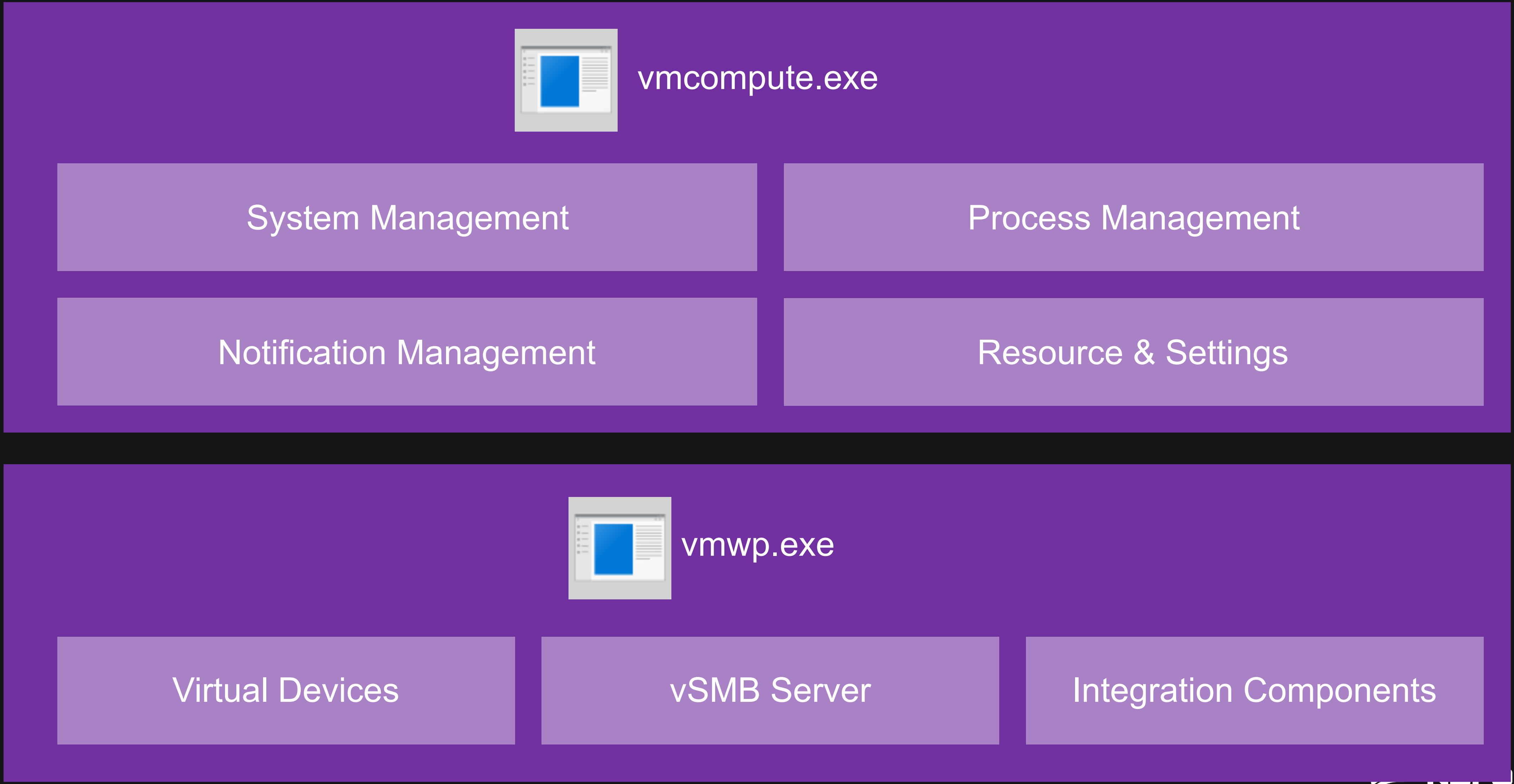
CXenonManager

CXenonContainer

vmcompute.exe

vmwp.exe

WDAG Architecture



vmcompute.exe

System Management

Process Management

Notification Management

Resource & Settings

vmwp.exe

Virtual Devices

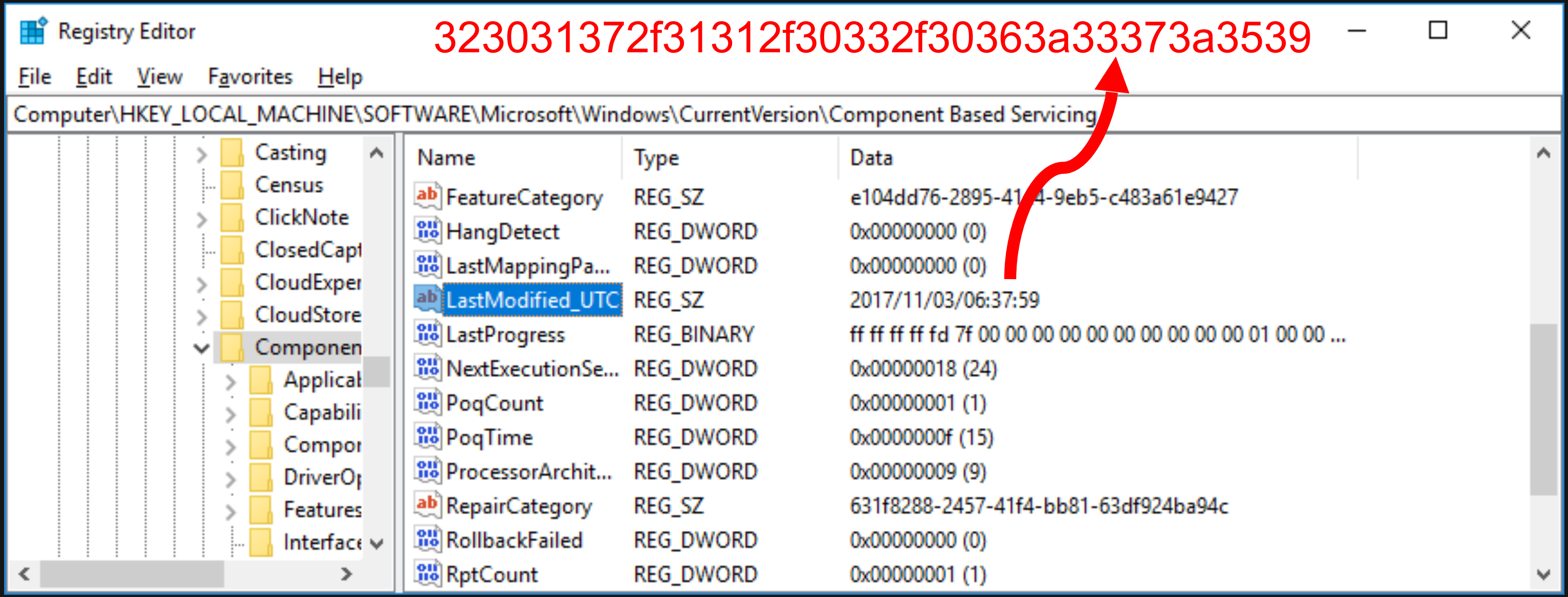
vSMB Server

Integration Components

WDAG Internals

Terminology

- Image Name
  - Hex string of HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\LastModified_UTC



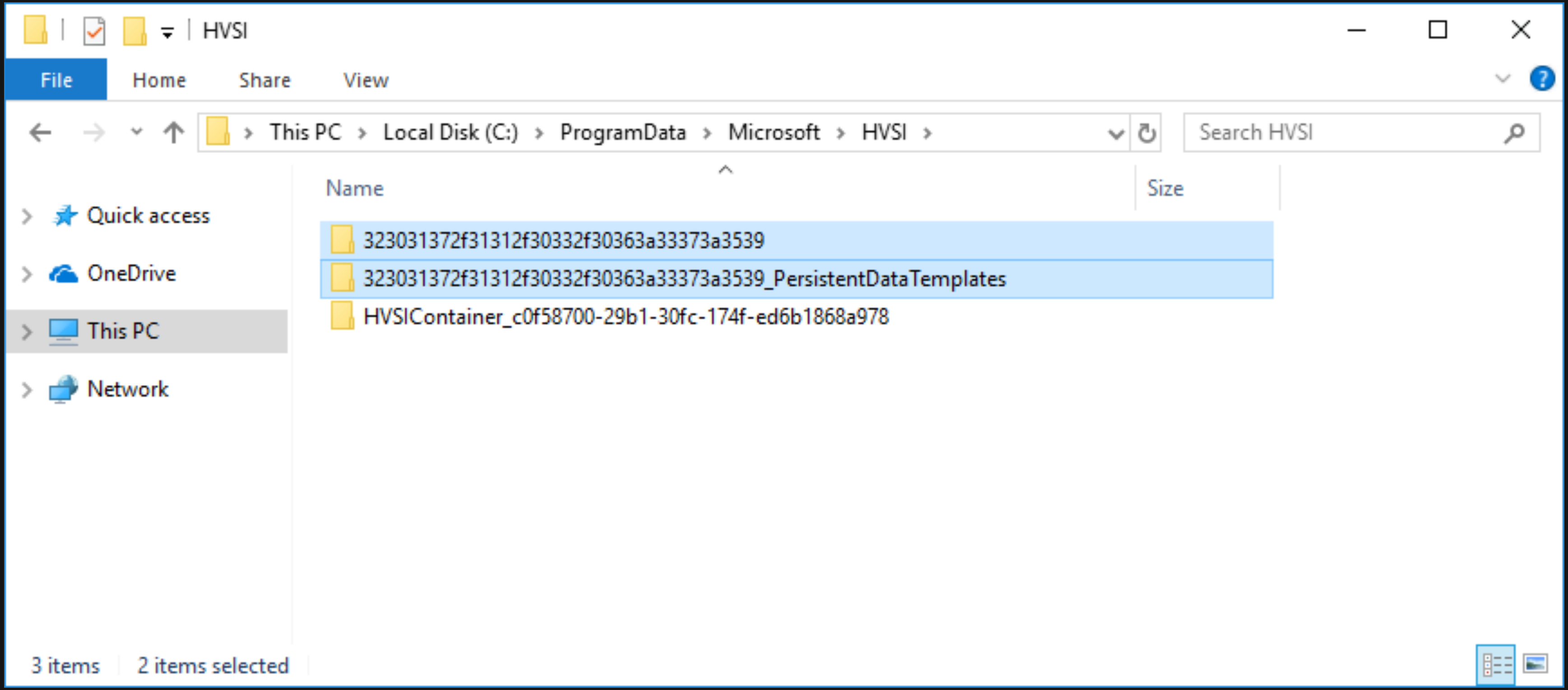
323031372f31312f30332f30363a33373a3539

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing

Name	Type	Data
FeatureCategory	REG_SZ	e104dd76-2895-41 4-9eb5-c483a61e9427
HangDetect	REG_DWORD	0x00000000 (0)
LastMappingPa...	REG_DWORD	0x00000000 (0)
LastModified_UTC	REG_SZ	2017/11/03/06:37:59
LastProgress	REG_BINARY	ff ff ff ff fd 7f 00 00 00 00 00 00 00 00 00 00 01 00 00 ...
NextExecutionSe...	REG_DWORD	0x00000018 (24)
PoqCount	REG_DWORD	0x00000001 (1)
PoqTime	REG_DWORD	0x0000000f (15)
ProcessorArchit...	REG_DWORD	0x00000009 (9)
RepairCategory	REG_SZ	631f8288-2457-41f4-bb81-63df924ba94c
RollbackFailed	REG_DWORD	0x00000000 (0)
RptCount	REG_DWORD	0x00000001 (1)

WDAG Internals

- Terminology
  - Image Name



323031372f31312f30332f30363a33373a3539

323031372f31312f30332f30363a33373a3539_PersistentDataTemplates

HVSIContainer_c0f58700-29b1-30fc-174f-ed6b1868a978

3 items 2 items selected

WDAG Internals

Terminology

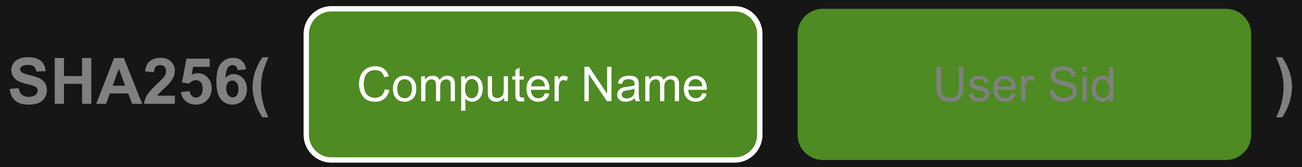
- Container ID

SHA256(Computer Name User Sid)

WDAG Internals

Terminology

- Container ID



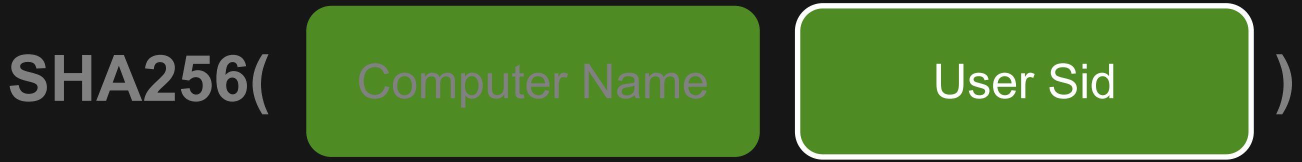
SHA256(Computer Name User Sid)

DESKTOP-7R43750

WDAG Internals

Terminology

- Container ID



SHA256(Computer Name User Sid)

S-1-5-21-2036491302-699820345-3847261429-1001

WDAG Internals

Terminology

- Container ID

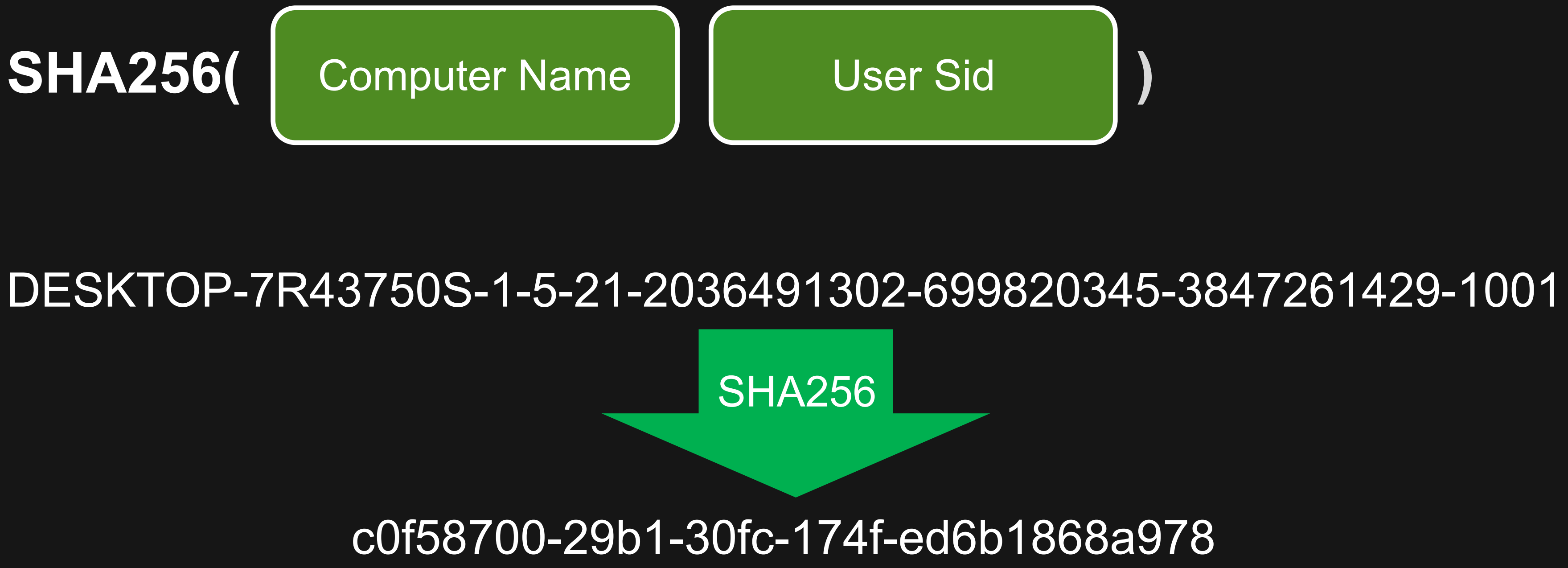
SHA256(Computer Name User Sid)

DESKTOP-7R43750S-1-5-21-2036491302-699820345-3847261429-1001

WDAG Internals

Terminology

- Container ID



SHA256(Computer Name User Sid)

DESKTOP-7R43750S-1-5-21-2036491302-699820345-3847261429-1001

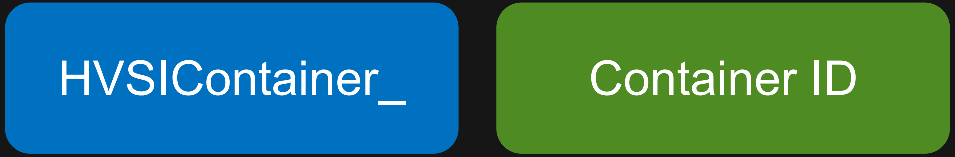
SHA256

c0f58700-29b1-30fc-174f-ed6b1868a978

WDAG Internals

Terminology

- Container Name



HVSIContainer_

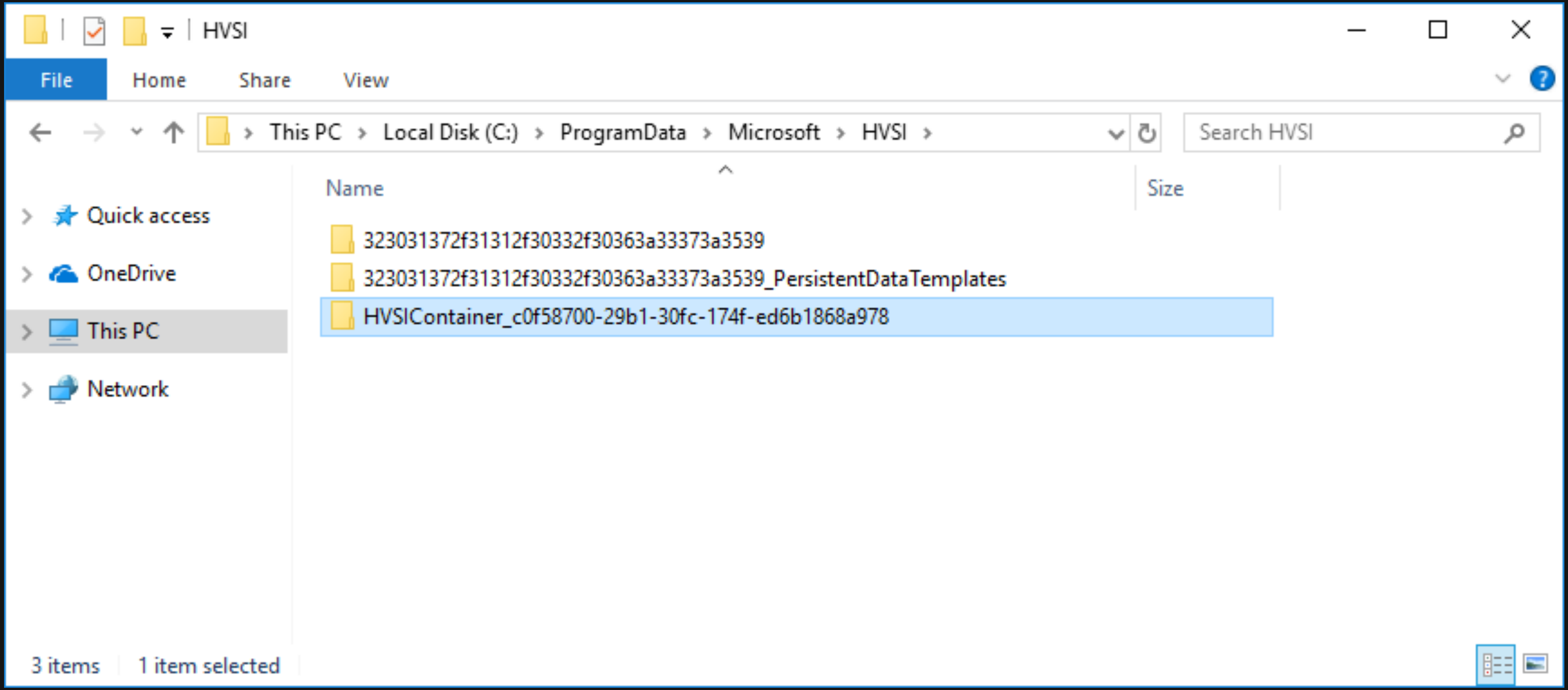
Container ID

HVSIContainer_c0f58700-29b1-30fc-174f-ed6b1868a978

WDAG Internals

Terminology

- Container Name



323031372f31312f30332f30363a33373a3539

323031372f31312f30332f30363a33373a3539_PersistentDataTemplates

HVSIContainer_c0f58700-29b1-30fc-174f-ed6b1868a978

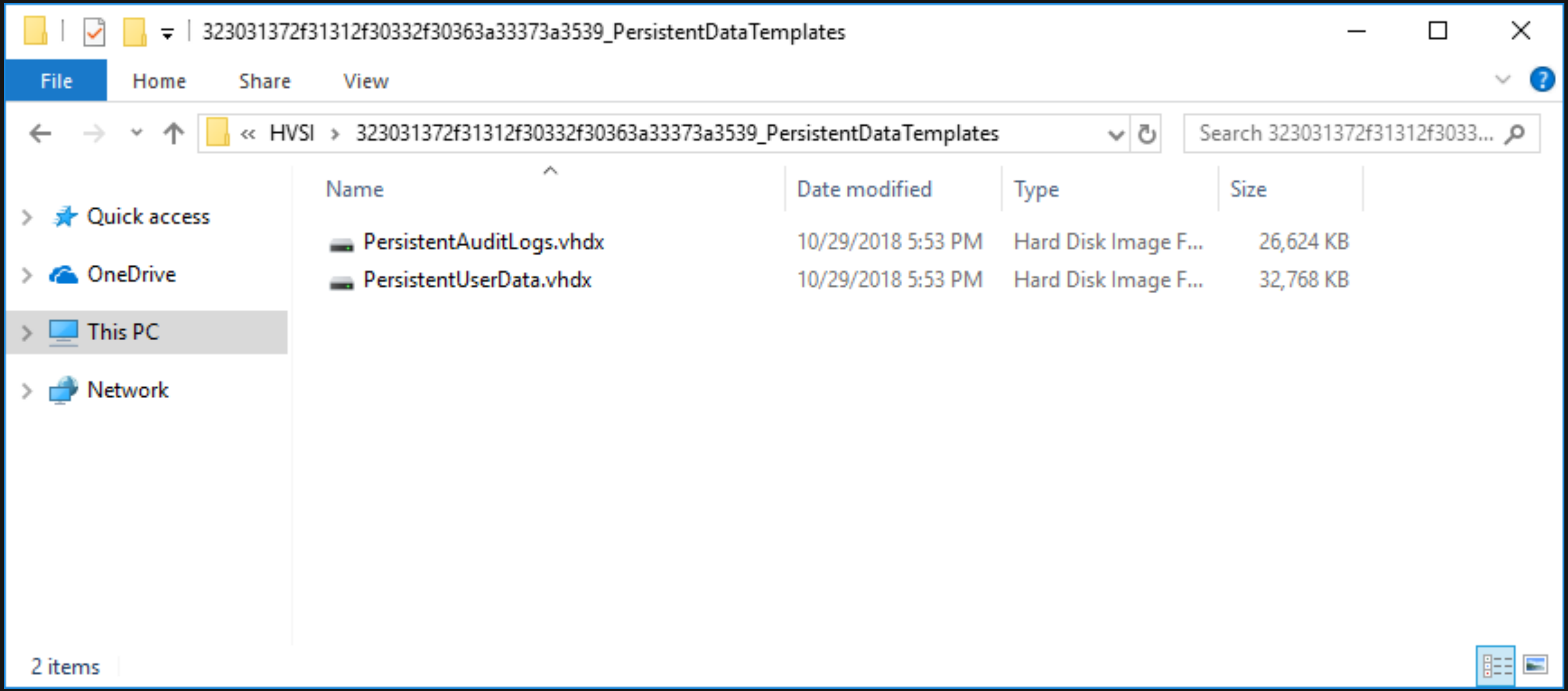
3 items 1 item selected

WDAG Internals

- Terminology
  - Runtime ID
    - Dynamic generated GUID for container instance
    - Generated each time when container is created

WDAG Internals

- How is the container created
  - Create Template Persistent Data Stores



323031372f31312f30332f30363a33373a3539_PersistentDataTemplates

« HVSI › 323031372f31312f30332f30363a33373a3539_PersistentDataTemplates

Search 323031372f31312f3033...

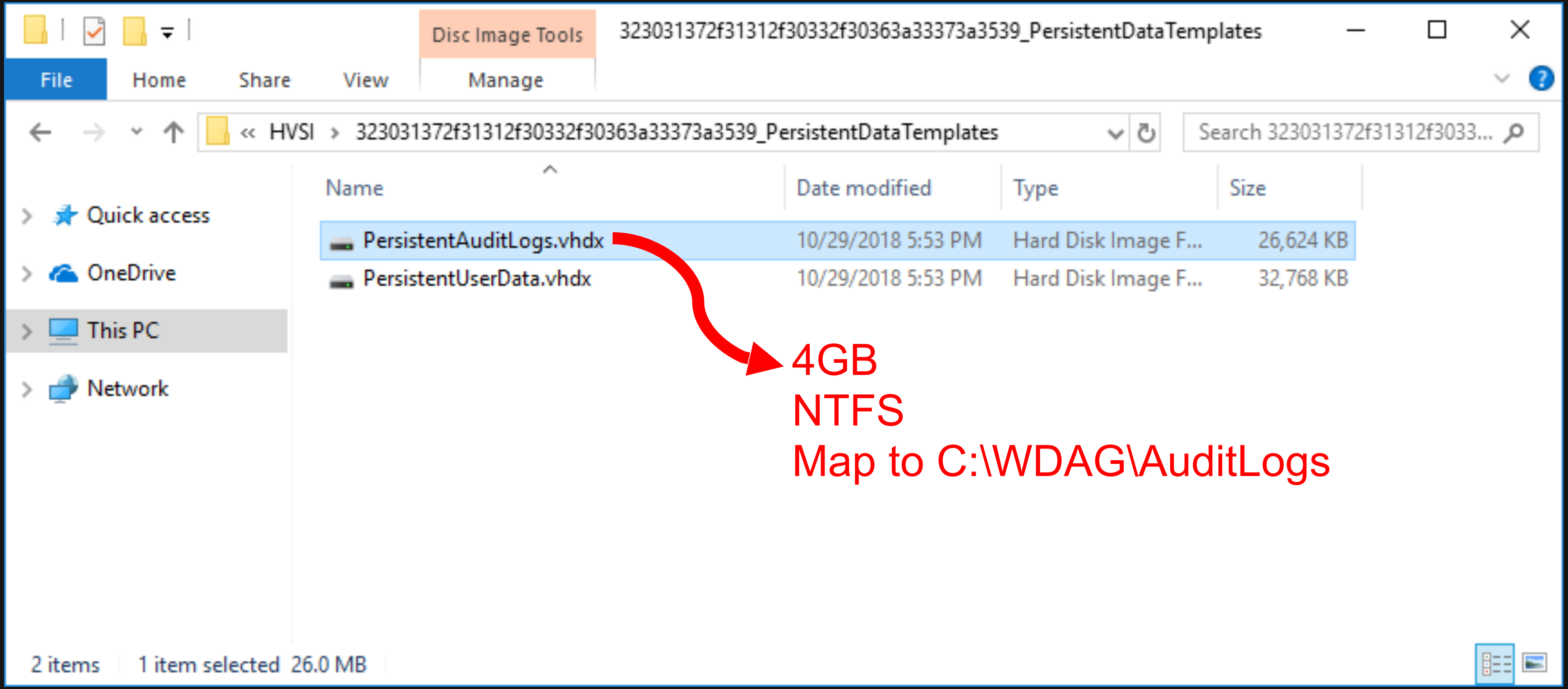
Name	Date modified	Type	Size
PersistentAuditLogs.vhdx	10/29/2018 5:53 PM	Hard Disk Image F...	26,624 KB
PersistentUserData.vhdx	10/29/2018 5:53 PM	Hard Disk Image F...	32,768 KB

2 items

WDAG Internals

How is the container created

- Create Template Persistent Data Stores



Disc Image Tools
323031372f31312f30332f30363a33373a3539_PersistentDataTemplates
File
Home
Share
View
Manage
HVSI
Search 323031372f31312f3033...
Quick access
OneDrive
This PC
Network

323031372f31312f30332f30363a33373a3539_PersistentDataTemplates

Name	Date modified	Type	Size
PersistentAuditLogs.vhdx	10/29/2018 5:53 PM	Hard Disk Image F...	26,624 KB
PersistentUserData.vhdx	10/29/2018 5:53 PM	Hard Disk Image F...	32,768 KB

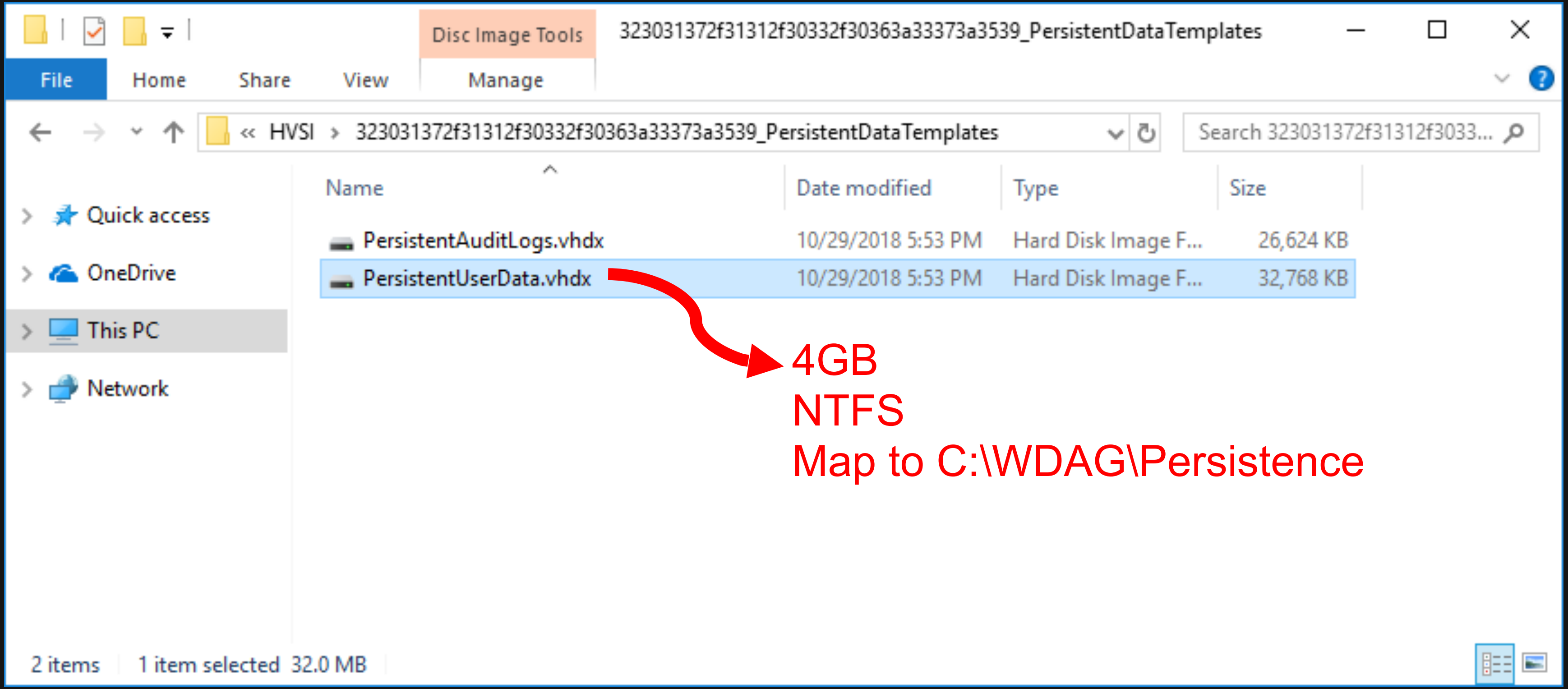
2 items   1 item selected 26.0 MB

4GB
NTFS
Map to C:\WDAG\AuditLogs

WDAG Internals

How is the container created

- Create Template Persistent Data Stores



Disc Image Tools
323031372f31312f30332f30363a33373a3539_PersistentDataTemplates
File
Home
Share
View
Manage
« HVSI › 323031372f31312f30332f30363a33373a3539_PersistentDataTemplates
Search 323031372f31312f3033...
Quick access
OneDrive
This PC
Network

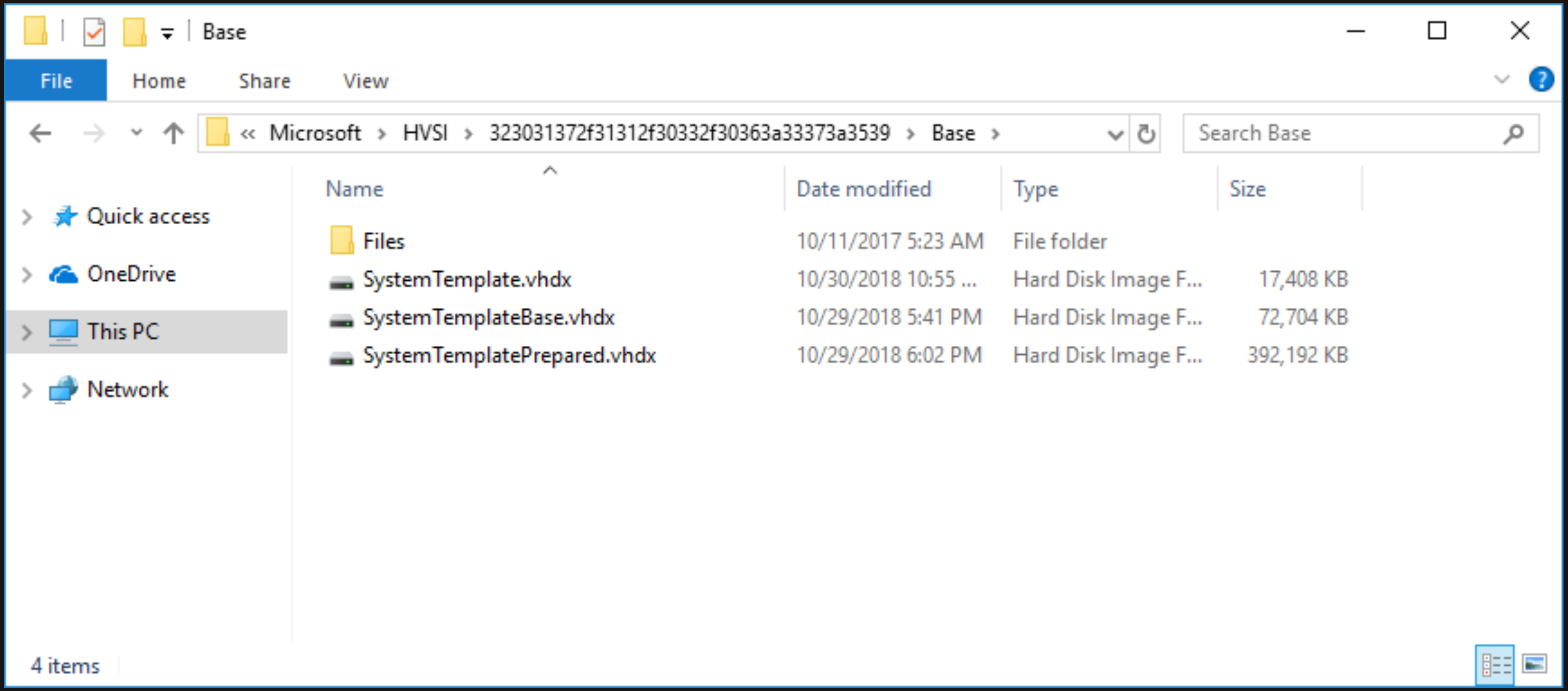
Name	Date modified	Type	Size
PersistentAuditLogs.vhdx	10/29/2018 5:53 PM	Hard Disk Image F...	26,624 KB
PersistentUserData.vhdx	10/29/2018 5:53 PM	Hard Disk Image F...	32,768 KB

2 items 1 item selected 32.0 MB

4GB
NTFS
Map to C:\WDAG\Persistence

WDAG Internals

- How is the container created
  - Create Base Image



Base

« Microsoft › HVSI › 323031372f31312f30332f30363a33373a3539 › Base ›

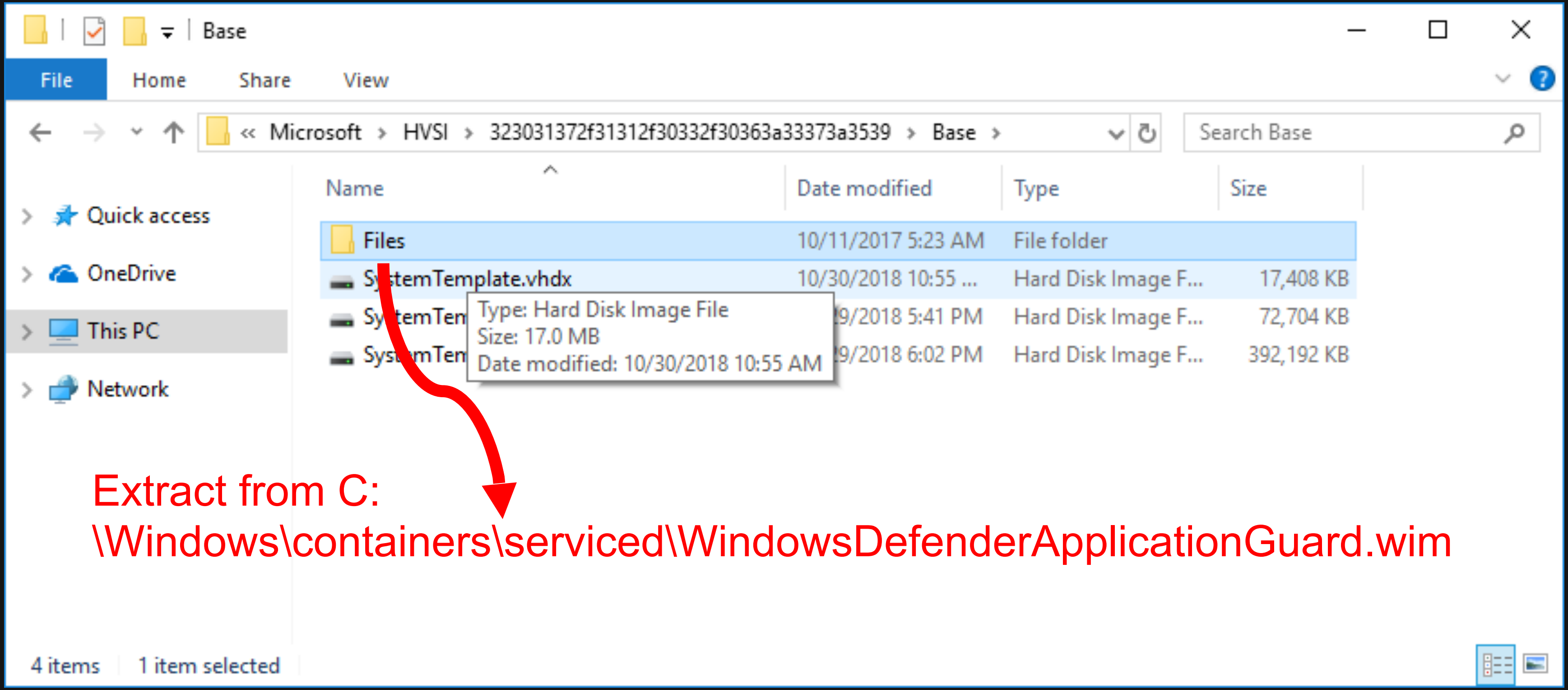
Name	Date modified	Type	Size
Files	10/11/2017 5:23 AM	File folder	
SystemTemplate.vhdx	10/30/2018 10:55 ...	Hard Disk Image F...	17,408 KB
SystemTemplateBase.vhdx	10/29/2018 5:41 PM	Hard Disk Image F...	72,704 KB
SystemTemplatePrepared.vhdx	10/29/2018 6:02 PM	Hard Disk Image F...	392,192 KB

4 items

WDAG Internals

How is the container created

- Create Base Image



Base

File
Home
Share
View
« Microsoft › HVSI › 323031372f31312f30332f30363a33373a3539 › Base ›
Search Base
Quick access
OneDrive
This PC
Network

Name	Date modified	Type	Size
Files	10/11/2017 5:23 AM	File folder	
SystemTemplate.vhdx	10/30/2018 10:55 ...	Hard Disk Image F...	17,408 KB
SystemTem	9/2018 5:41 PM	Hard Disk Image F...	72,704 KB
SystemTem	9/2018 6:02 PM	Hard Disk Image F...	392,192 KB

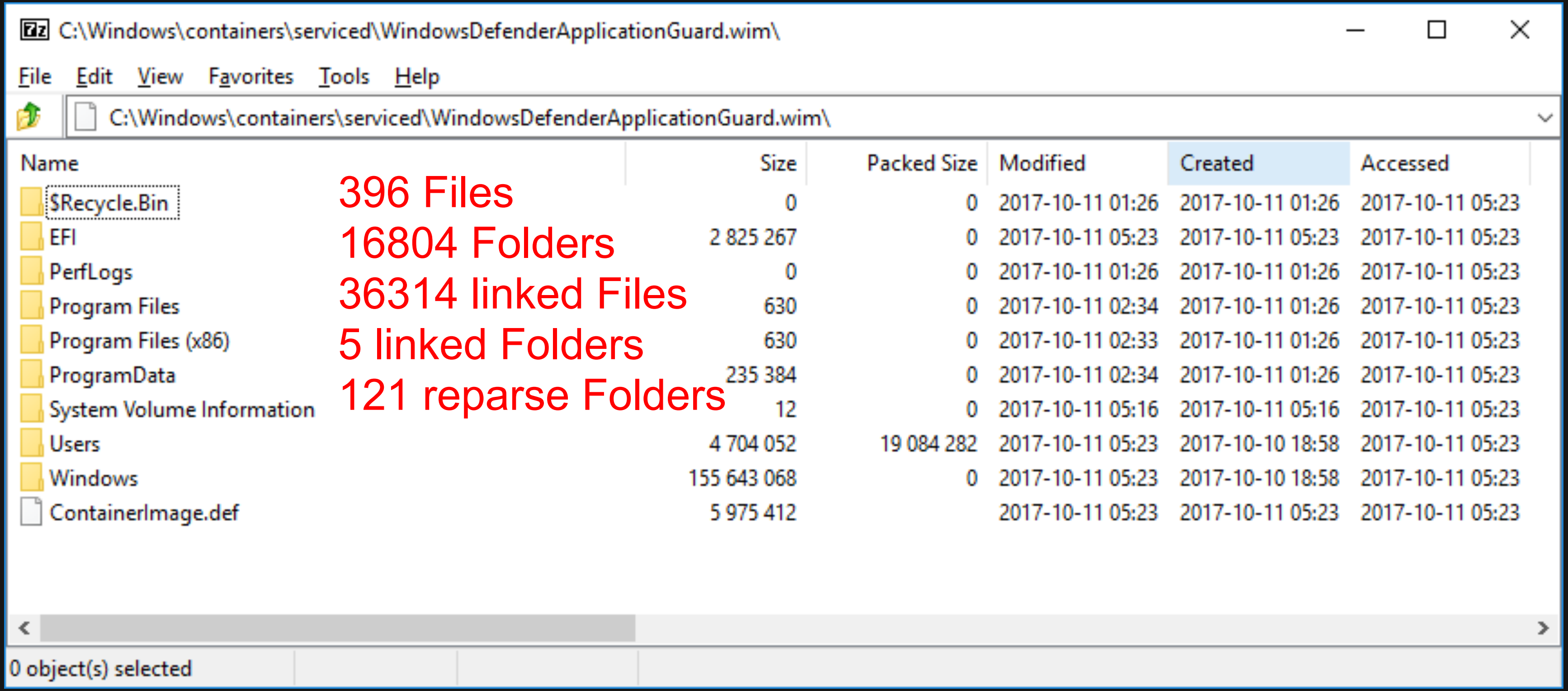
Type: Hard Disk Image File
Size: 17.0 MB
Date modified: 10/30/2018 10:55 AM

4 items 1 item selected

Extract from C:
\Windows\containers\serviced\WindowsDefenderApplicationGuard.wim

WDAG Internals

- How is the container created
  - Create Base Image



C:\Windows\containers\serviced\WindowsDefenderApplicationGuard.wim\

C:\Windows\containers\serviced\WindowsDefenderApplicationGuard.wim\

396 Files
16804 Folders
36314 linked Files
5 linked Folders
121 reparse Folders

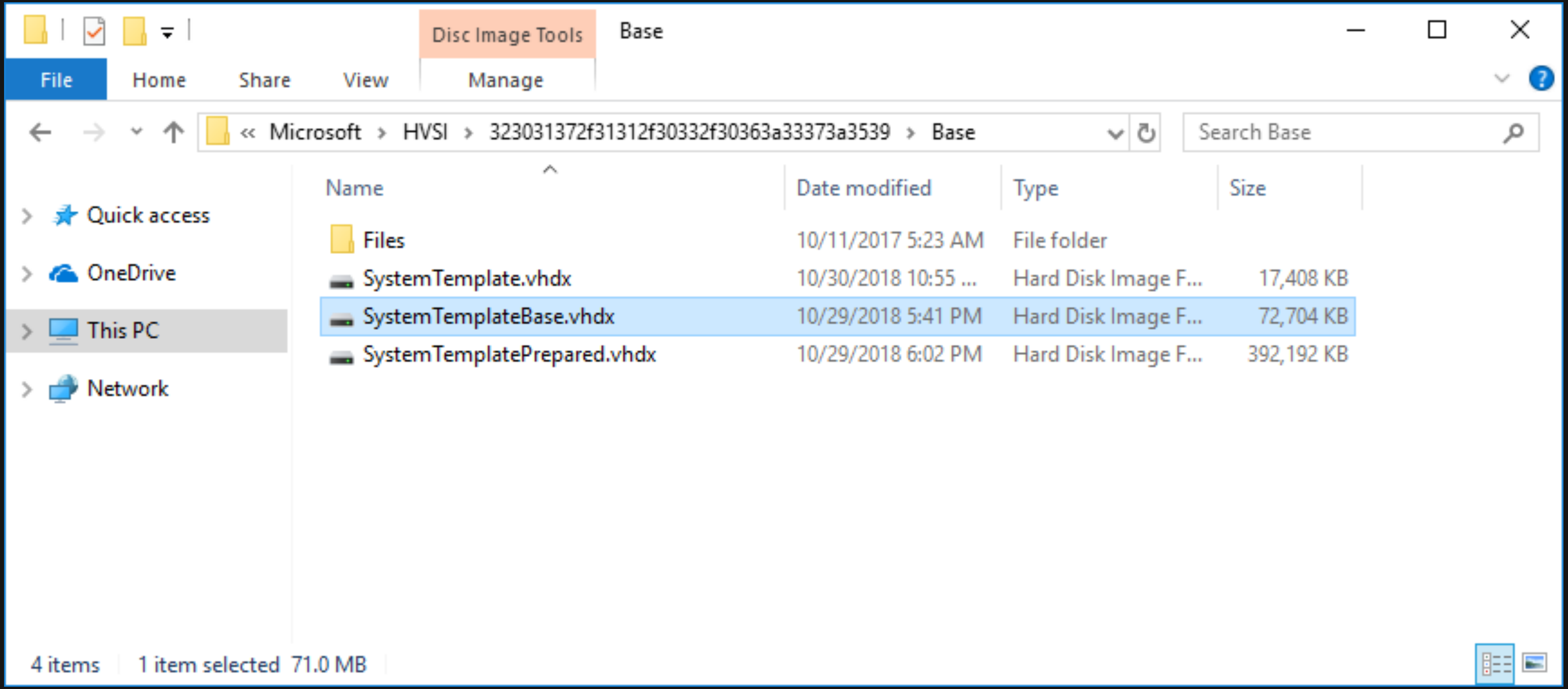
Name	Size	Packed Size	Modified	Created	Accessed
$Recycle.Bin	0	0	2017-10-11 01:26	2017-10-11 01:26	2017-10-11 05:23
EFI	2 825 267	0	2017-10-11 05:23	2017-10-11 05:23	2017-10-11 05:23
PerfLogs	0	0	2017-10-11 01:26	2017-10-11 01:26	2017-10-11 05:23
Program Files	630	0	2017-10-11 02:34	2017-10-11 01:26	2017-10-11 05:23
Program Files (x86)	630	0	2017-10-11 02:33	2017-10-11 01:26	2017-10-11 05:23
ProgramData	235 384	0	2017-10-11 02:34	2017-10-11 01:26	2017-10-11 05:23
System Volume Information	12	0	2017-10-11 05:16	2017-10-11 05:16	2017-10-11 05:23
Users	4 704 052	19 084 282	2017-10-11 05:23	2017-10-10 18:58	2017-10-11 05:23
Windows	155 643 068	0	2017-10-11 05:23	2017-10-10 18:58	2017-10-11 05:23
ContainerImage.def	5 975 412		2017-10-11 05:23	2017-10-11 05:23	2017-10-11 05:23

0 object(s) selected

WDAG Internals

How is the container created

- Create Base Image



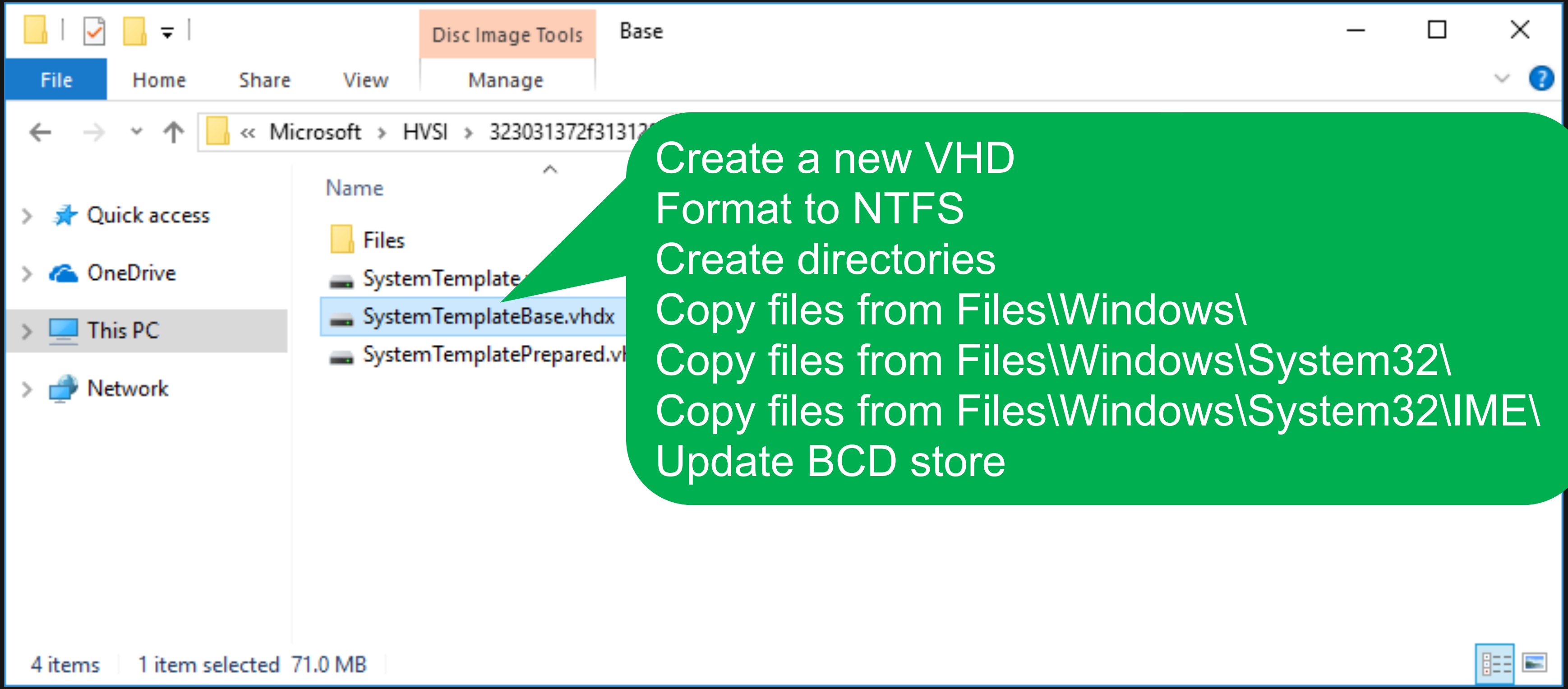
Name	Date modified	Type	Size
Files	10/11/2017 5:23 AM	File folder	
SystemTemplate.vhdx	10/30/2018 10:55 ...	Hard Disk Image F...	17,408 KB
SystemTemplateBase.vhdx	10/29/2018 5:41 PM	Hard Disk Image F...	72,704 KB
SystemTemplatePrepared.vhdx	10/29/2018 6:02 PM	Hard Disk Image F...	392,192 KB

4 items 1 item selected 71.0 MB

WDAG Internals

How is the container created

- Create Base Image

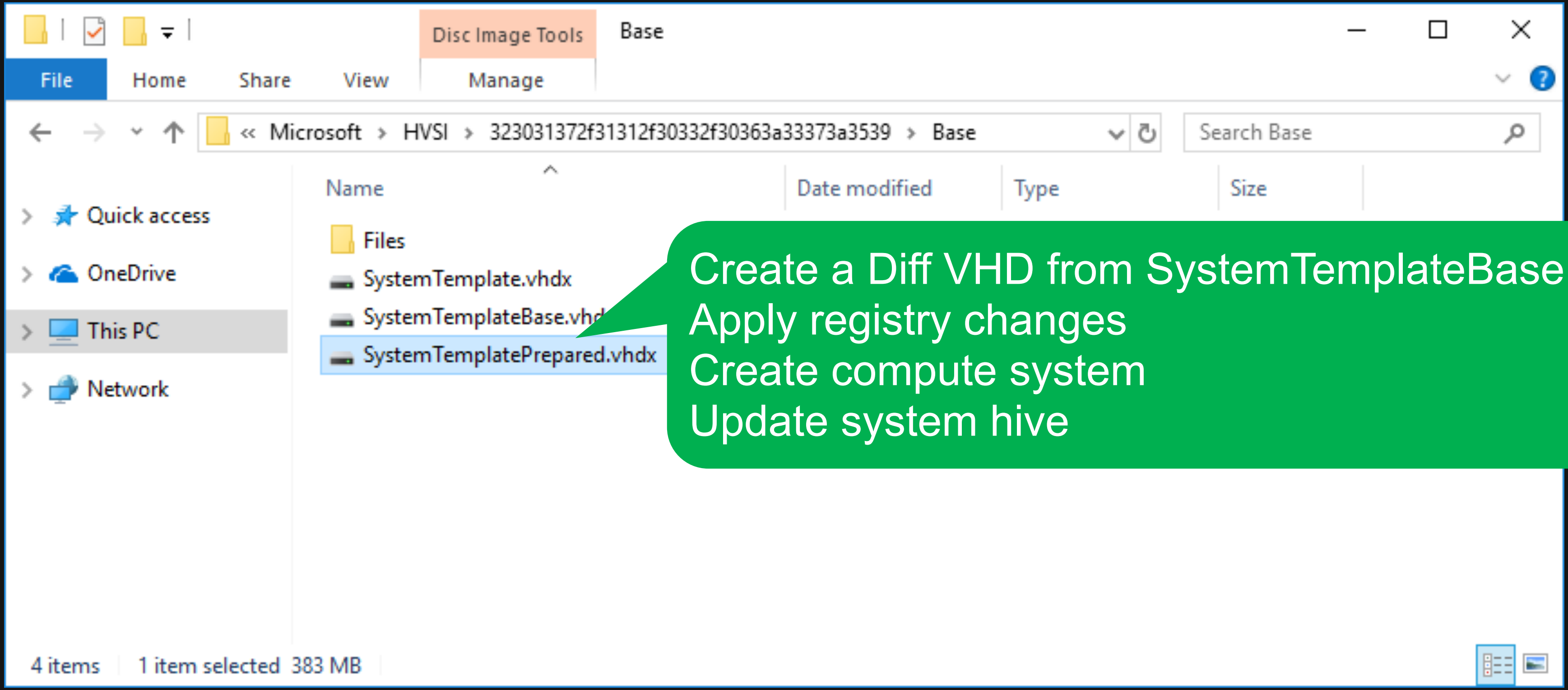


Create a new VHD
Format to NTFS
Create directories
Copy files from Files\Windows\
Copy files from Files\Windows\System32\
Copy files from Files\Windows\System32\IME\
Update BCD store

WDAG Internals

How is the container created

- Create Base Image



Files
SystemTemplate.vhdx
SystemTemplateBase.vhd
SystemTemplatePrepared.vhdx

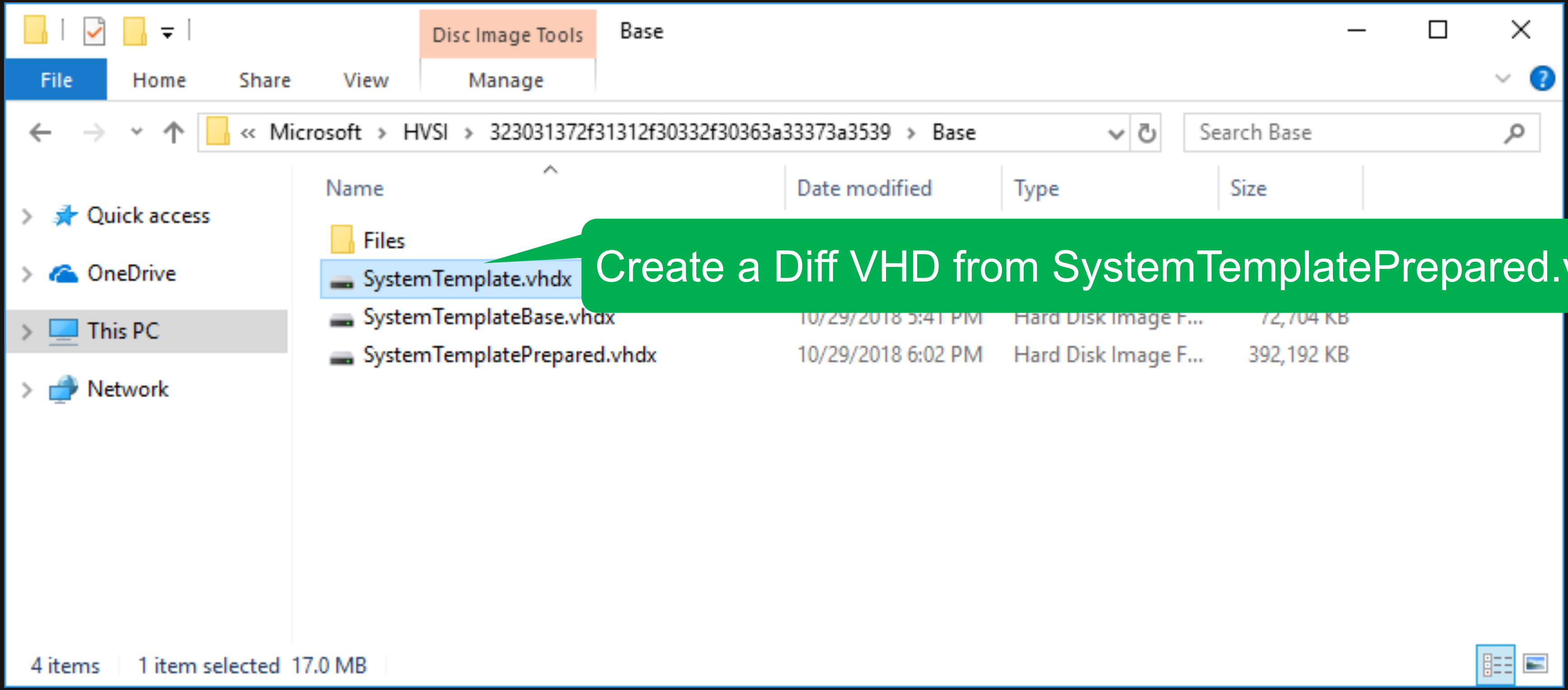
4 items 1 item selected 383 MB

Create a Diff VHD from SystemTemplateBase.vhdx
Apply registry changes
Create compute system
Update system hive

WDAG Internals

How is the container created

- Create Base Image



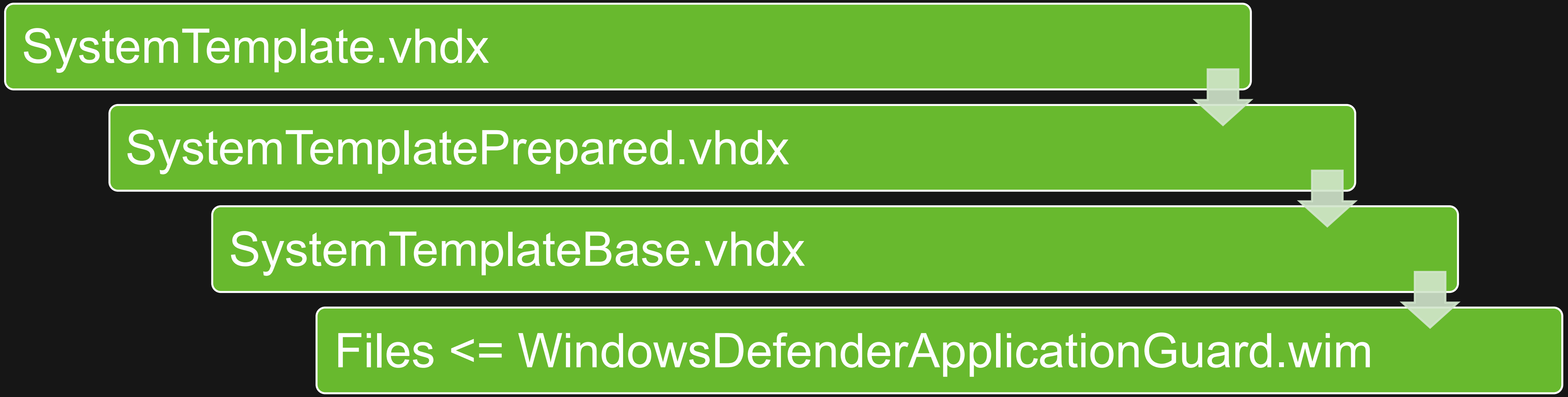
Name	Date modified	Type	Size
Files			
SystemTemplate.vhdx			
SystemTemplateBase.vhdx	10/29/2018 5:41 PM	Hard Disk Image F...	72,704 KB
SystemTemplatePrepared.vhdx	10/29/2018 6:02 PM	Hard Disk Image F...	392,192 KB

Create a Diff VHD from SystemTemplatePrepared.vhdx

NSFOCUS

WDAG Internals

- How is the container created
  - Create Base Image



SystemTemplate.vhdx

SystemTemplatePrepared.vhdx

SystemTemplateBase.vhdx

Files <= WindowsDefenderApplicationGuard.wim

WDAG Internals

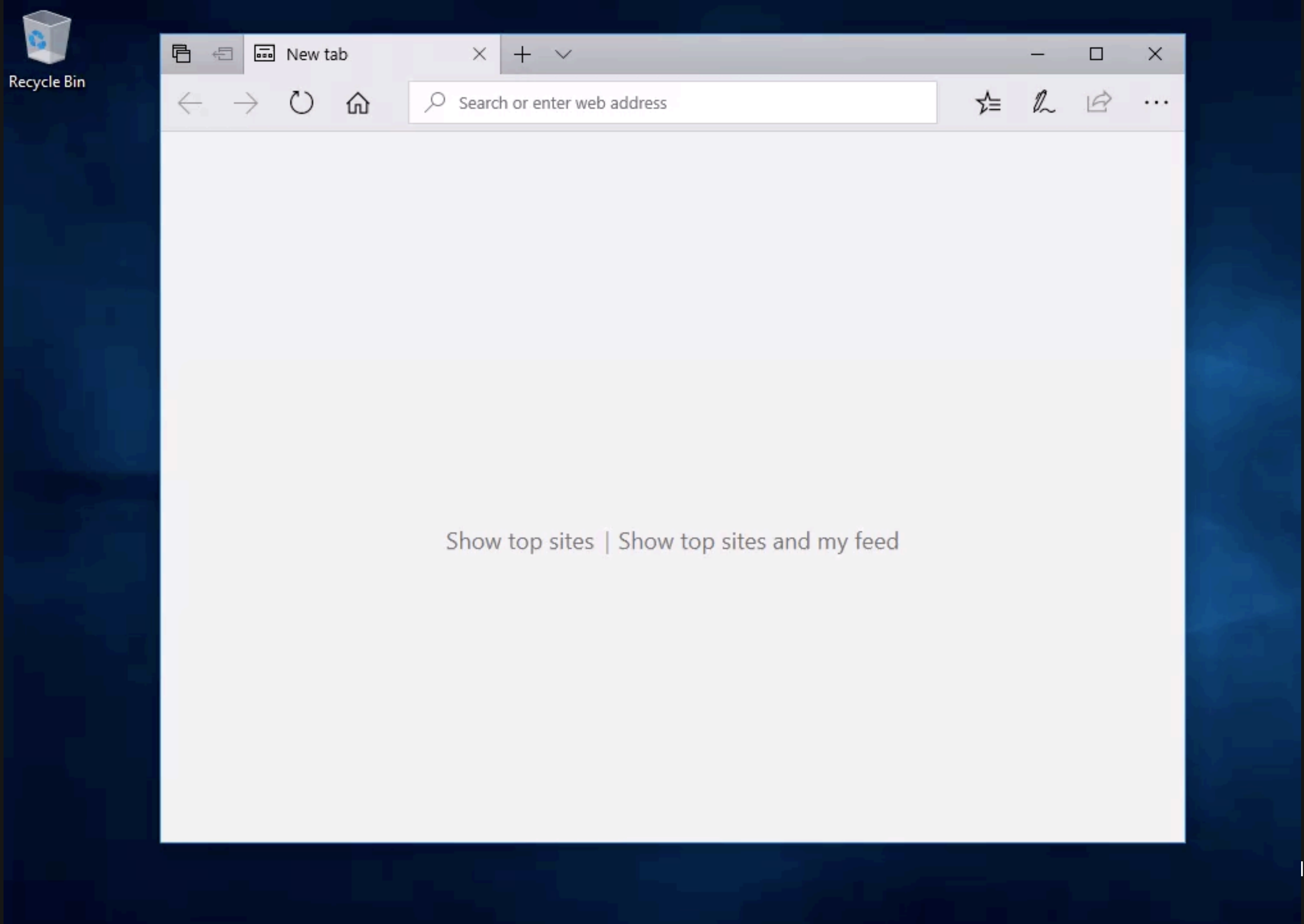
How is the container created

- Create Container
  - Generate Runtime ID
  - Prepare HVSI NAT
  - Attach Persistent Data Stores
  - Create Container Settings
  - Create Sandbox Layer
  - Create Compute System
  - Create Container Credential
  - Start Compute System
  - Apply Settings to Container
  - Init RDP Logon

```
{
  "SystemType":"Container",
  "Name":"HVSIContainer_c0f58700-29b1-30fc-174f-ed6b1868a978",
  "HvPartition":true,
  "Owner":"HVSI",
  "HvRuntime":{
    "RuntimeId":"3c810477-6845-43fd-aba0-c29d4d430998",
    "SkipTemplate":true,
    "EnableRdp":true,
    "RdpAccessSids":["S-1-5-21-2036491302-699820345-3847261429-1001","S-1-15-2-4241113689-1525372122-3928165819-2899915964-1654067008-1728629048-1671459956" ],
    "SynchronizeQPC":true,
    "BootFromLayers":true,
    "EnableMemoryHotHint":true,
    "EnableMemoryColdHint":true,
    "EnablePrivateMemoryCompressionStore":true,
    "EnableBattery":true,
    "BugcheckSavedStateFileName":"wdag.vmrs"
  },
  "HostName":"3c810477-6",
  "RegistryChanges":{"AddValues":[{"Key":{"Hive":"System","Name":"ControlSet001\\Services\\EventLog\\Security"},"Name":"MaxSize","Type":"DWord","DWordValue":20971520},...]},
  "MemoryMaximumInMB":4000,
  "ProcessorCount":4,
  "DirectFileMappingMB":1024,
  "SharedMemoryMB":1024,
  "SandboxPath":"C:\\ProgramData\\Microsoft\\HVSI\\HVSIContainer_c0f58700-29b1-30fc-174f-ed6b1868a978",
  "Layers":[{"Id":"1b3979c8-279b-42eb-b2b9-750767ee9e3f","Path":"C:\\ProgramData\\Microsoft\\HVSI\\323031372f31312f30332f30363a33373a3539\\Base"}],
  "MappedVirtualDisks":[
    {"HostPath":"C:\\Users\\test\\AppData\\Local\\Microsoft\\WDAG\\PersistentAuditLogs.vhdx","ContainerPath":"C:\\WDAG\\AuditLogs","OverwriteIfExists":true},
    {"HostPath":"C:\\Users\\test\\AppData\\Local\\Microsoft\\WDAG\\PersistentUserData.vhdx","ContainerPath":"C:\\WDAG\\Persistence","OverwriteIfExists":true}
  ],
  "NetworkEndpoints":[{
    "Id":"00000000-0000-0000-0000-000000000000",
    "EndpointName":"3c810477-6845-43fd-aba0-c29d4d430998",
    "StaticMacAddress":"02174FED6B18",
    "NetworkId":"161df6ed-7ce7-450f-8ddb-4603ff64edfc"
  }],
  "VsockStdioPortRange":{"Min":0,"Max":0},
  "EnableUtcRelay":true,
  "HvSocketConfig":{
    "ServiceTable":{
      "abd802e8-ffcc-40d2-a5f1-f04b1d12cbc8":{"BindSecurityDescriptor":"D:P(A;;FA;;;WD)(A;;FA;;;S-1-15-3-3)","ConnectSecurityDescriptor":"D:P(D;;FA;;;WD)"}
    }
  }
}
```

Reform WDAG for Research

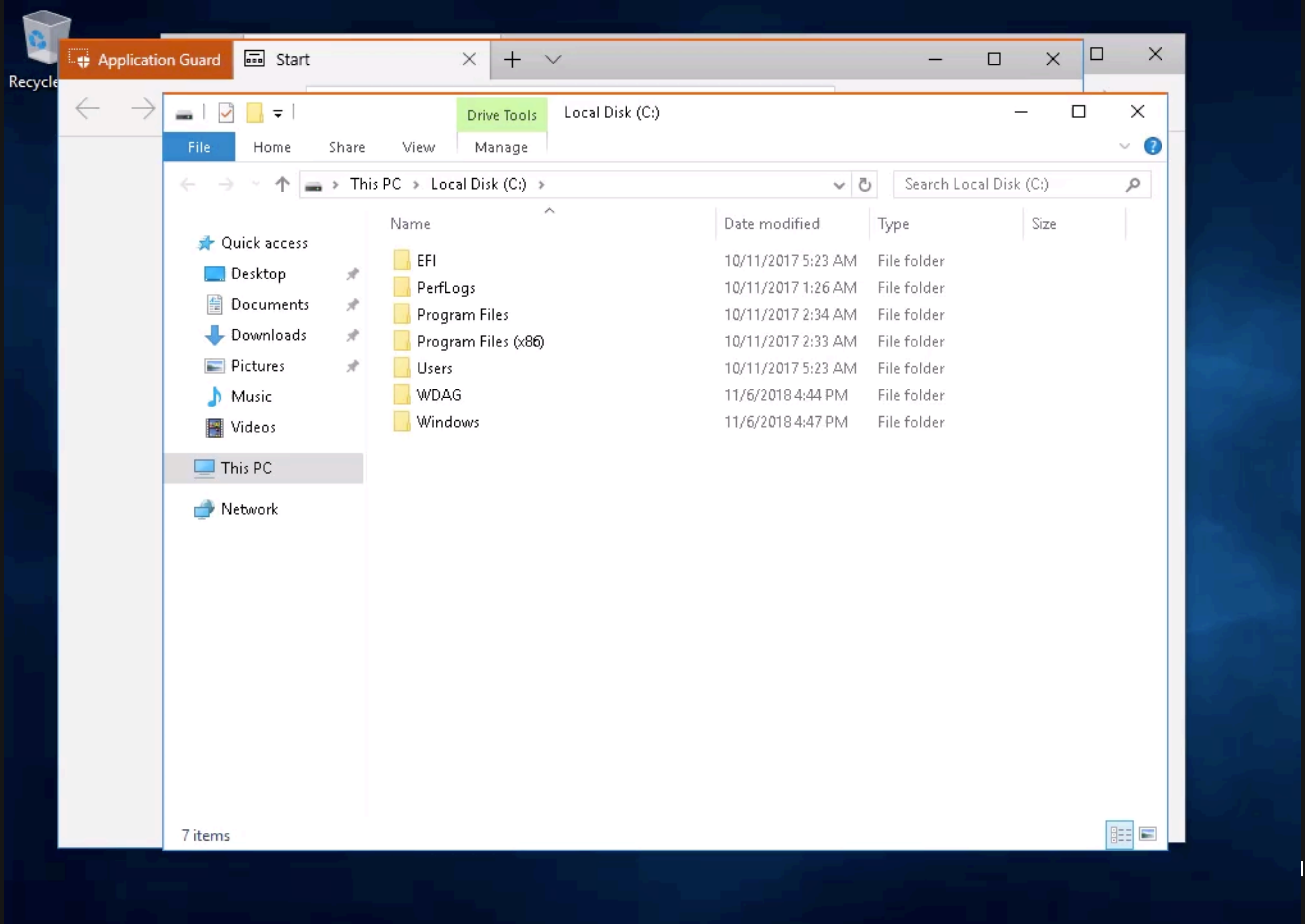
- Step 1: Launch File Explorer in WDAG


Recycle Bin
New tab
Search or enter web address
Show top sites | Show top sites and my feed

Reform WDAG for Research

Step 2: Modify Device Guard Rule

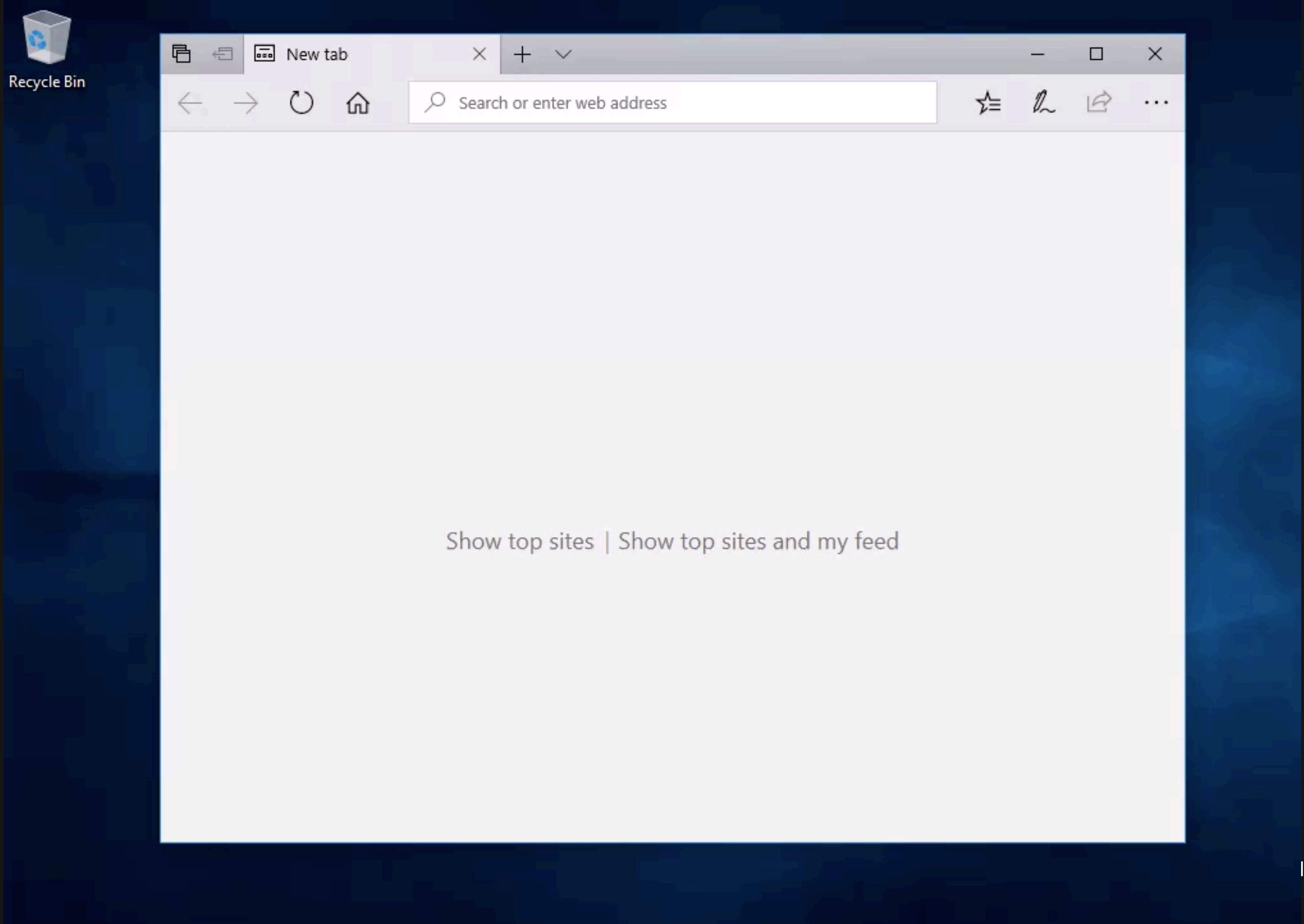
- WDAG deploy a very strict rule inside the container
  - UMCI is enabled
  - Only Microsoft Signers are allowed
  - 171 files are explicitly denied
    - cmd.Exe
    - CONTROL.EXE
    - mmc.exe
    - netsh.exe
    - regedit.exe
    - windbg.Exe
    - wmic.exe
    - wscript.exe
    - ...



Name	Date modified	Type	Size
EFI	10/11/2017 5:23 AM	File folder	
PerfLogs	10/11/2017 1:26 AM	File folder	
Program Files	10/11/2017 2:34 AM	File folder	
Program Files (x86)	10/11/2017 2:33 AM	File folder	
Users	10/11/2017 5:23 AM	File folder	
WDAG	11/6/2018 4:44 PM	File folder	
Windows	11/6/2018 4:47 PM	File folder	

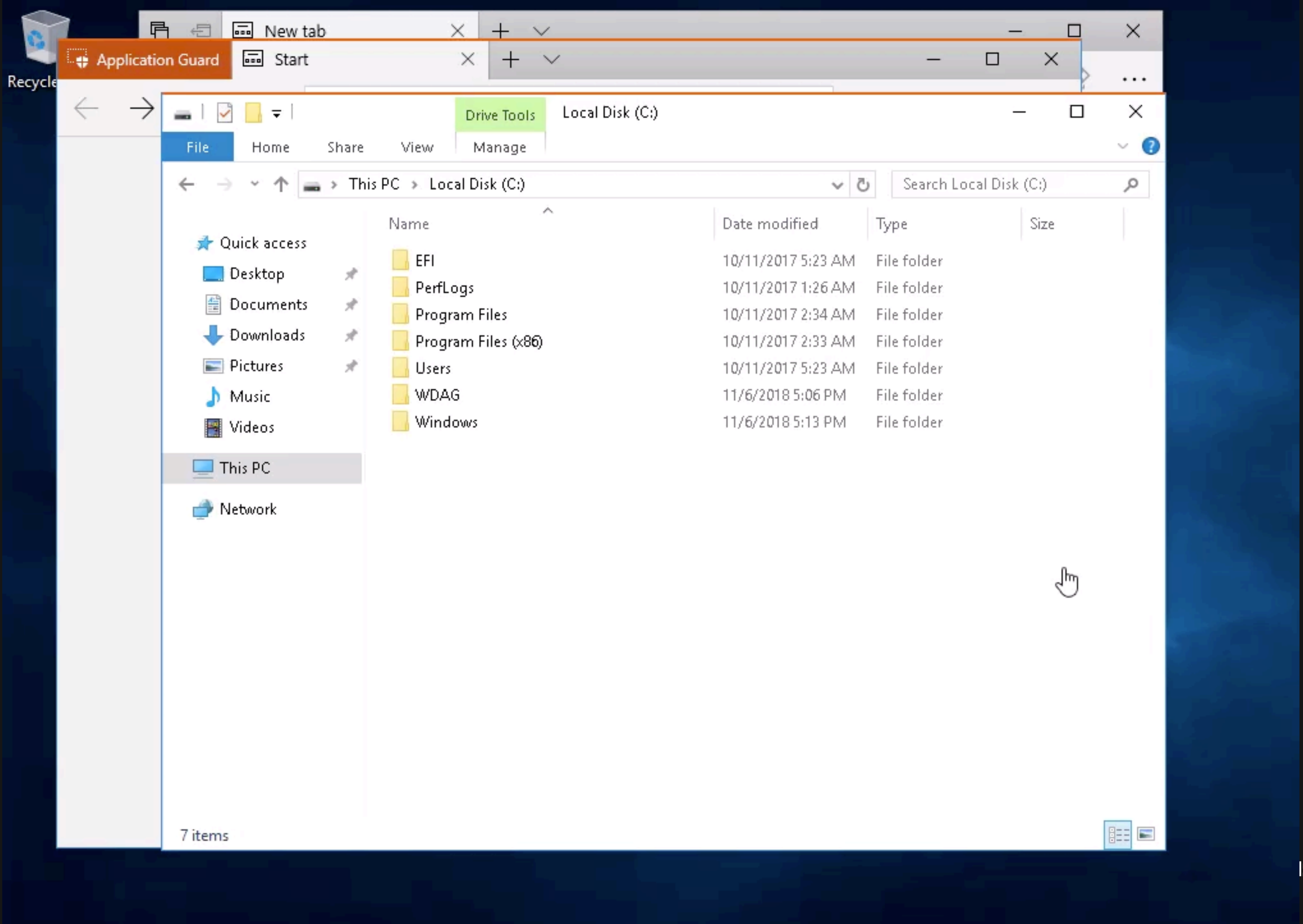
Reform WDAG for Research

- Step 2: Modify Device Guard Rule
  - The policy file can be modified outside the container


Recycle Bin
New tab
Search or enter web address
Show top sites | Show top sites and my feed

Reform WDAG for Research

- Step 3: Install WinDbg



Name	Date modified	Type	Size
EFI	10/11/2017 5:23 AM	File folder	
PerfLogs	10/11/2017 1:26 AM	File folder	
Program Files	10/11/2017 2:34 AM	File folder	
Program Files (x86)	10/11/2017 2:33 AM	File folder	
Users	10/11/2017 5:23 AM	File folder	
WDAG	11/6/2018 5:06 PM	File folder	
Windows	11/6/2018 5:13 PM	File folder	

Reform WDAG for Research

Step 3: Install WinDbg

- We do not have sufficient privileges to install program
  - The logged on user is a normal user
  - The administrator user is disabled

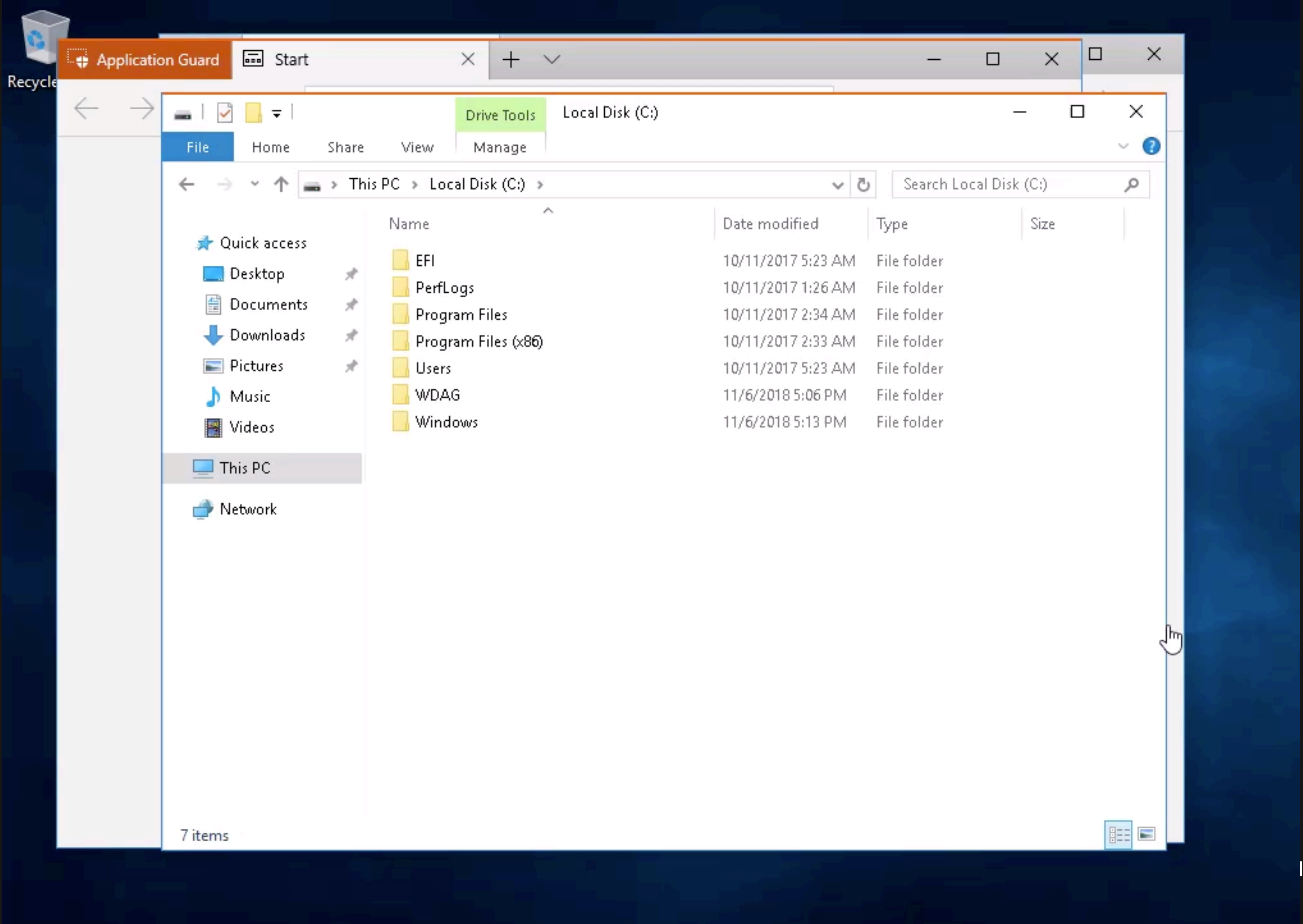
Reform WDAG for Research

Step 3: Install WinDbg

- Exploit an EoP vulnerability

  or

- Copy a installed version into the container

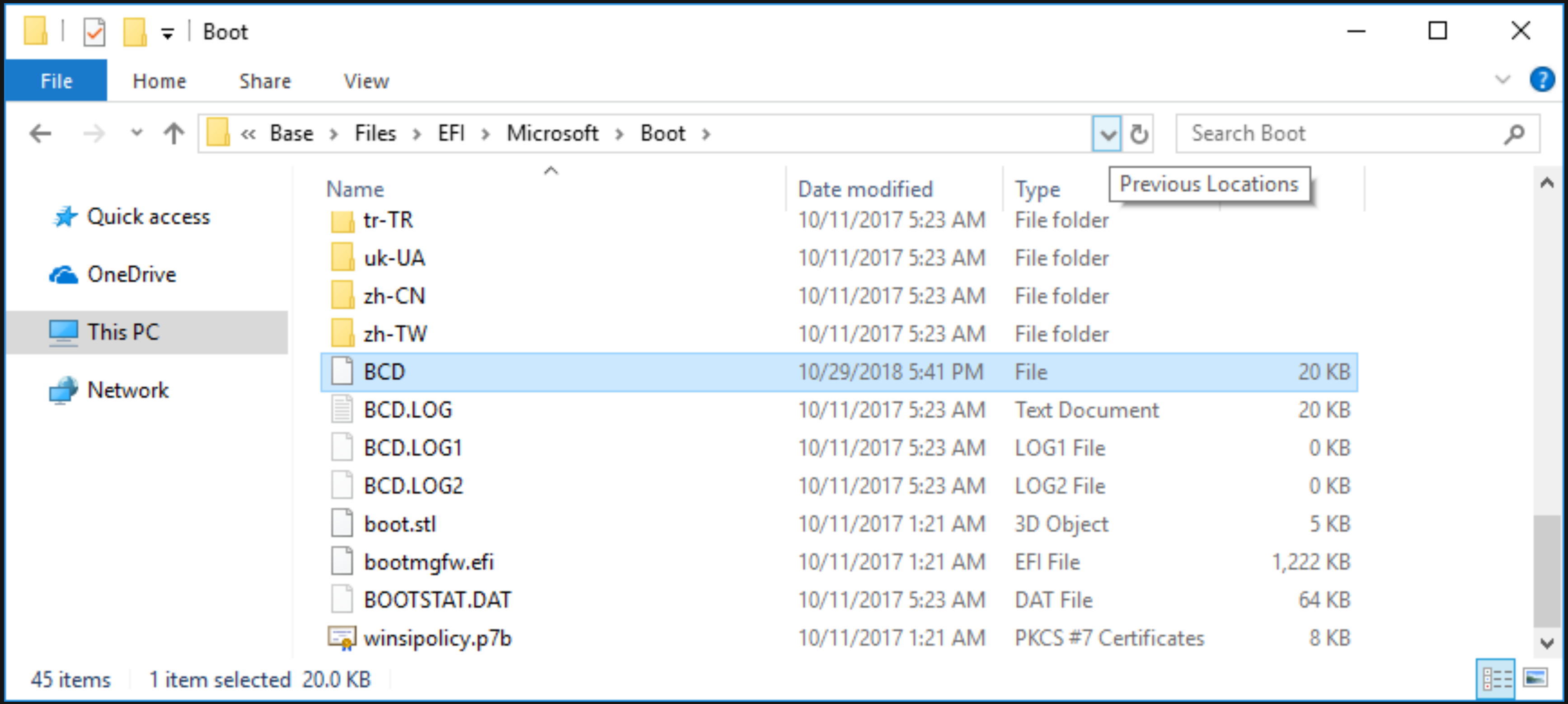


Name	Date modified	Type	Size
EFI	10/11/2017 5:23 AM	File folder	
PerfLogs	10/11/2017 1:26 AM	File folder	
Program Files	10/11/2017 2:34 AM	File folder	
Program Files (x86)	10/11/2017 2:33 AM	File folder	
Users	10/11/2017 5:23 AM	File folder	
WDAG	11/6/2018 5:06 PM	File folder	
Windows	11/6/2018 5:13 PM	File folder	

Reform WDAG for Research

Step 4: Setting Up Kernel Debugging

- Edit BCD store of the container



Name	Date modified	Type	Size
tr-TR	10/11/2017 5:23 AM	File folder	
uk-UA	10/11/2017 5:23 AM	File folder	
zh-CN	10/11/2017 5:23 AM	File folder	
zh-TW	10/11/2017 5:23 AM	File folder	
BCD	10/29/2018 5:41 PM	File	20 KB
BCD.LOG	10/11/2017 5:23 AM	Text Document	20 KB
BCD.LOG1	10/11/2017 5:23 AM	LOG1 File	0 KB
BCD.LOG2	10/11/2017 5:23 AM	LOG2 File	0 KB
boot.stl	10/11/2017 1:21 AM	3D Object	5 KB
bootmgfw.efi	10/11/2017 1:21 AM	EFI File	1,222 KB
BOOTSTAT.DAT	10/11/2017 5:23 AM	DAT File	64 KB
winsipolicy.p7b	10/11/2017 1:21 AM	PKCS #7 Certificates	8 KB

45 items 1 item selected 20.0 KB

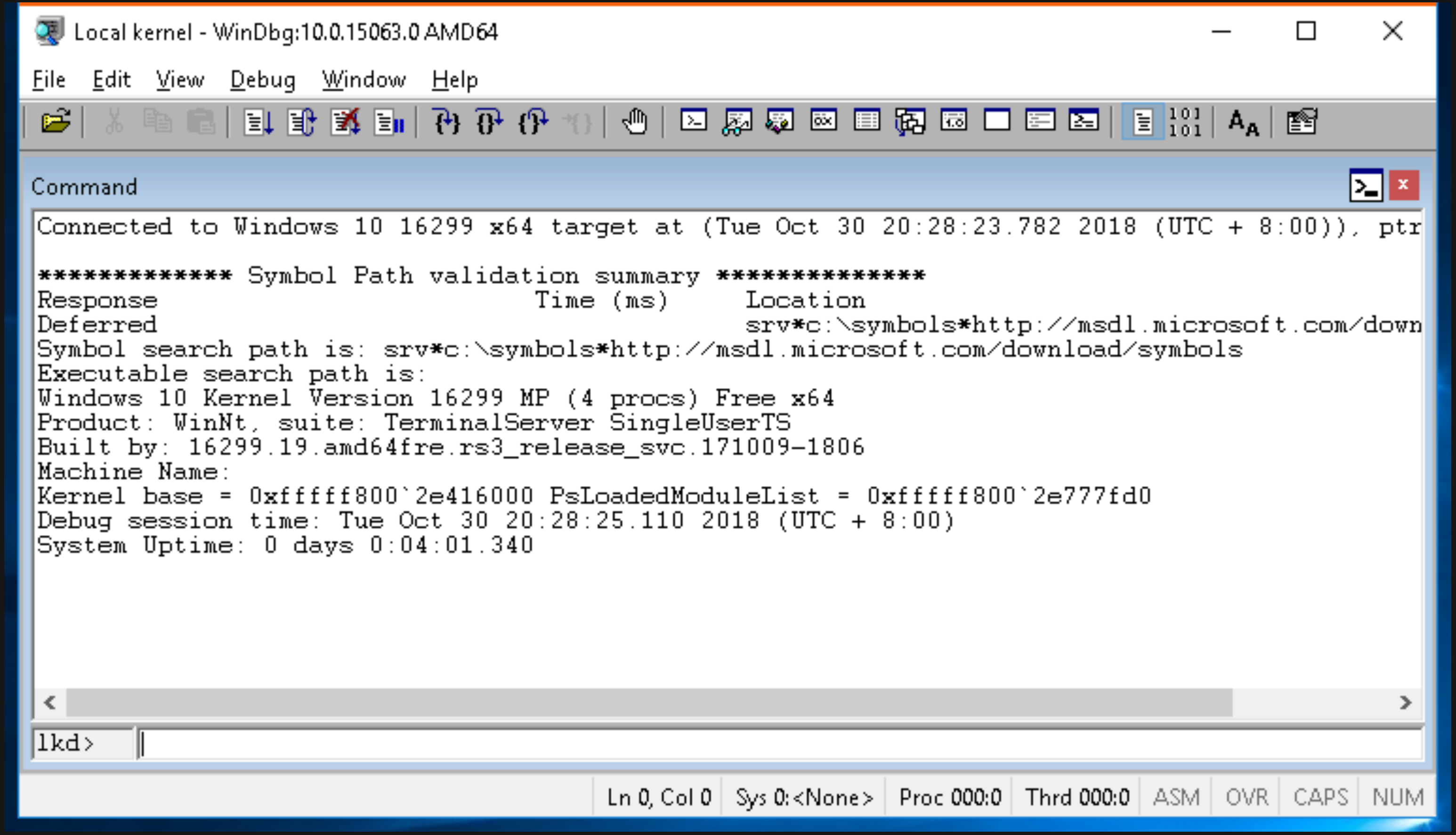
Reform WDAG for Research

Step 4: Setting Up Kernel Debugging

- Currently only local debugging is possible
  - No COM port or USB or 1394
  - Network connection is restricted

Reform WDAG for Research

- Step 4: Setting Up Kernel Debugging

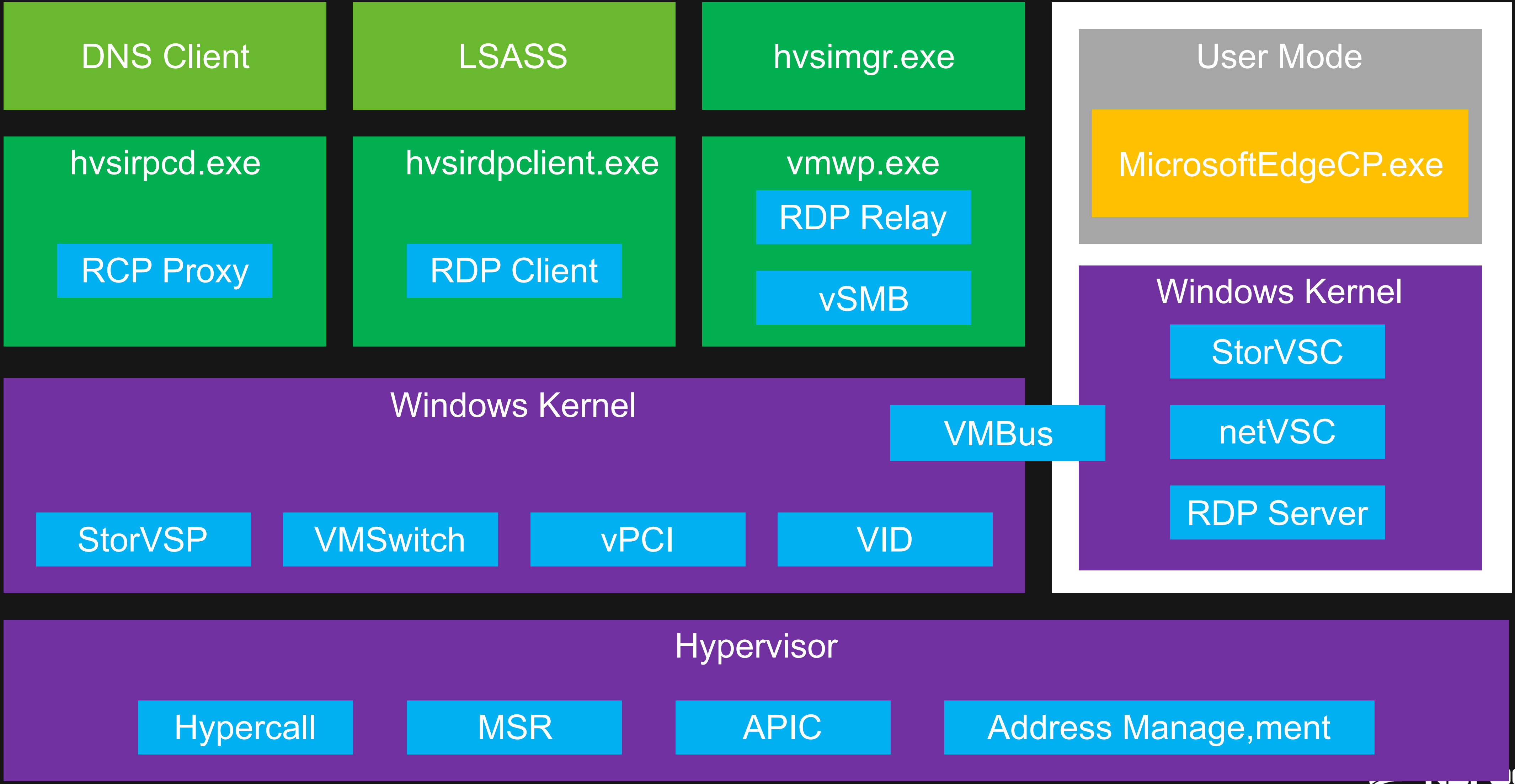


Local kernel - WinDbg:10.0.15063.0 AMD64
File Edit View Debug Window Help
Command
Ln 0, Col 0
Sys 0:<None>
Proc 000:0
Thrd 000:0
ASM
OVR
CAPS
NUM

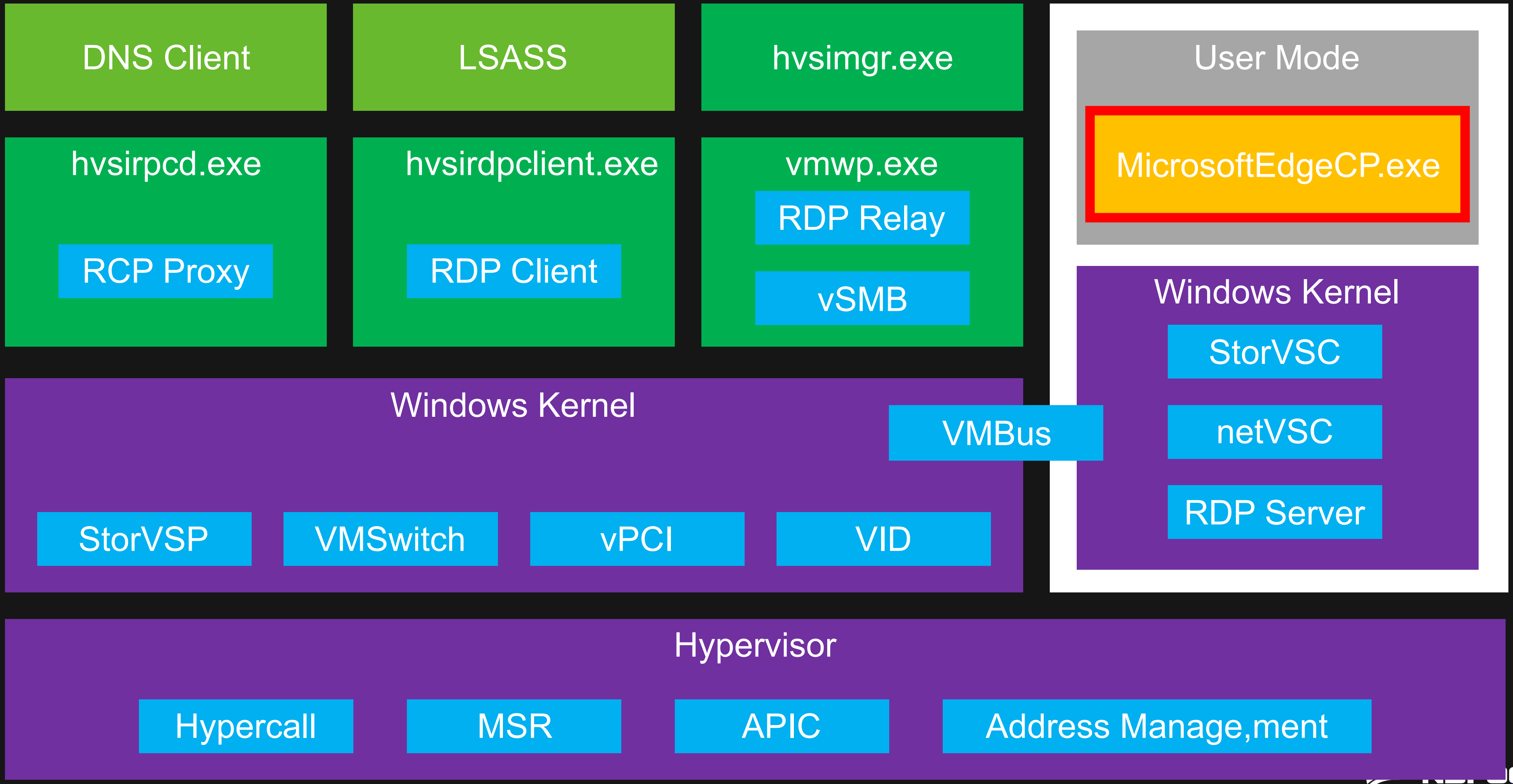
```
Connected to Windows 10 16299 x64 target at (Tue Oct 30 20:28:23.782 2018 (UTC + 8:00)), ptr

************* Symbol Path validation summary **************
Response                         Time (ms)     Location
Deferred                                       srv*c:\symbols*http://msdl.microsoft.com/down
Symbol search path is: srv*c:\symbols*http://msdl.microsoft.com/download/symbols
Executable search path is:
Windows 10 Kernel Version 16299 MP (4 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Built by: 16299.19.amd64fre.rs3_release_svc.171009-1806
Machine Name:
Kernel base = 0xfffff800`2e416000 PsLoadedModuleList = 0xfffff800`2e777fd0
Debug session time: Tue Oct 30 20:28:25.110 2018 (UTC + 8:00)
System Uptime: 0 days 0:04:01.340
```

```
lkd>
```

WDAG Attack Surface



WDAG Attack Surface



DNS Client

LSASS

hvsimgr.exe

User Mode

MicrosoftEdgeCP.exe

hvsirpcd.exe

RCP Proxy

hvsirdpclient.exe

RDP Client

vmwp.exe

RDP Relay

vSMB

Windows Kernel

StorVSC

netVSC

RDP Server

Windows Kernel

VMBus

StorVSP

VMSwitch

vPCI

VID

Hypervisor

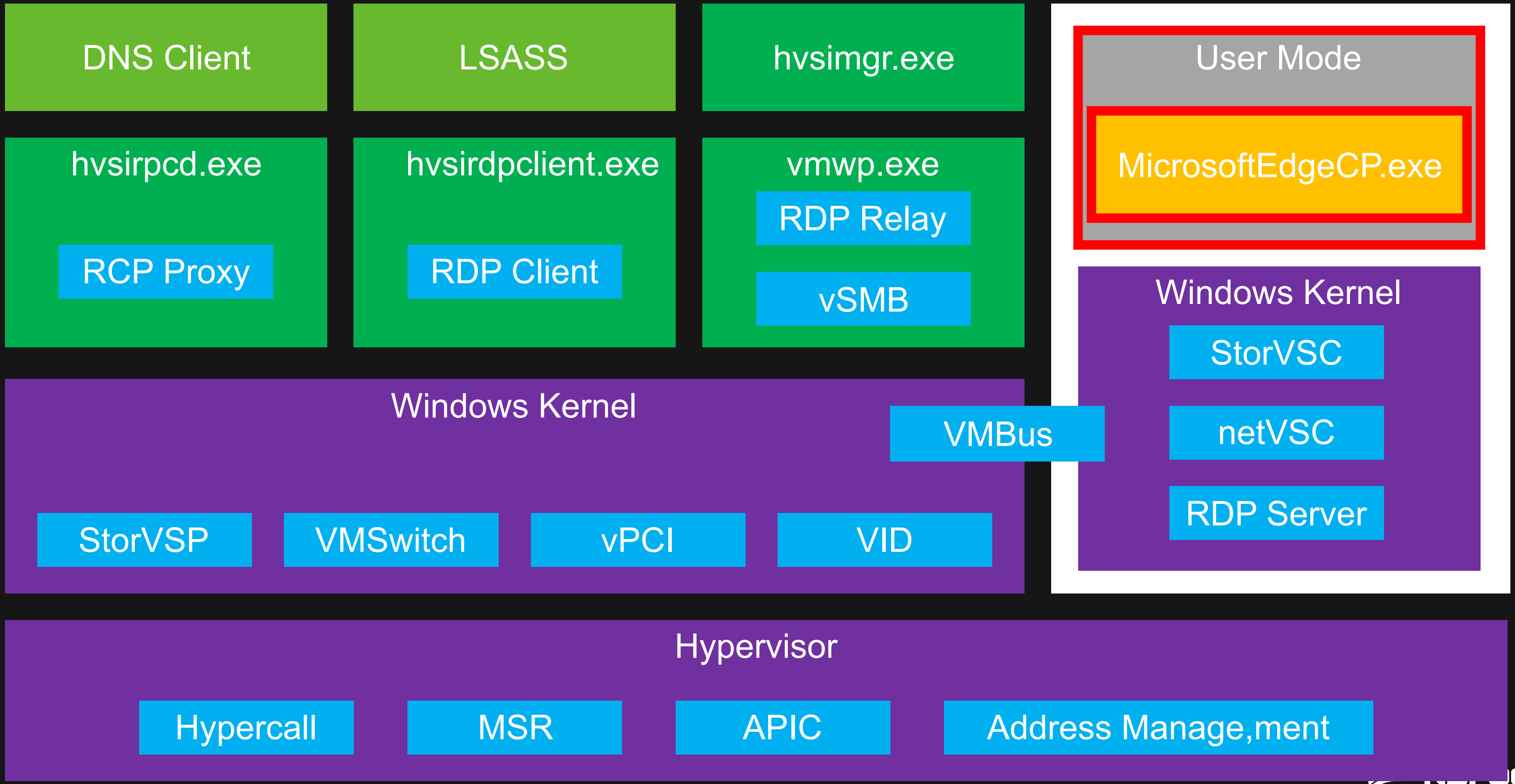
Hypercall

MSR

APIC

Address Manage,ment

WDAG Attack Surface



DNS Client

LSASS

hvsimgr.exe

User Mode

MicrosoftEdgeCP.exe

hvsirpcd.exe

RCP Proxy

hvsirdpclient.exe

RDP Client

vmwp.exe

RDP Relay

vSMB

Windows Kernel

StorVSC

netVSC

RDP Server

Windows Kernel

VMBus

StorVSP

VMSwitch

vPCI

VID

Hypervisor

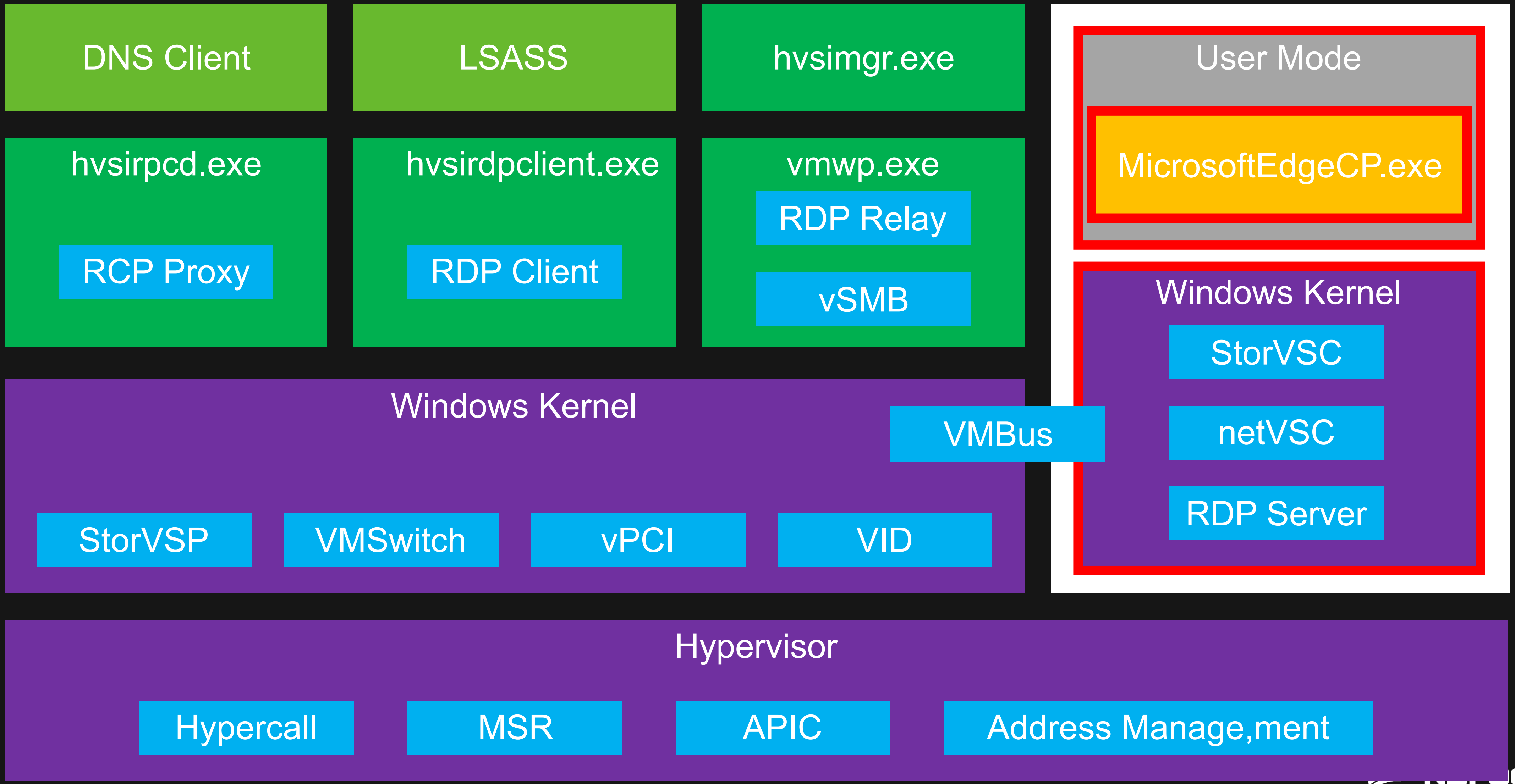
Hypercall

MSR

APIC

Address Manage,ment

WDAG Attack Surface



DNS Client

LSASS

hvsimgr.exe

hvsirpcd.exe

RCP Proxy

hvsirdpclient.exe

RDP Client

vmwp.exe

RDP Relay

vSMB

Windows Kernel

VMBus

StorVSP

VMSwitch

vPCI

VID

User Mode

MicrosoftEdgeCP.exe

Windows Kernel

StorVSC

netVSC

RDP Server

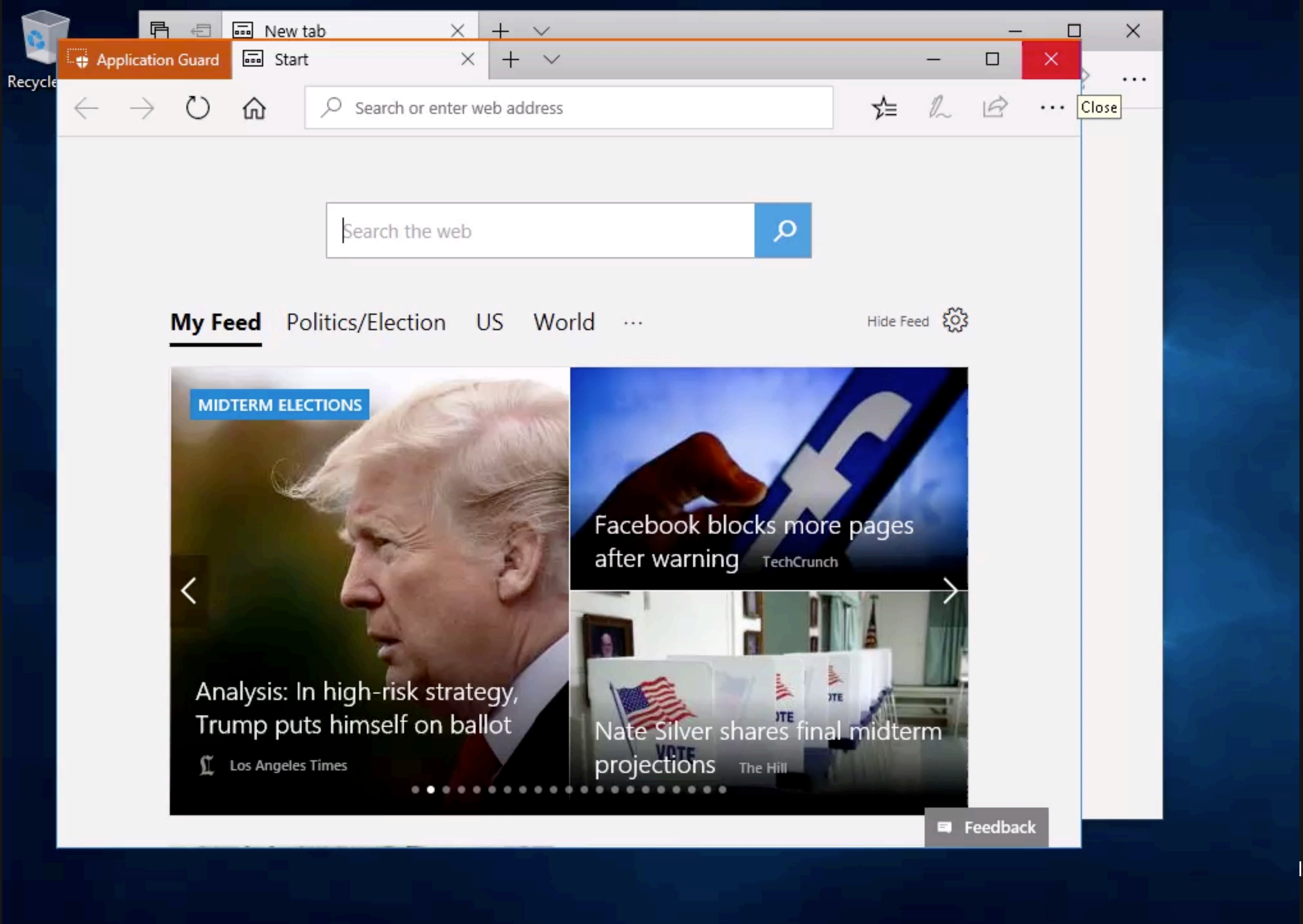
Hypervisor

Hypercall

MSR

APIC

Address Manage,ment

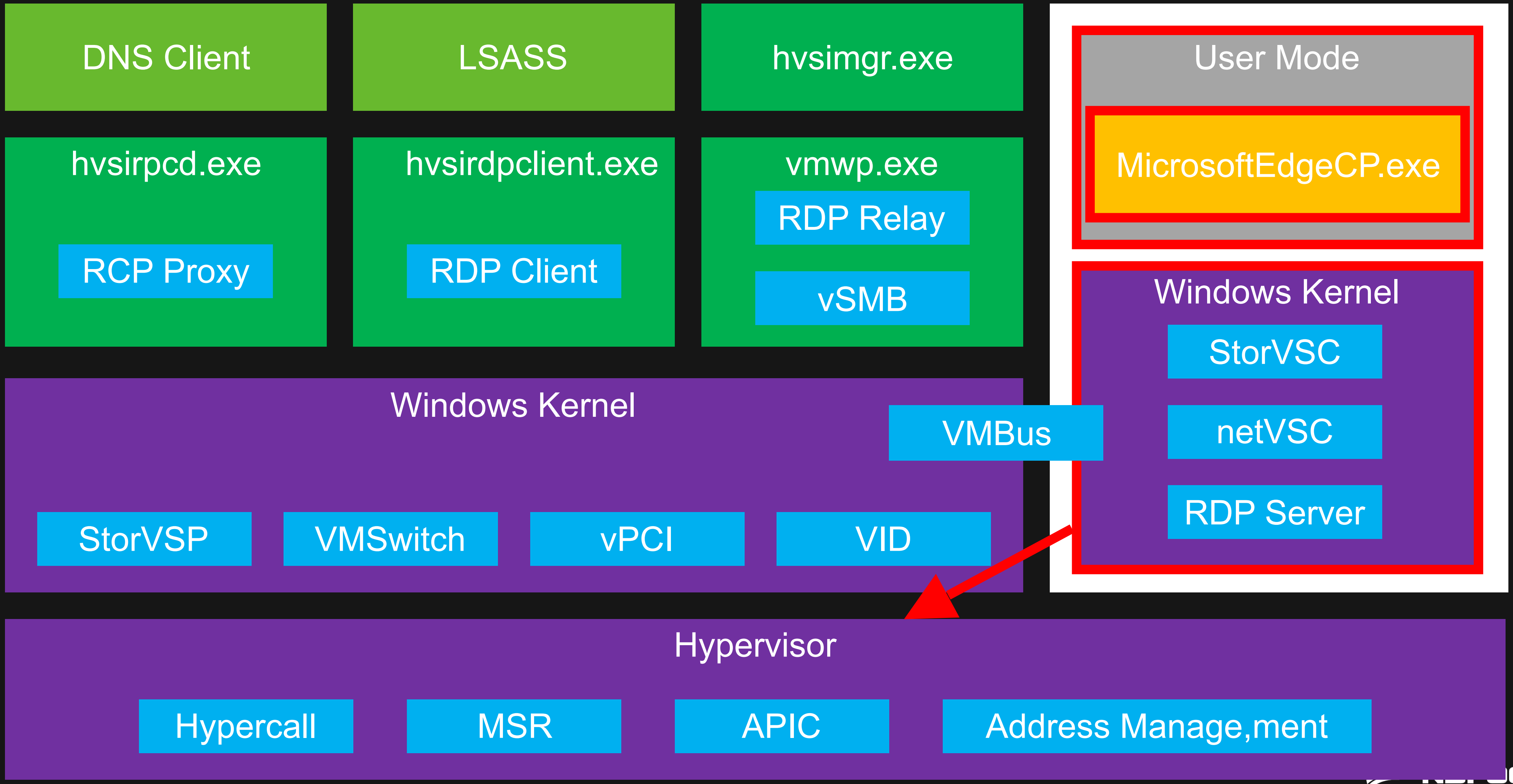


Analysis: In high-risk strategy, Trump puts himself on ballot Los Angeles Times

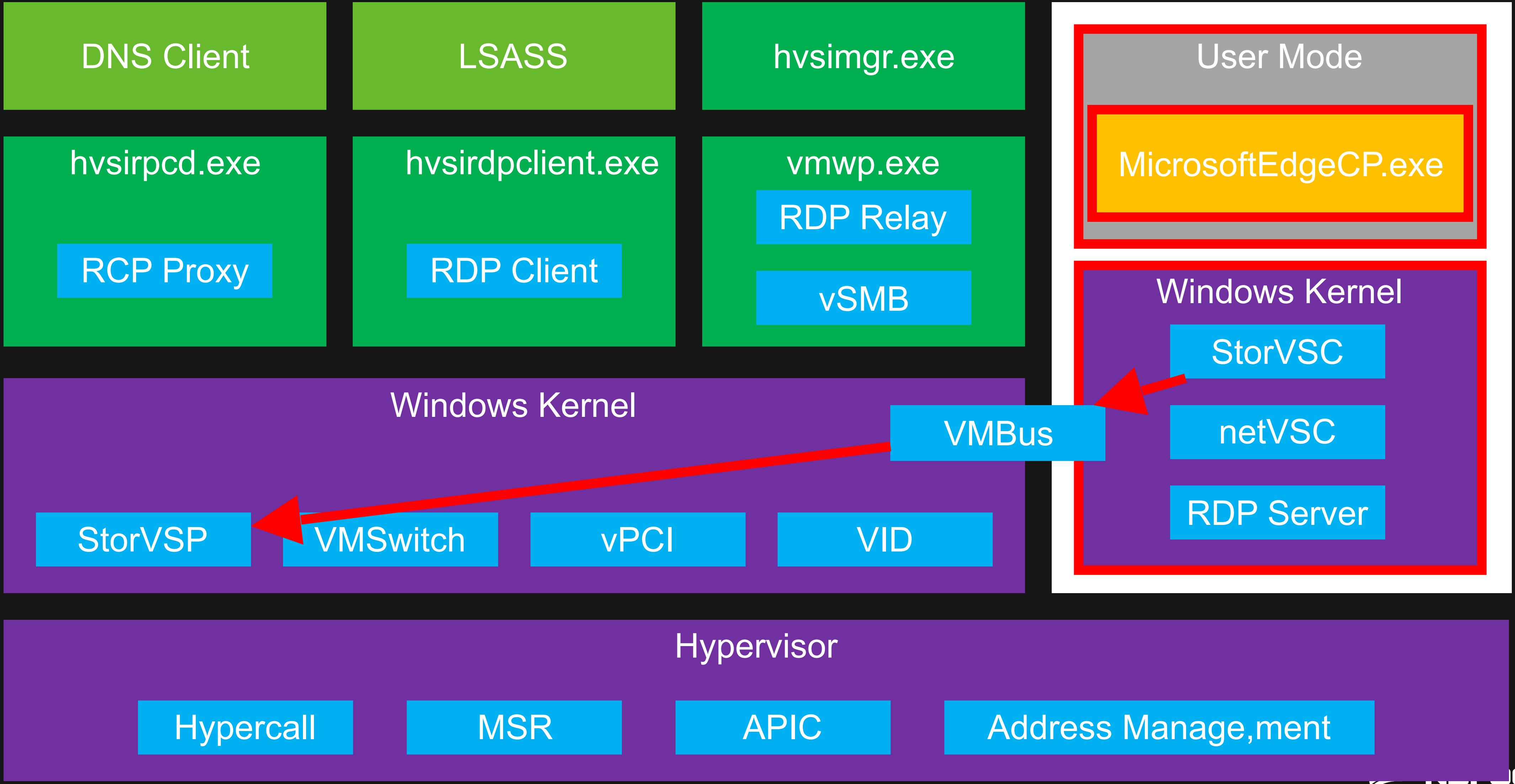
Facebook blocks more pages after warning TechCrunch

Nate Silver shares final midterm projections The Hill

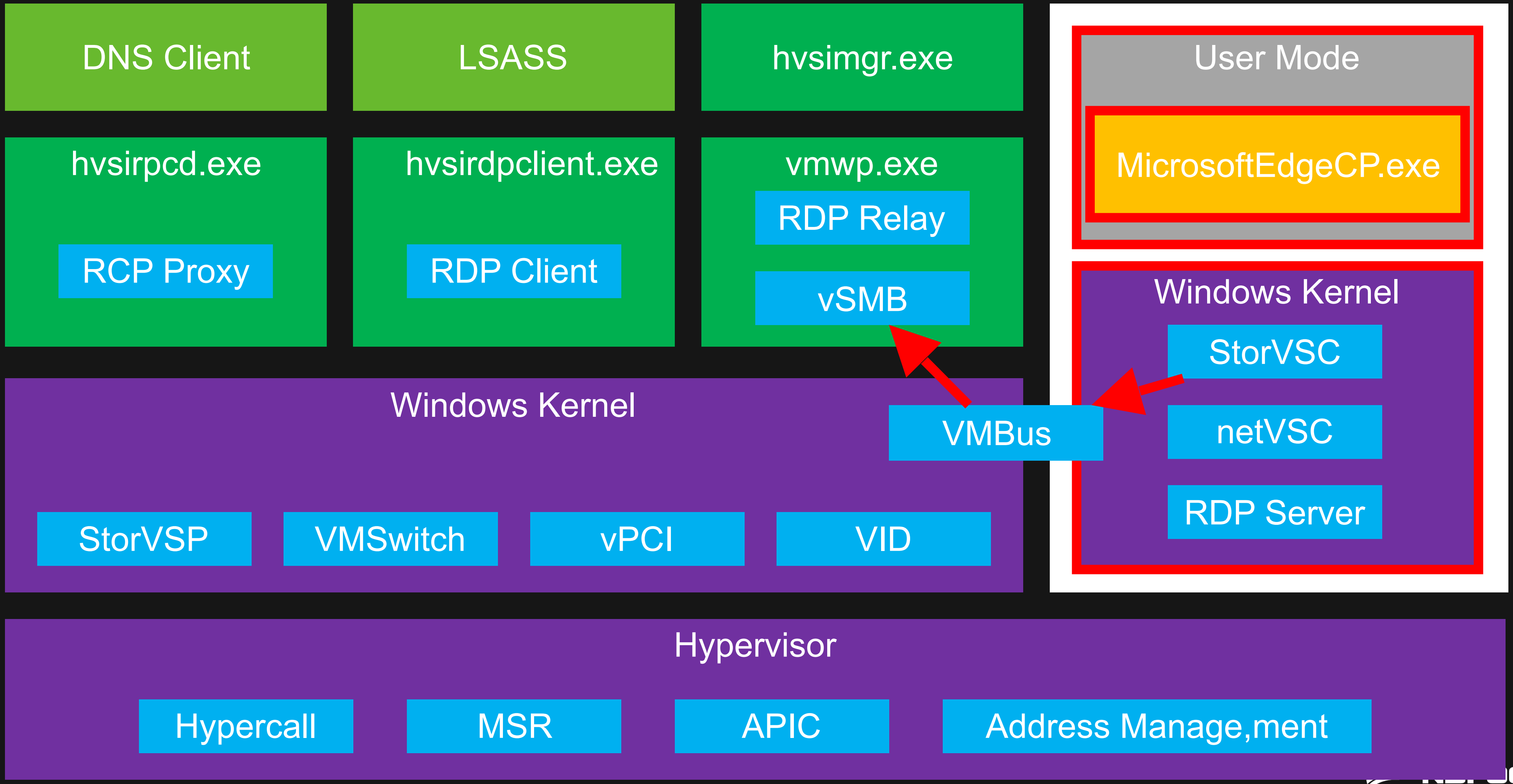
WDAG Attack Surface



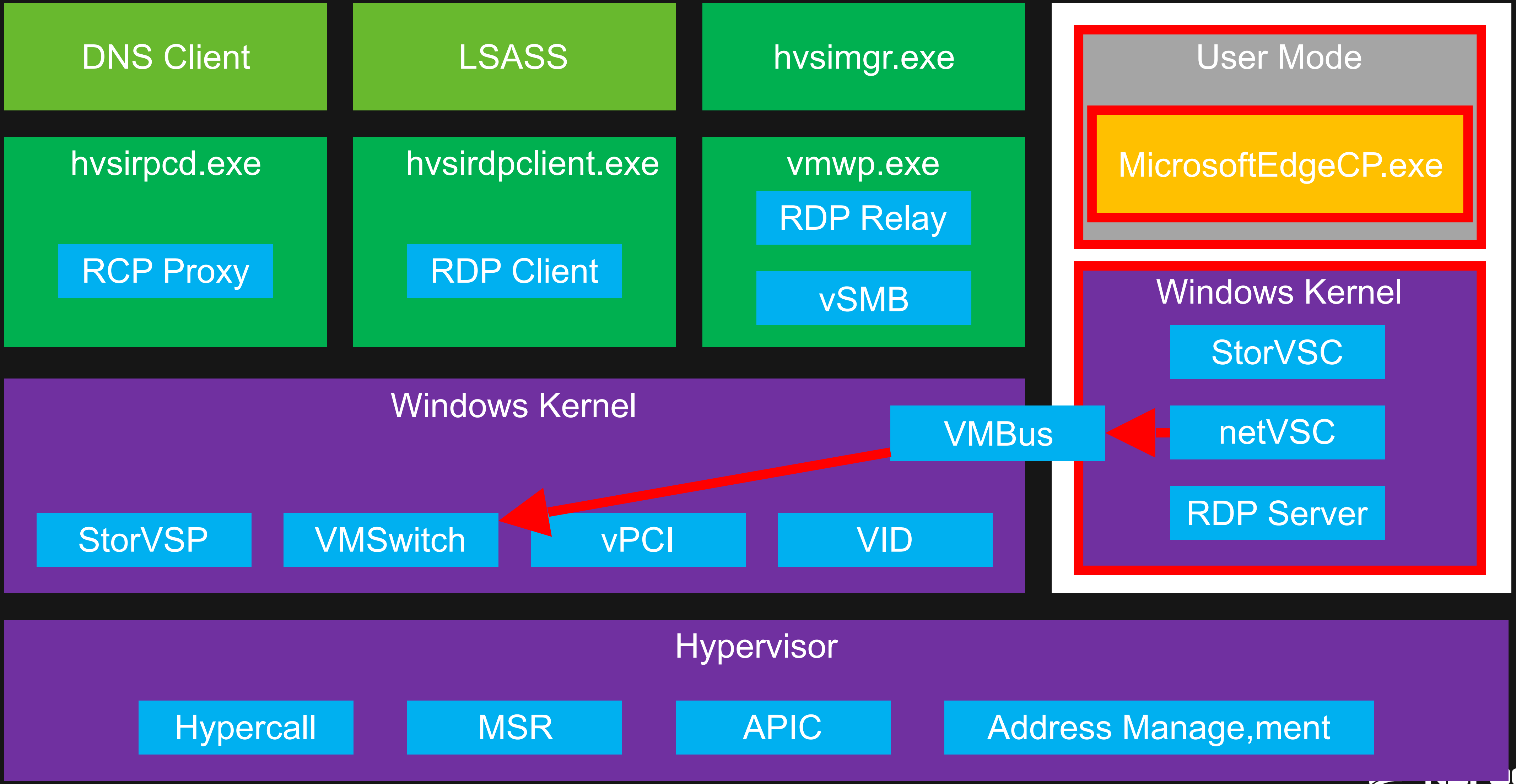
WDAG Attack Surface



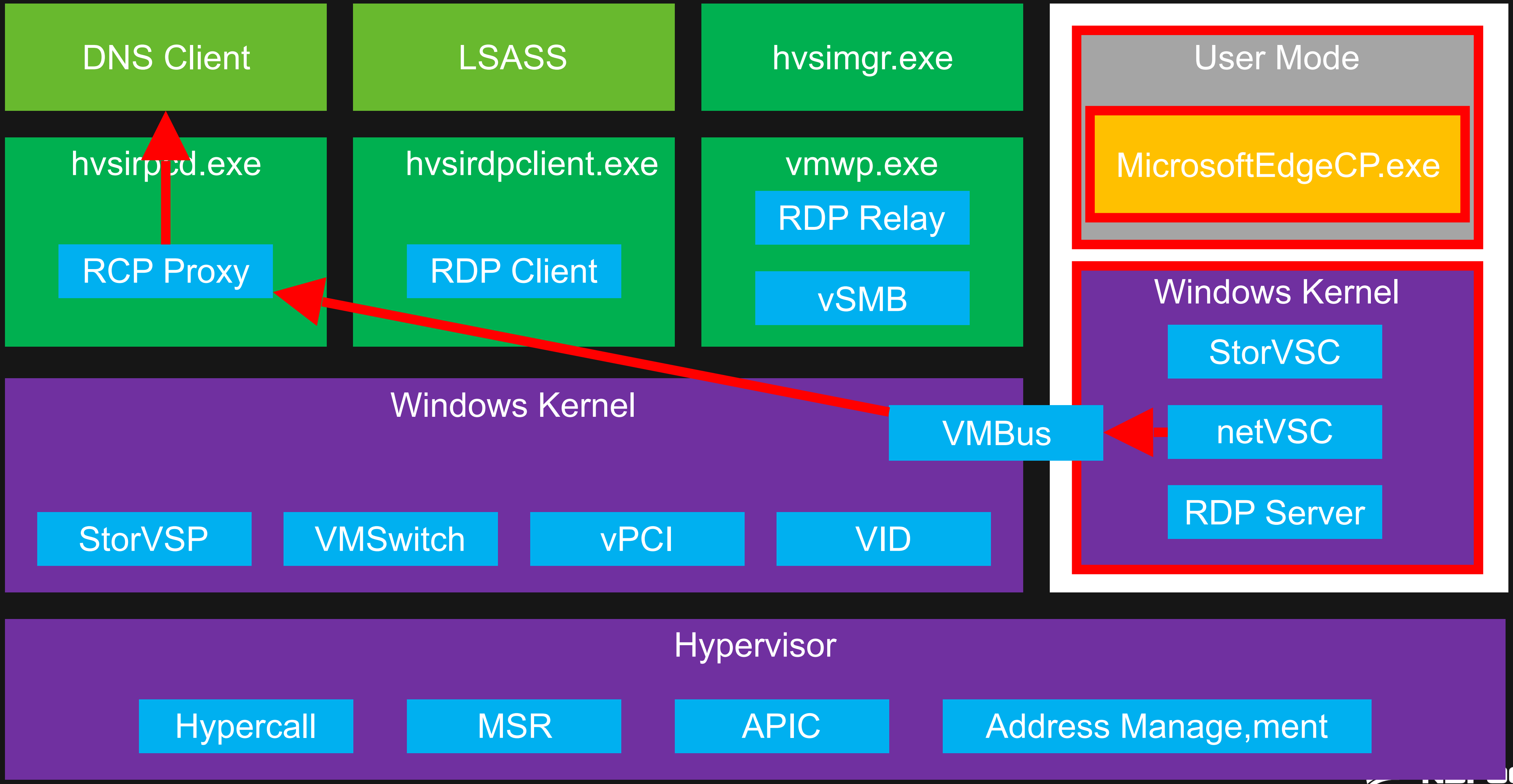
WDAG Attack Surface



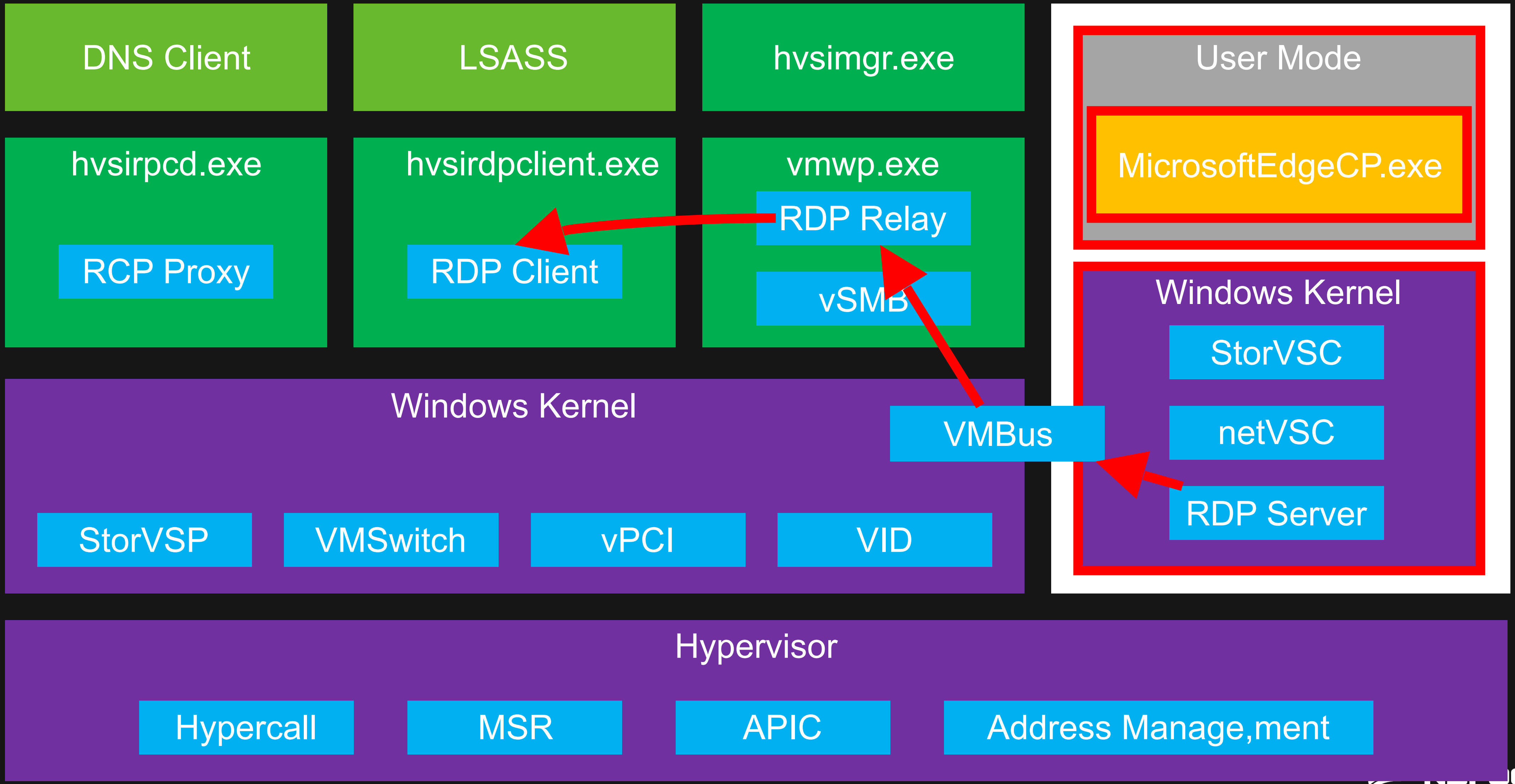
WDAG Attack Surface



WDAG Attack Surface



WDAG Attack Surface



Q&A

Thanks!

NSFOCUS