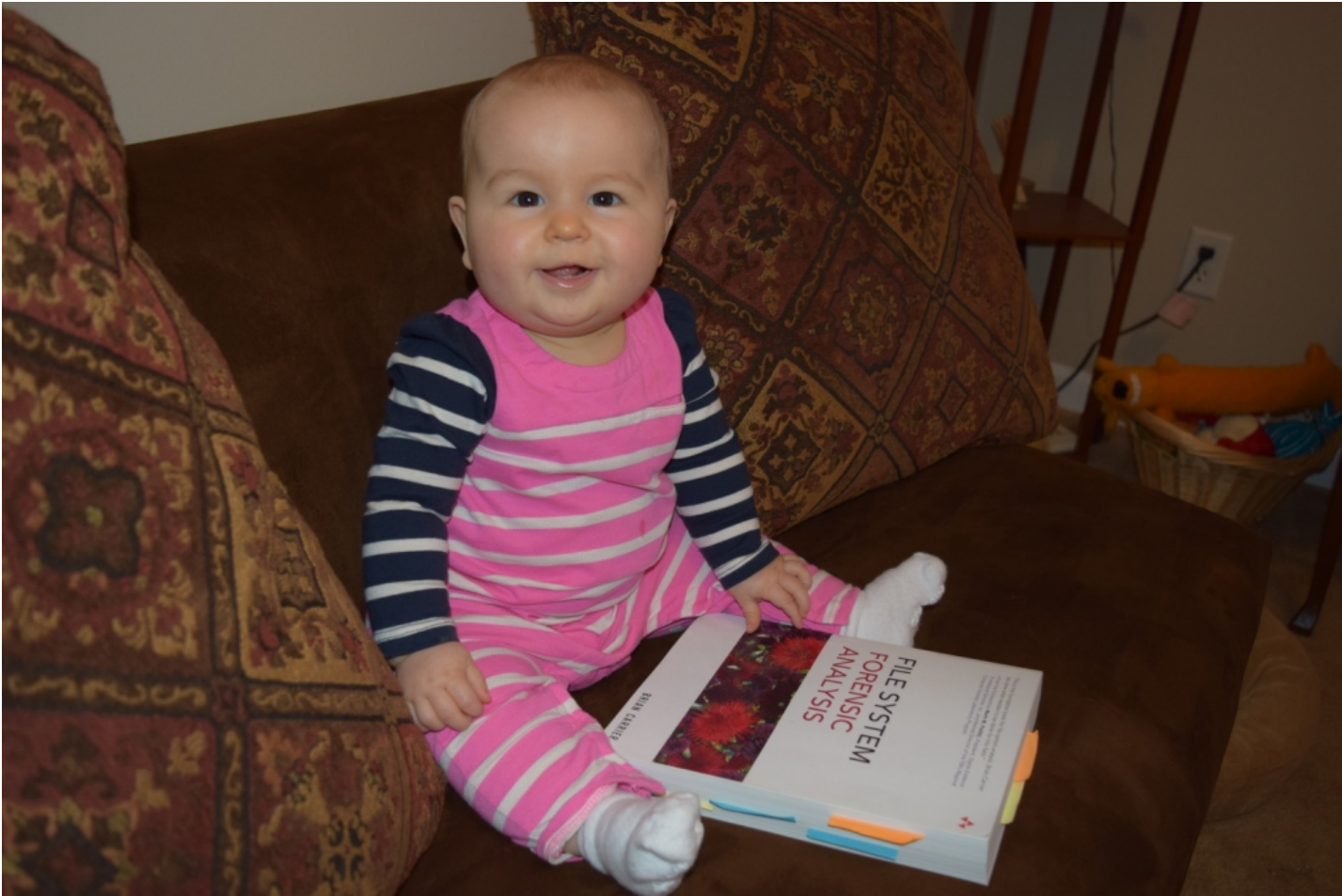


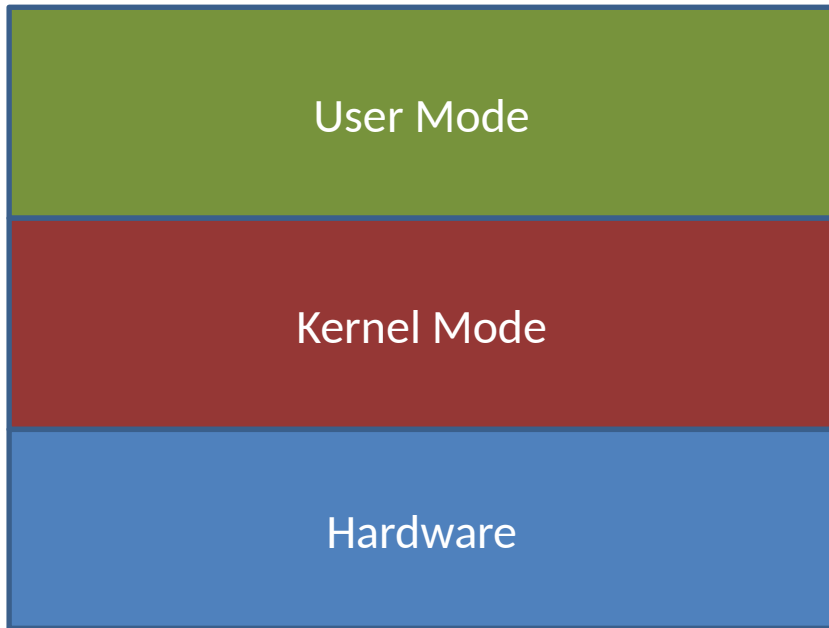
Virtualization-Based Security: A Forensics Perspective

August 7, 2017

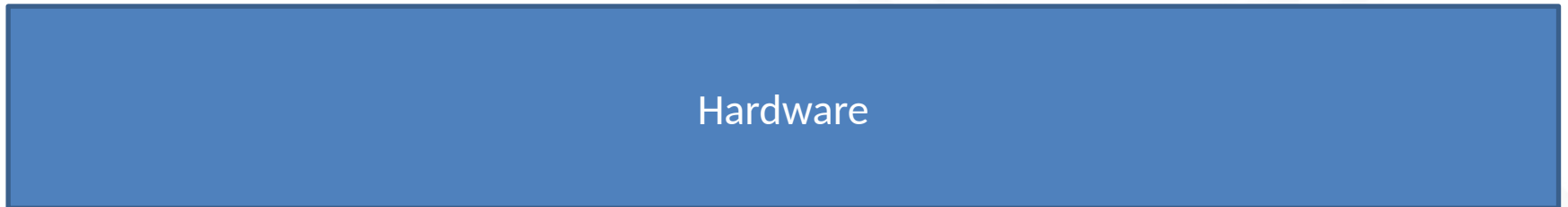
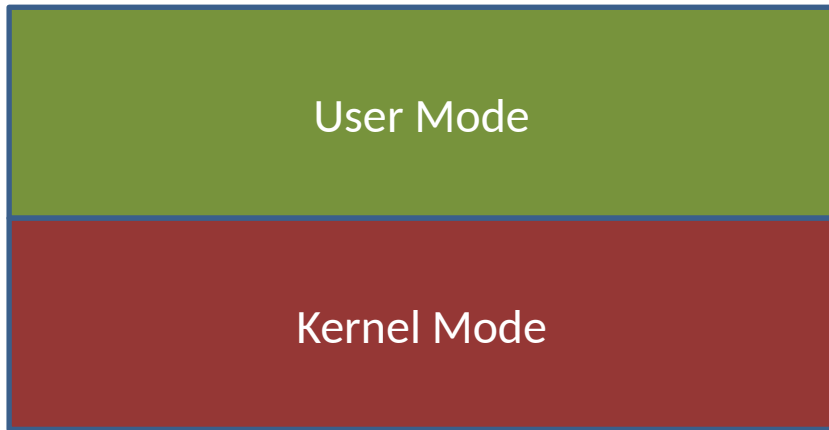
Jason Hale, MSc, CCE, GCFA
One Source Discovery



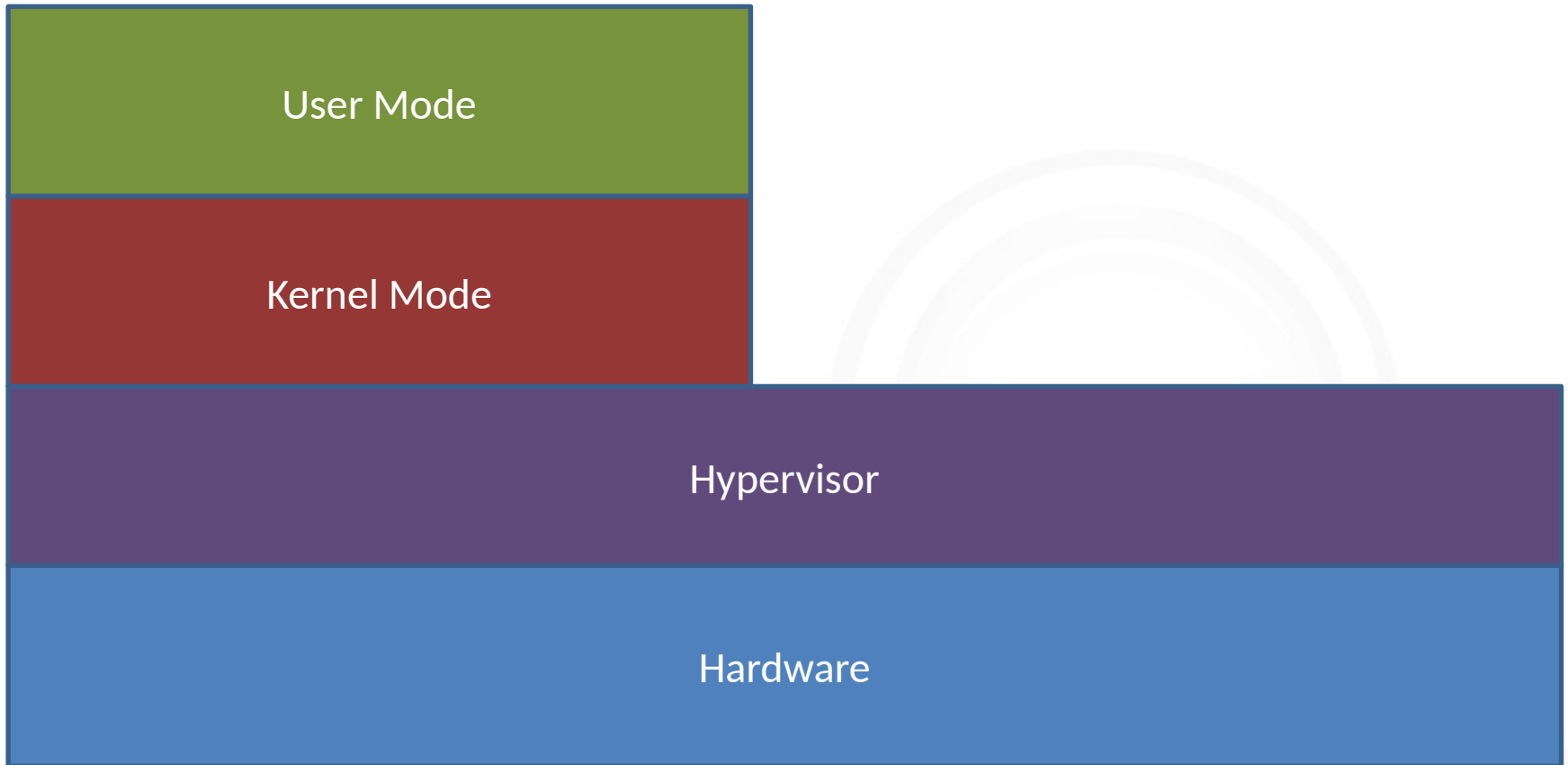
Windows 10 VBS/VSM



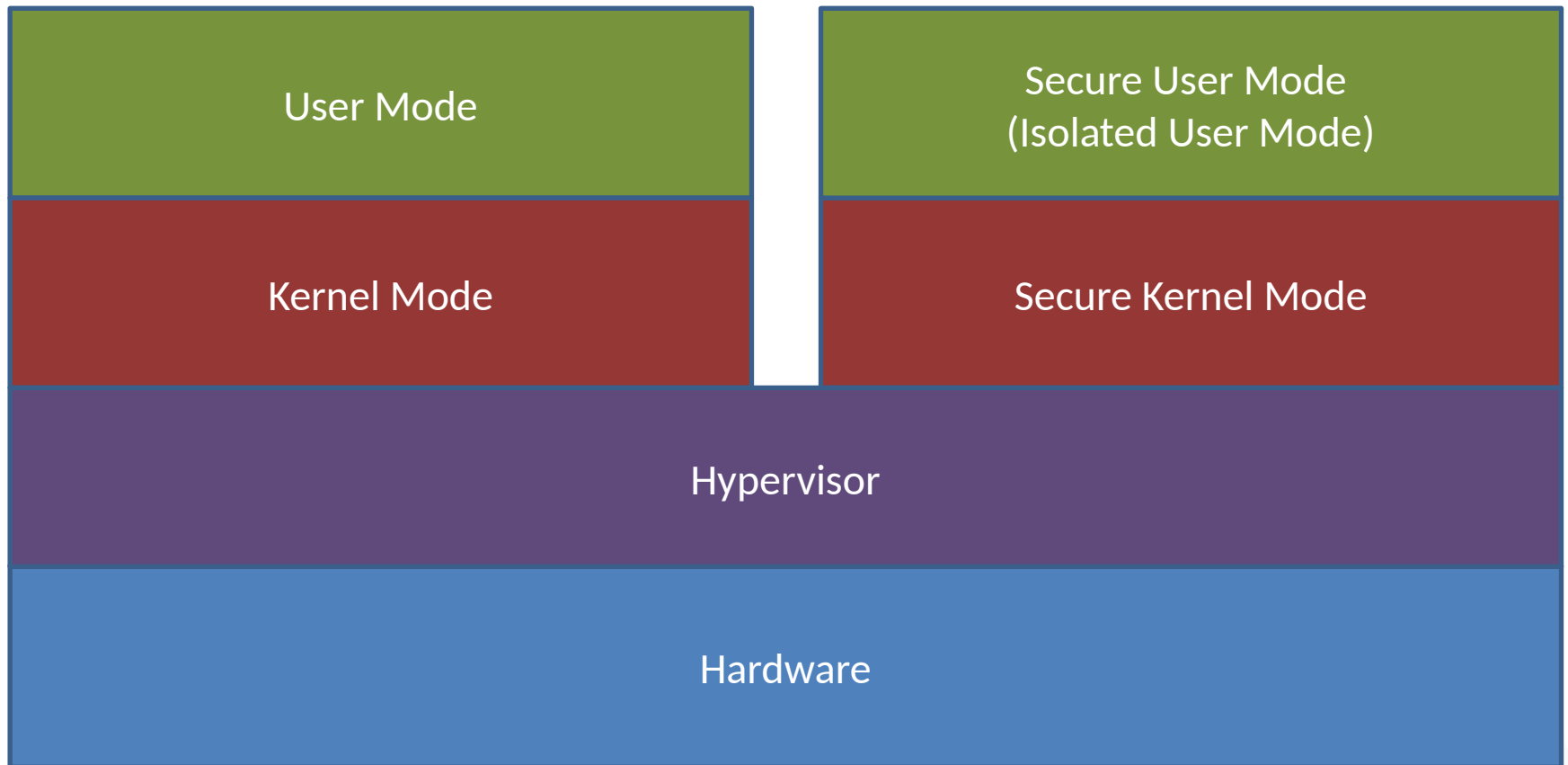
Windows 10 VBS/VSM



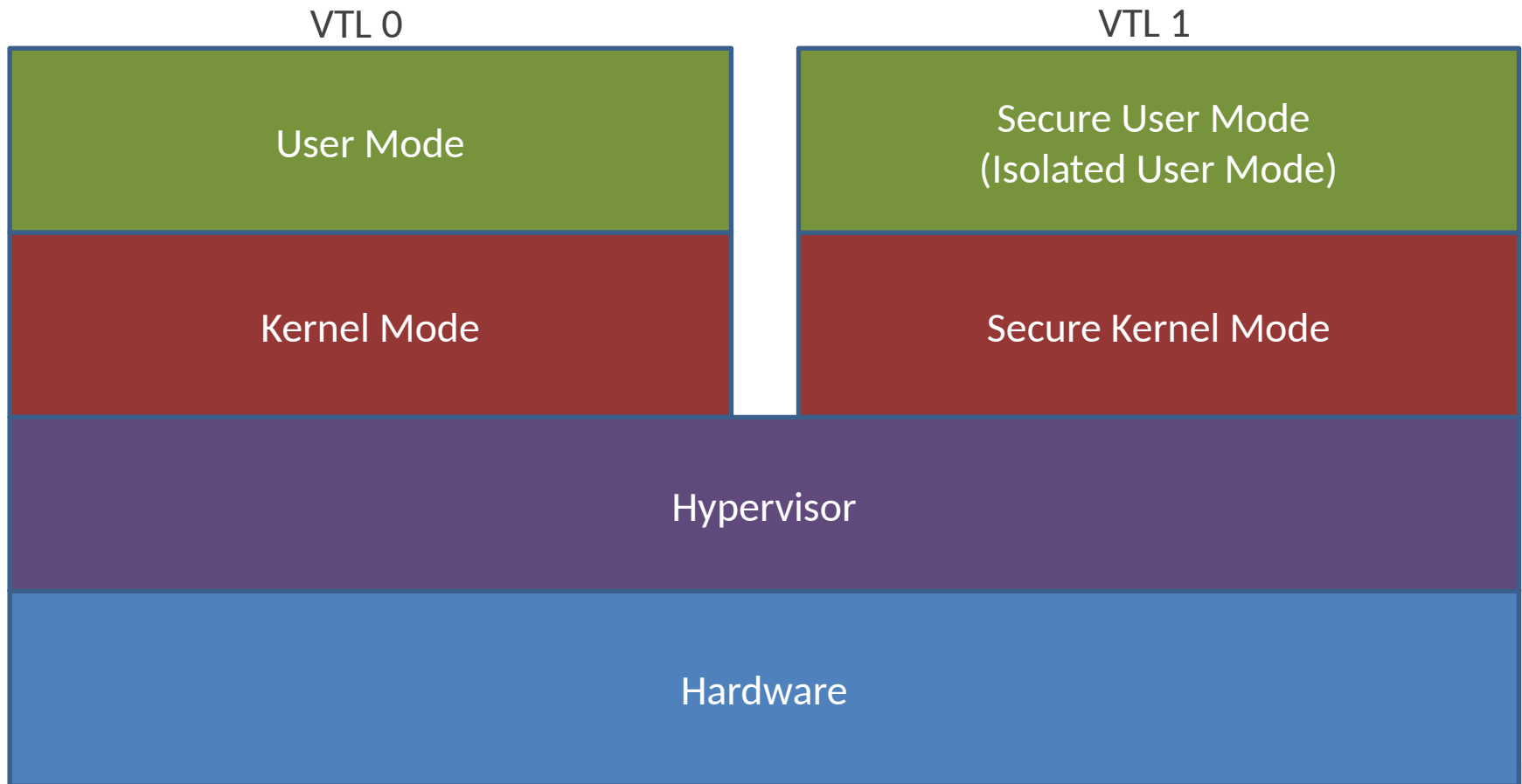
Windows 10 VBS/VSM



Windows 10 VBS/VSM



Windows 10 VBS/VSM



Technologies Using VBS

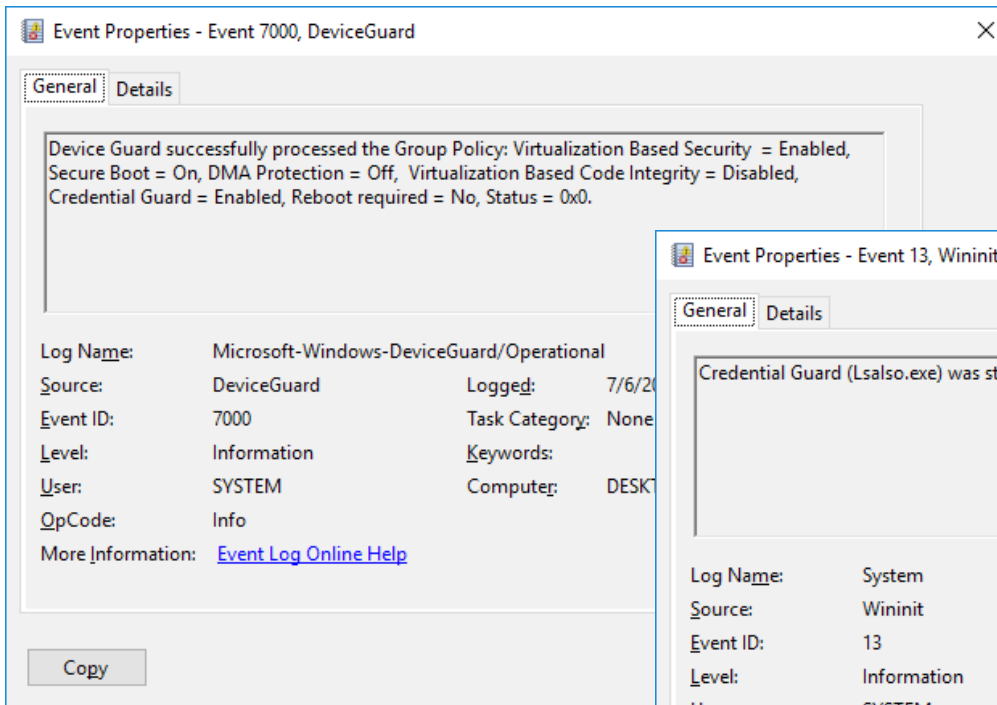
- Credential Guard
- Device Guard
- Hyper Guard
- Application Guard
- Exploit Guard
- Host Guardian and Shielded Fabric

GUARD ALL THE THINGS



VBS and Disk Forensics

System, Security, DeviceGuard event log



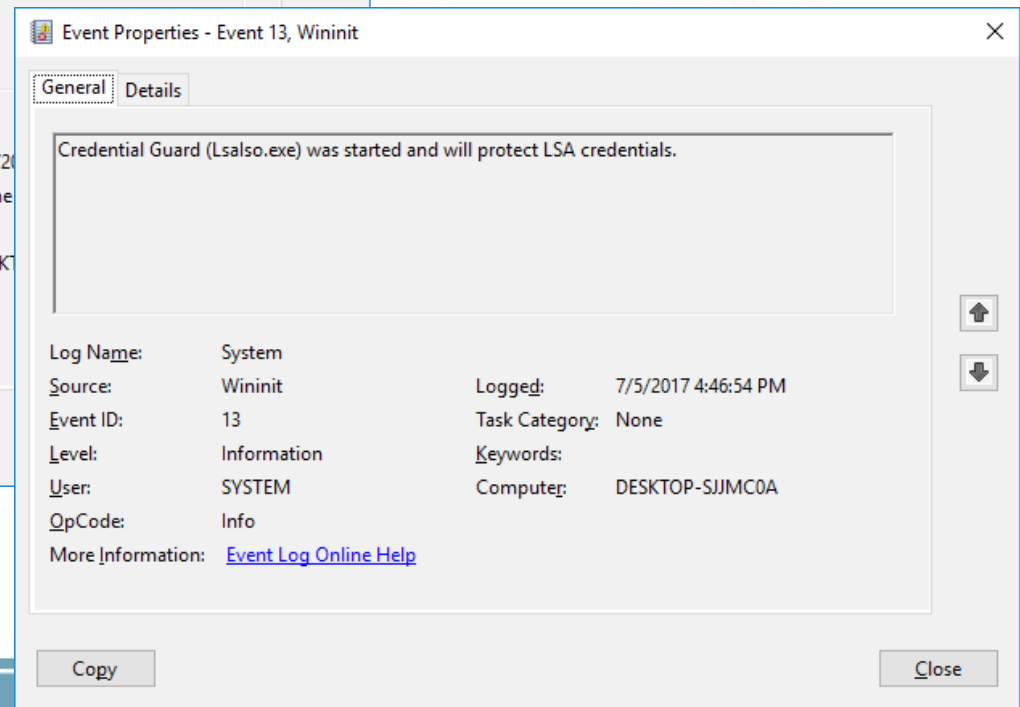
Event Properties - Event 7000, DeviceGuard

General Details

Device Guard successfully processed the Group Policy: Virtualization Based Security = Enabled, Secure Boot = On, DMA Protection = Off, Virtualization Based Code Integrity = Disabled, Credential Guard = Enabled, Reboot required = No, Status = 0x0.

Log Name: Microsoft-Windows-DeviceGuard/Operational
Source: DeviceGuard Logged: 7/6/2017 4:46:54 PM
Event ID: 7000 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-SJJMCOA
OpCode: Info
More Information: [Event Log Online Help](#)

Copy



Event Properties - Event 13, Wininit

General Details

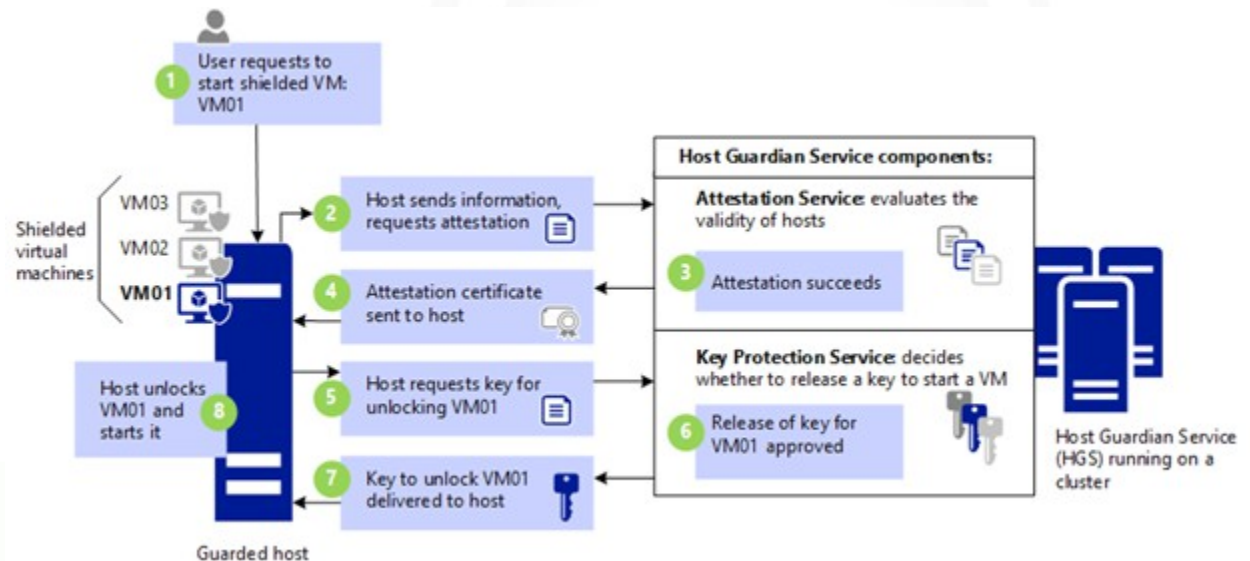
Credential Guard (Lsals.exe) was started and will protect LSA credentials.

Log Name: System
Source: Wininit Logged: 7/5/2017 4:46:54 PM
Event ID: 13 Task Category: None
Level: Information Keywords:
User: SYSTEM Computer: DESKTOP-SJJMCOA
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

VBS and Disk Forensics

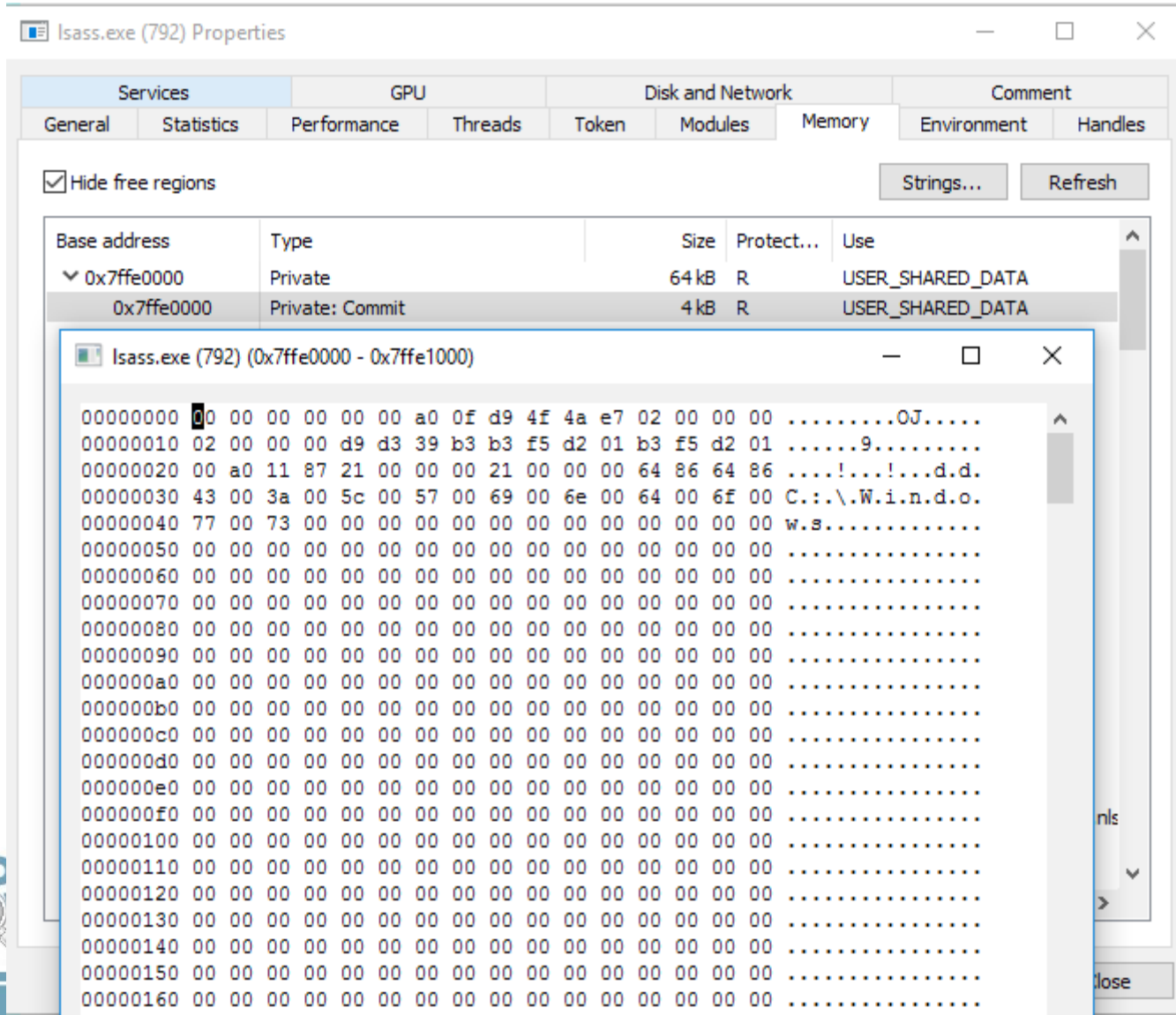
- No prefetch files for trustlets
- Shielded VMs – BitLocker encrypted
 - Attestation logs



VBS and Memory Forensics

- Acquisition currently the biggest hurdle
- Memory acquisition tools run in normal mode
- Normal kernel handles memory management
- VTL1 page allocations will be visible, but access to those pages may not be available

VBS and Memory Forensics



Isass.exe (792) Properties

Services | GPU | Disk and Network | Comment

General | Statistics | Performance | Threads | Token | Modules | Memory | Environment | Handles

Hide free regions

Strings... Refresh

Base address	Type	Size	Protect...	Use
0x7ffe0000	Private	64 kB	R	USER_SHARED_DATA
0x7ffe0000	Private: Commit	4 kB	R	USER_SHARED_DATA

Isass.exe (792) (0x7ffe0000 - 0x7ffe1000)

```
00000000 00 00 00 00 00 00 a0 0f d9 4f 4a e7 02 00 00 00 .....0J.....
00000010 02 00 00 00 d9 d3 39 b3 b3 f5 d2 01 b3 f5 d2 01 .....9.....
00000020 00 a0 11 87 21 00 00 00 21 00 00 00 64 86 64 86 ....!...!...d.d.
00000030 43 00 3a 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 C:\Windows.
00000040 77 00 73 00 00 00 00 00 00 00 00 00 00 00 00 00 w.s.....
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

VBS and Memory Forensics

Lsalso.exe (784) Properties

GPU | Disk and Network | Comment

General | Statistics | Performance | Threads | Token | Modules | Memory | Environment | Handles

Hide free regions

Strings... Refresh

Base address	Type	Size	Protect...	Use
0x7ffe0000	Private	64 kB	R	USER_SHARED_DATA
0x7ffe0000	Private: Commit	4 kB	R	USER_SHARED_DATA
0x7ffe1000	Private: Reserved	60 kB		USER_SHARED_DATA
TEB (thread 788)				
0x1acbf50000	Private	1,024 kB	RW	
0x1acbf50000	Private	512 kB	RW	
0x1acbfce0000	Private	1,024 kB	RW	
0x7df5ff960000	Mapped	2,147,483,...	NA	
0x7ff6d47d0000	Private	8 kB	RW	
0x7ff6d47e0000	Private	8 kB	RW	
0x7ff6d47f0000	Private	8 kB	RW	
0x7ff6d4800000	Private	8 kB	RW	
0x7ff6d4810000	Private	8 kB	RW	
0x7ff6d4810000	Private	4 kB	RW	PEB
0x7ff6d4820000				

Process Hacker

Unable to read memory: Invalid access to memory location.

OK

Close



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

0% complete



For more information about this issue and possible fixes, visit <http://windows.com/stopcode>

If you call a support person, give them this info:

Stop Code: SYSTEM_SERVICE_EXCEPTION

What failed: pmeA766.tmp

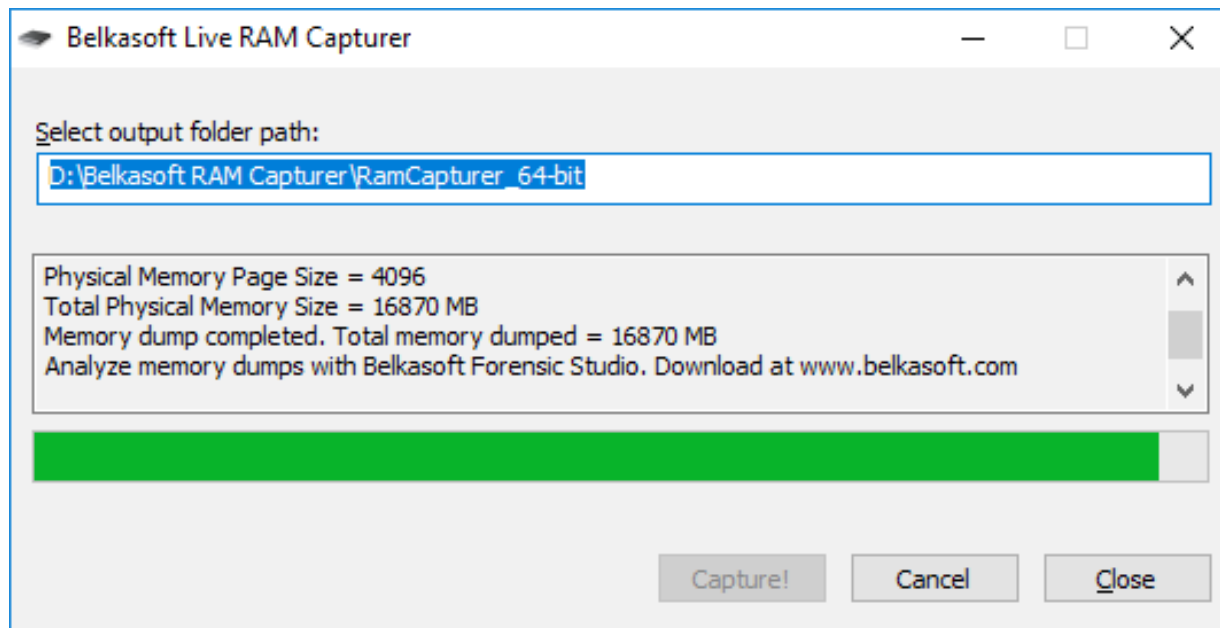
Memory Acquisition Test Results

Unsuccessful	
Tool	Result
<i>winpmem v1.6.2</i>	BSOD
<i>winpmem v2.1.post4</i>	BSOD
<i>Dumplt v1.3.2.20110401</i>	BSOD
<i>Dumplt v3.0.109.20161007</i>	Load driver error*
<i>Magnet RAM Capture v1.0.0.0034</i>	BSOD
<i>Magnet RAM Capture v1.1.1</i>	BSOD
<i>FTK Imager Lite v3.1.1</i>	BSOD

-Tested on Windows 1607 and 1703

*Non-EV driver signed after July 29, 2015

Belkasoft RAM Capturer



Dumplt v3.0.20170620

```
E:\Dumplt.exe

DumpIt 3.0.20170620.1
Copyright (C) 2007 - 2017, Matthieu Suiche <http://www.msuiche.net>
Copyright (C) 2012 - 2014, MoonSols Limited <http://www.moonsols.com>
Copyright (C) 2015 - 2017, Comae Technologies FZE <http://www.comae.io>

Destination path:          \??\E:\LENOVO-20170705-211411.dmp

Computer name:             LENOVO

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

[+] Information:
Dump Type:                 Microsoft Crash Dump

[+] Machine Information:
Windows version:           10.0.15063
MachineId:                 58EB7381-52A8-11CB-9C70-ED069E383733
TimeStamp:                 131437628531654104
Cr3:                       0x1aa000
KdCopyDataBlock:          0xffffffff8011647d8dc
KdDebuggerData:           0xffffffff801165bd4f0
KdpDataBlockEncoded:      0xffffffff801165f04b0

Current date/time:         [2017-07-05 (YYYY-MM-DD) 21:14:13 (UTC)]
+ Processing... Done.

Acquisition finished at:  [2017-07-05 (YYYY-MM-DD) 21:28:24 (UTC)]
Time elapsed:              14:11 minutes:seconds (851 secs)

Created file size:         16843382784 bytes ( 16063 Mb)
```



osforensics v5.1.1001

The screenshot displays the OSForensics v5.1.1001 Memory Viewer interface. The left sidebar contains a 'Workflow' menu with options: Start, Manage Case, File Name Search, Create Index, Search Index, Recent Activity, Deleted Files Search, Mismatch File Search, Memory Viewer (selected), Prefetch Viewer, Raw Disk Viewer, Registry Viewer, File System Browser, SQLite DB Browser, Web Browser, Passwords, System Information, Verify / Create Hash, and Hash Sets. The main window is titled 'Memory Viewer' and has tabs for 'Live Analysis' and 'Static Analysis'. A 'Dump Physical Memory' button is highlighted. Below it is a table with columns: Process, PID, CPU %, Total CPU Time, User Time, Kernel Time, and Process Create Time. A 'Physical Memory Dump' dialog box is open, displaying the text: 'Generating raw dump.... this may take a few minutes' and 'Please refrain from performing other activities while this dialog box is visible.' Below the dialog is a table with the following data:

Process	PID	CPU %	Total CPU Time	User Time	Kernel Time	Process Create Time
svchost.exe	904		00:00:00.015	00:00:00.015	00:00:00.000	8/6/2017, 19:54:16
svchost.exe	1004		00:00:00.015	00:00:00.015	00:00:00.000	8/6/2017, 12:11:54
svchost.exe	1060		00:00:00.500	00:00:00.250	00:00:00.250	8/6/2017, 12:11:55

Below the table are tabs for 'Process Info', 'Handles', 'Modules', 'Memory Space', and 'Memory Layout'. The 'Process Info' tab is active, showing fields: Image Path, Product, Description, Version, User Name, Integrity Level, Digitally Signed, and Digital Signer. A second 'Physical Memory Dump' dialog box is open, displaying the message: 'Full physical memory dump successfully generated!' with an 'OK' button.

VBS and Memory Forensics

```
-----> pslist()
 _EPROCESS          name          pid  ppid  thread_count  handle_count  session_id  wow64  process_create_time  process_exit_time
-----
```

_EPROCESS	name	pid	ppid	thread_count	handle_count	session_id	wow64	process_create_time	process_exit_time
0x970910691040		0	0	0	-	-	False	-	-
0x9709136e0540	svchost.exe	304	764	13	-	0	False	2017-07-05 17:04:51Z	-
0x97091198f040	Secure System	364	4	0	-	-	False	2017-07-05 17:04:45Z	-
0x9709119af780	smss.exe	368	4	2	-	-	False	2017-07-05 17:04:45Z	-
0x97091145f4c0	smartscreen.ex	604	956	8	-	1	False	2017-07-05 17:21:23Z	-
0x9709121ac680	csrss.exe	612	440	11	-	0	False	2017-07-05 17:04:48Z	-
0x970912fe8780	smss.exe	680	368	0	-	1	False	2017-07-05 17:04:49Z	2017-07-05 17:04:50Z
0x970913a27780	svchost.exe	684	764	11	-	0	False	2017-07-05 17:04:52Z	-
0x970912fe5780	wininit.exe	688	440	1	-	0	False	2017-07-05 17:04:49Z	-
0x970912feb780	csrss.exe	696	680	12	-	1	False	2017-07-05 17:04:49Z	-
0x9709135d3780	services.exe	764	688	6	-	0	False	2017-07-05 17:04:49Z	-
0x9709135cb780	LsaIso.exe	784	688	2	-	0	False	2017-07-05 17:04:49Z	-
0x970911e1a780	lsass.exe	792	688	8	-	0	False	2017-07-05 17:04:49Z	-
0x970911ea6080	winlogon.exe	876	680	4	-	1	False	2017-07-05 17:04:50Z	-
0x970911f53380	svchost.exe	956	764	24	-	0	False	2017-07-05 17:04:50Z	-
0x970913757780	dwm.exe	976	876	12	-	1	False	2017-07-05 17:04:51Z	-
0x970917fc6780	SynTPLpr.exe	1036	4904	1	-	1	False	2017-07-05 17:04:59Z	-
0x970917fc4780	SynLenovoHelpe	1072	4904	2	-	1	False	2017-07-05 17:04:59Z	-
0x9709136b75c0	svchost.exe	1100	764	88	-	0	False	2017-07-05 17:04:52Z	-
0x9709136b3780	svchost.exe	1120	764	27	-	0	False	2017-07-05 17:04:52Z	-
0x970913792780	svchost.exe	1196	764	26	-	0	False	2017-07-05 17:04:52Z	-
0x9709136ad340	svchost.exe	1204	764	17	-	0	False	2017-07-05 17:04:52Z	-
0x9709136a9780	svchost.exe	1216	764	29	-	0	False	2017-07-05 17:04:52Z	-
0x9709137ef780	WUDFHost.exe	1316	1120	7	-	0	False	2017-07-05 17:04:52Z	-
0x9709138cb780	ibmpmsvc.exe	1560	764	6	-	0	False	2017-07-05 17:04:52Z	-
0x9709138f1500	LPlatSvc.exe	1568	764	9	-	0	False	2017-07-05 17:04:52Z	-
0x9709138c5780	igfxCUIService	1776	764	4	-	0	False	2017-07-05 17:04:52Z	-
0x9709138a2780	svchost.exe	1784	764	23	-	0	False	2017-07-05 17:04:52Z	-
0x97091389e780	svchost.exe	1932	764	9	-	0	False	2017-07-05 17:04:52Z	-
0x970913a7b780	svchost.exe	2032	764	18	-	0	False	2017-07-05 17:04:52Z	-
0x9709134ac780	spoolsv.exe	2180	764	13	-	0	False	2017-07-05 17:04:53Z	-
0x970913461780	svchost.exe	2400	764	16	-	0	False	2017-07-05 17:04:53Z	-
0x970913463780	BtwRSupportSer	2408	764	3	-	0	False	2017-07-05 17:04:53Z	-
0x970913b17780	SynTPEnhServic	2488	764	3	-	0	False	2017-07-05 17:04:53Z	-
0x970913575780	svchost.exe	2552	764	11	-	0	False	2017-07-05 17:04:53Z	-

VBS and Memory Forensics

```
1 | 20170705.mem 14:39:53> procinfo 784
-----> procinfo(784)
*****
Pid: 784 LsaIso.exe

Process Environment
ALLUSERSPROFILE=C:\ProgramData
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DESKTOP-SJJMC0A
...

PE Infomation
Attribute Value
-----
Machine IMAGE_FILE_MACHINE_AMD64
TimeDateStamp 2017-03-28 05:36:31Z
Characteristics IMAGE_FILE_EXECUTABLE_IMAGE, IMAGE_FILE_LARGE_ADDRESS_AWARE
GUID/Age 1C6758214C9C4C04A3FFC814597FA1341
PDB LsaIso.pdb
...

Sections (Relative to 0x7ff6d5230000):
Perm Name Raw Off VMA Size
-----
xr- .text 0x00000000400 0x00000000100 0x000000021e00
-r- .rdata 0x000000022200 0x000000023000 0x00000000da00
-rw .data 0x00000002fc00 0x000000031000 0x00000000400
-r- .pdata 0x000000030000 0x000000032000 0x000000001600
-r- .tPolicy 0x000000031600 0x000000034000 0x00000000600
...

Data Directories:
----- VMA Size
-----
IMAGE_DIRECTORY_ENTRY_EXPORT 0x7ff6d525e920 0x00000000054
IMAGE_DIRECTORY_ENTRY_IMPORT 0x7ff6d525e974 0x000000000230
IMAGE_DIRECTORY_ENTRY_RESOURCE 0x7ff6d5265000 0x000000000400
IMAGE_DIRECTORY_ENTRY_EXCEPTION 0x7ff6d5262000 0x0000000014ac
IMAGE_DIRECTORY_ENTRY_SECURITY 0x7ff6d5262c00 0x000000002998
...

Import Directory (Original):
Name Mapped Function
-----
...

Export Directory:
Entry Stat Ord Name
-----
0x7ff6d5264470 M 0 LsaIso.exe!s_IumPolicyMetadata (lsaiso!s_IumPolicyMetadata)
0x7ff6d525e95d M 1 LsaIso.exe! (lsaiso!)
Version Information:
key value
-----
CompanyName Microsoft Corporation
FileDescription Credential Guard
```



Future/Additional Work

- Windows Defender Application Guard
 - Is web history, cache, etc. of protected pages available?
 - What information related to WDAG is available from a memory dump?

Thank You!

jhale@onesourcediscovery.com
@jasonshale