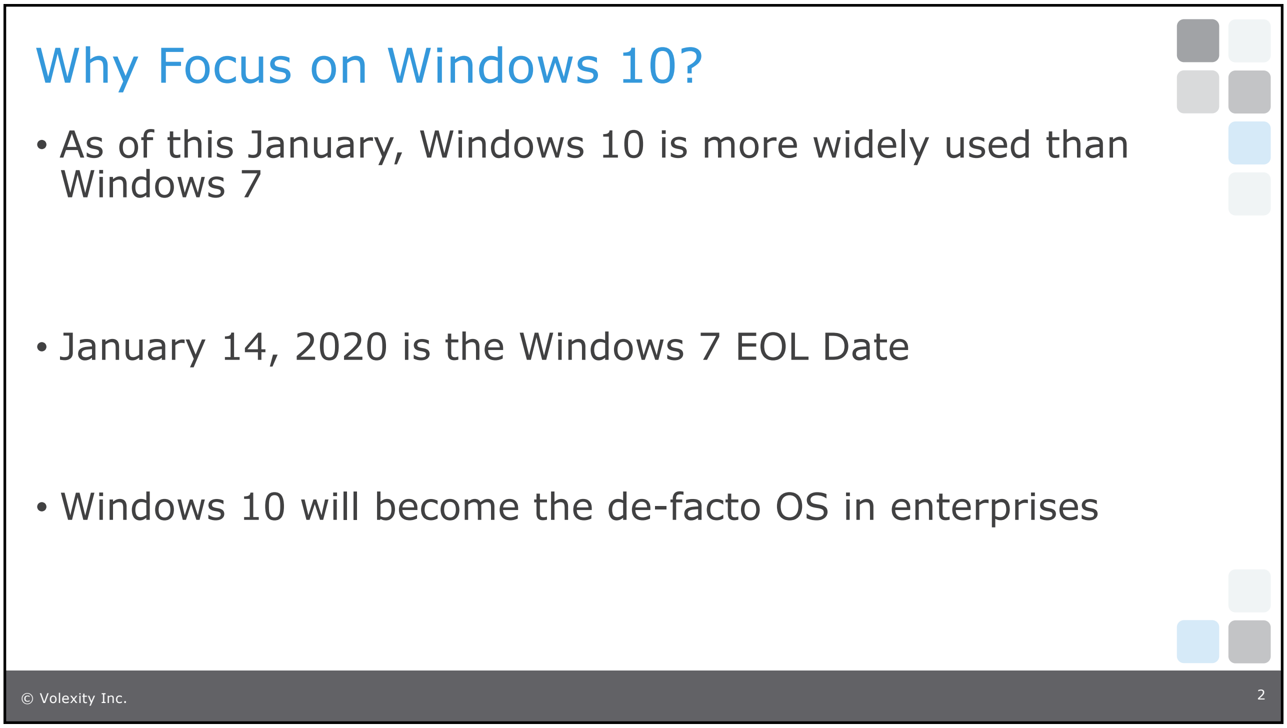
VOLEXITY

Windows 10 DFIR and InfoSec Challenges

Andrew Case / @attrc

1

1



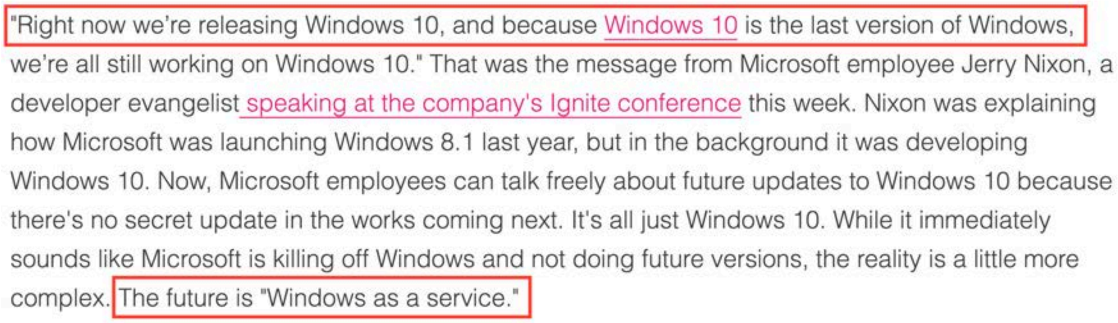
Why Focus on Windows 10?

- As of this January, Windows 10 is more widely used than Windows 7
- January 14, 2020 is the Windows 7 EOL Date
- Windows 10 will become the de-facto OS in enterprises

2

2

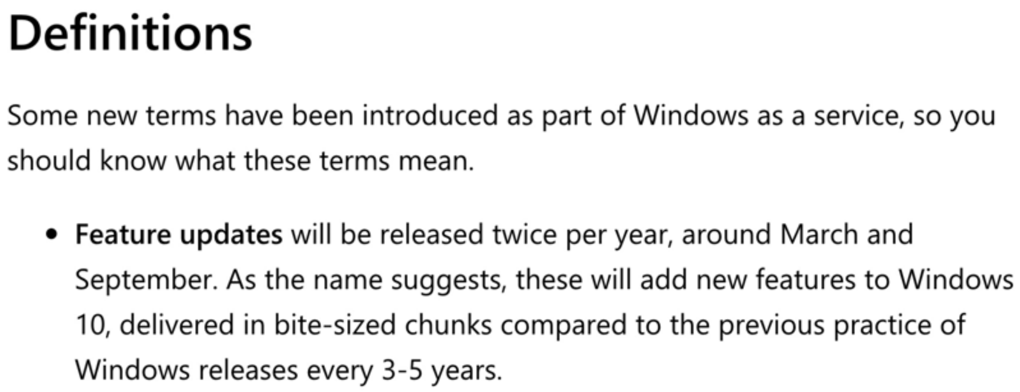
Windows 10 is the LAST Version of Windows



"Right now we're releasing Windows 10, and because Windows 10 is the last version of Windows, we're all still working on Windows 10." That was the message from Microsoft employee Jerry Nixon, a developer evangelist speaking at the company's Ignite conference this week. Nixon was explaining how Microsoft was launching Windows 8.1 last year, but in the background it was developing Windows 10. Now, Microsoft employees can talk freely about future updates to Windows 10 because there's no secret update in the works coming next. It's all just Windows 10. While it immediately sounds like Microsoft is killing off Windows and not doing future versions, the reality is a little more complex. The future is "Windows as a service."

Source: [1]

Windows as a Service (WAAS)



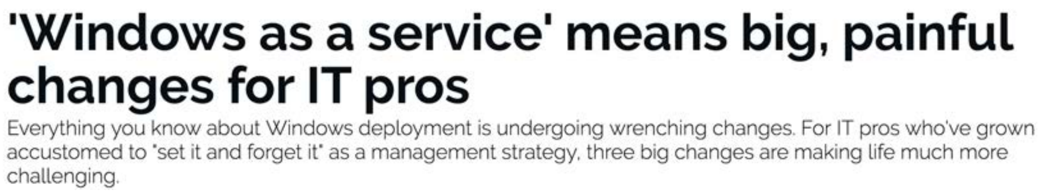
Definitions

Some new terms have been introduced as part of Windows as a service, so you should know what these terms mean.

- **Feature updates** will be released twice per year, around March and September. As the name suggests, these will add new features to Windows 10, delivered in bite-sized chunks compared to the previous practice of Windows releases every 3-5 years.

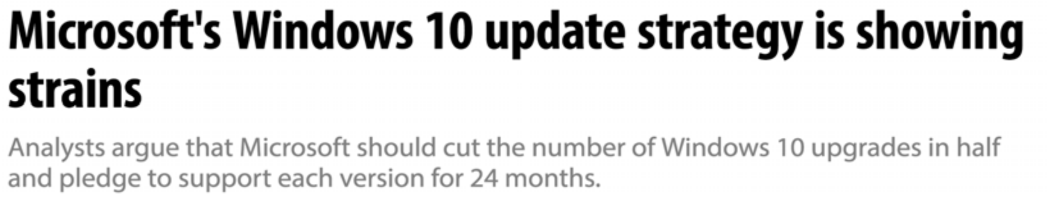
Source: [2]

WAAS = IT & InfoSec Pain



'Windows as a service' means big, painful changes for IT pros

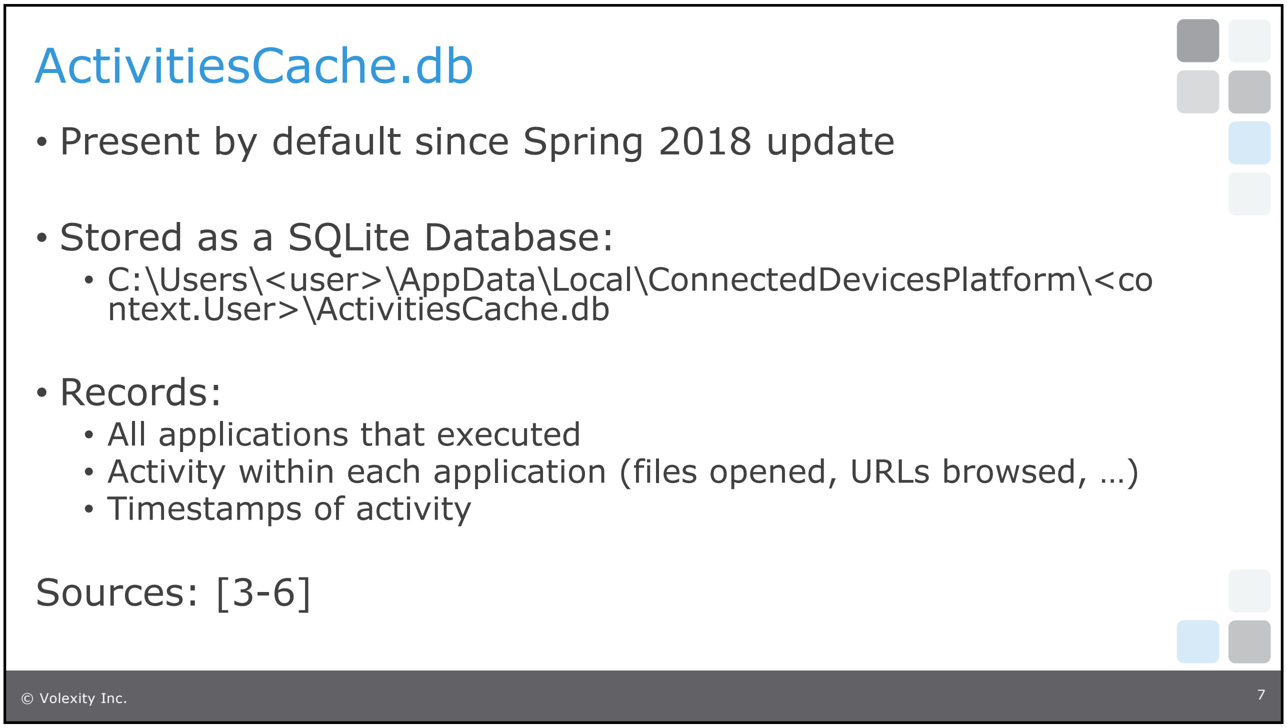
Everything you know about Windows deployment is undergoing wrenching changes. For IT pros who've grown accustomed to "set it and forget it" as a management strategy, three big changes are making life much more challenging.



Microsoft's Windows 10 update strategy is showing strains

Analysts argue that Microsoft should cut the number of Windows 10 upgrades in half and pledge to support each version for 24 months.

Windows 10 File System Analysis

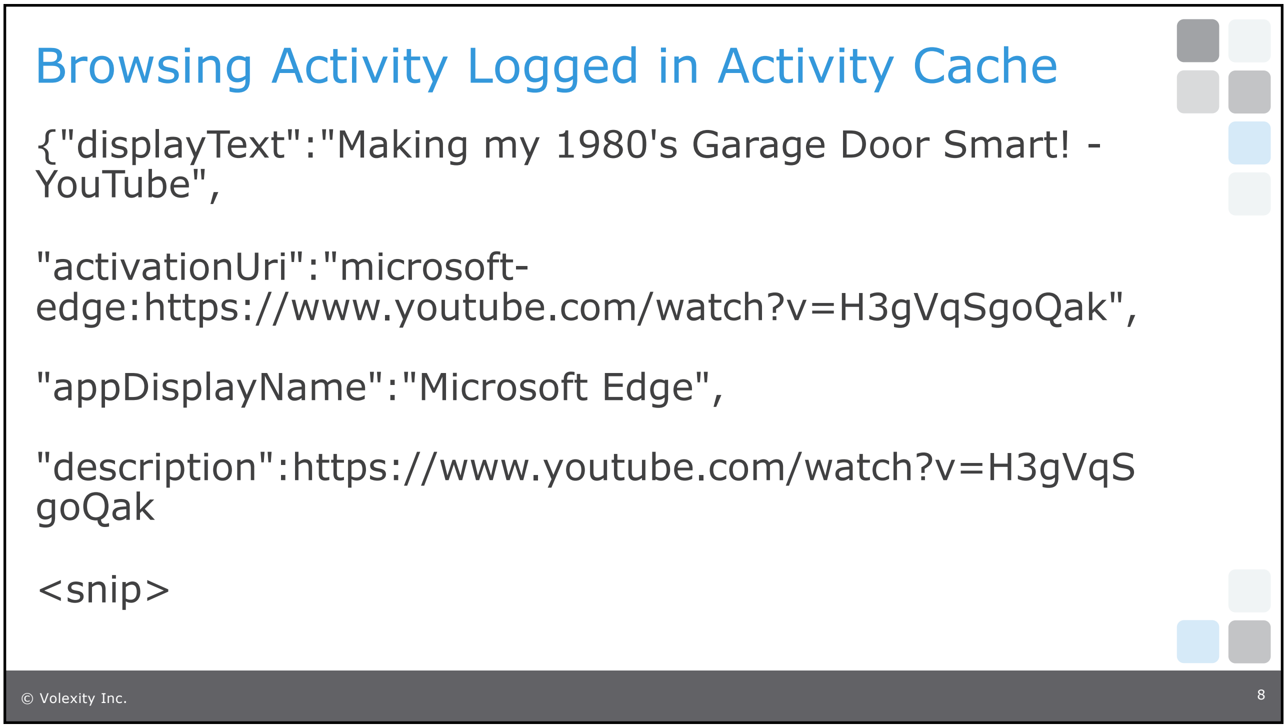


ActivitiesCache.db

- Present by default since Spring 2018 update
- Stored as a SQLite Database:
  - C:\Users\<user>\AppData\Local\ConnectedDevicesPlatform\<context.User>\ActivitiesCache.db
- Records:
  - All applications that executed
  - Activity within each application (files opened, URLs browsed, …)
  - Timestamps of activity

Sources: [3-6]

7



Browsing Activity Logged in Activity Cache

{"displayText":"Making my 1980's Garage Door Smart! - YouTube",

"activationUri":"microsoft-edge:https://www.youtube.com/watch?v=H3gVqSgoQak",

"appDisplayName":"Microsoft Edge",

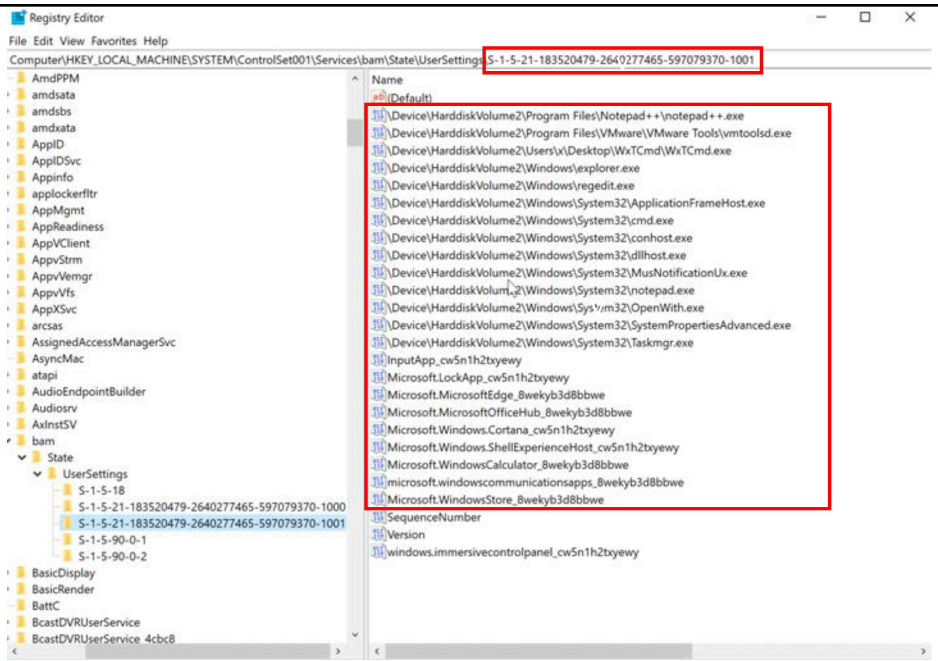
"description":https://www.youtube.com/watch?v=H3gVqSgoQak

<snip>

8

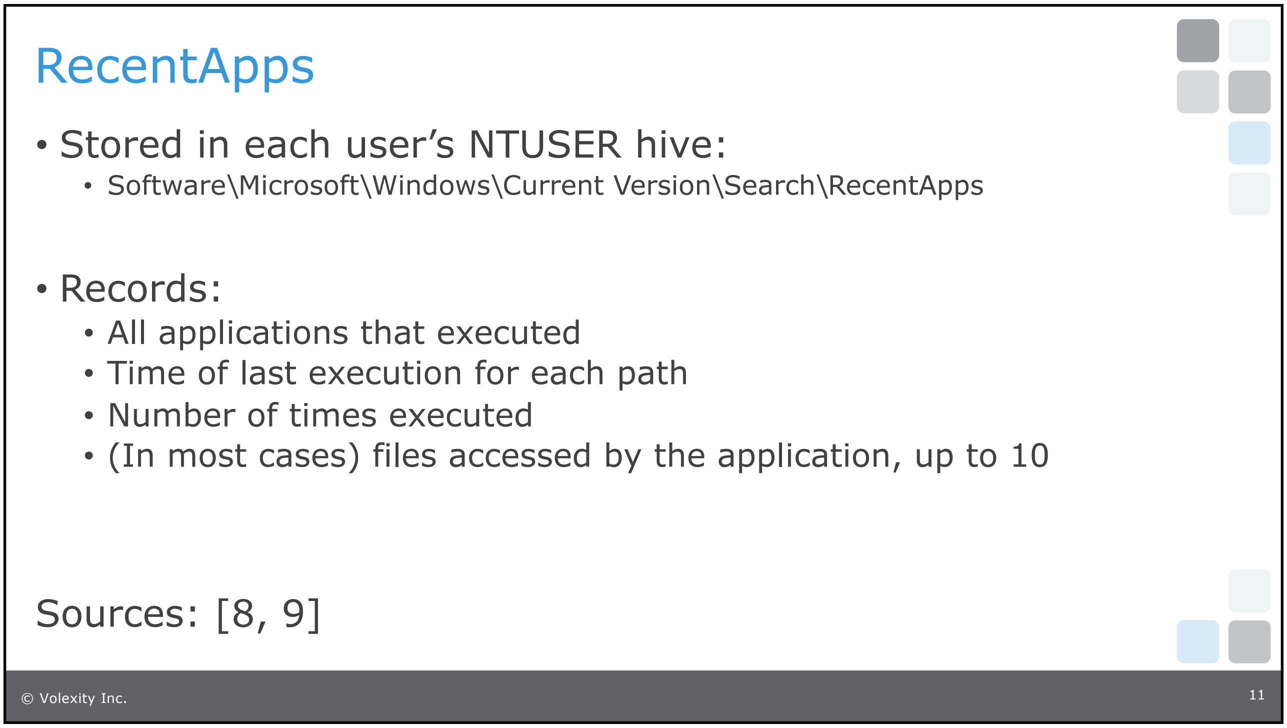
Background Activity Monitor

- Present since Fall 2017 release
- Stored in the System hive:
  - CurrentControlSet/Services/bam/UserSettings
- Records:
  - All applications that executed
  - User (SID) responsible for execution
  - Time of last execution for each path



```
Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-183520479-2640277465-597079370-1001
```

```
(Default)
\Device\HarddiskVolume2\Program Files\Notepad++\notepad++.exe
\Device\HarddiskVolume2\Program Files\VMware\VMware Tools\vmtoolsd.exe
\Device\HarddiskVolume2\Users\x\Desktop\WxTCmd\WxTCmd.exe
\Device\HarddiskVolume2\Windows\explorer.exe
\Device\HarddiskVolume2\Windows\regedit.exe
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe
\Device\HarddiskVolume2\Windows\System32\cmd.exe
\Device\HarddiskVolume2\Windows\System32\conhost.exe
\Device\HarddiskVolume2\Windows\System32\dllhost.exe
\Device\HarddiskVolume2\Windows\System32\MusNotificationUx.exe
\Device\HarddiskVolume2\Windows\System32\notepad.exe
\Device\HarddiskVolume2\Windows\System32\OpenWith.exe
\Device\HarddiskVolume2\Windows\System32\SystemPropertiesAdvanced.exe
\Device\HarddiskVolume2\Windows\System32\Taskmgr.exe
InputApp_cw5n1h2txyewy
Microsoft.LockApp_cw5n1h2txyewy
Microsoft.MicrosoftEdge_8wekyb3d8bbwe
Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe
Microsoft.Windows.Cortana_cw5n1h2txyewy
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy
Microsoft.WindowsCalculator_8wekyb3d8bbwe
microsoft.windowscommunicationsapps_8wekyb3d8bbwe
Microsoft.WindowsStore_8wekyb3d8bbwe
SequenceNumber
Version
windows.immersivecontrolpanel_cw5n1h2txyewy
```



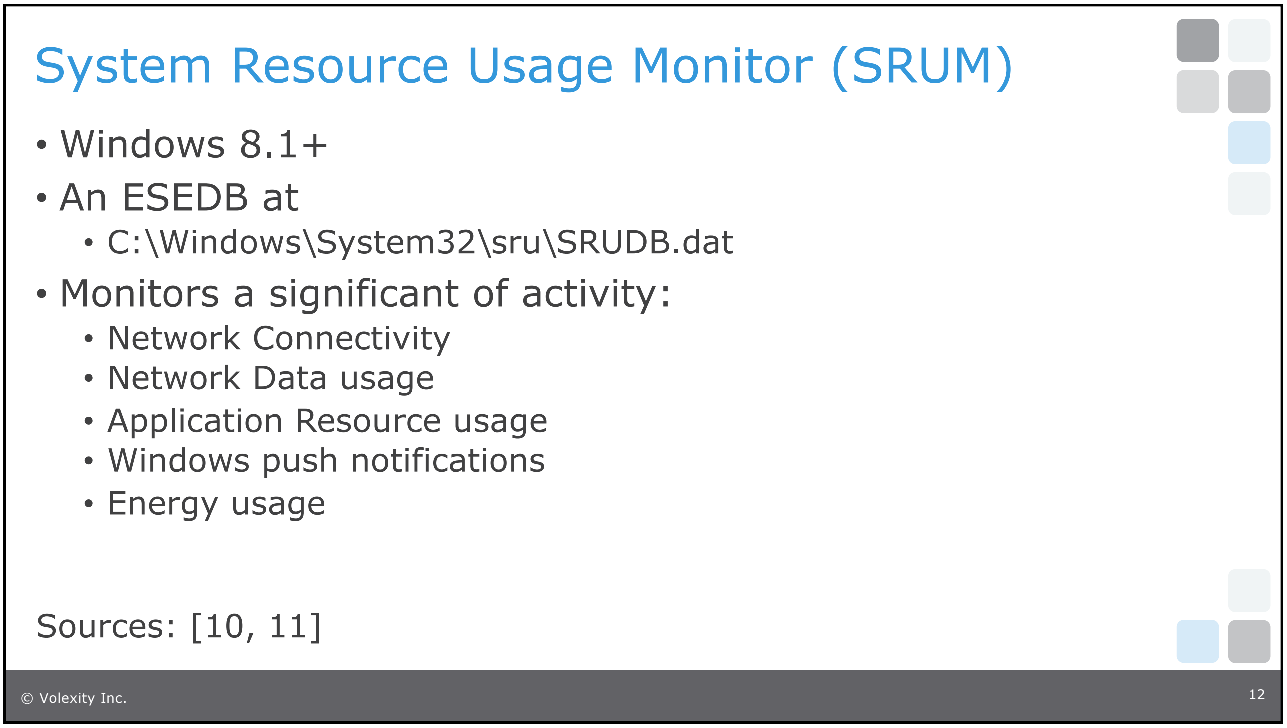
RecentApps

- Stored in each user’s NTUSER hive:
  - Software\Microsoft\Windows\Current Version\Search\RecentApps
- Records:
  - All applications that executed
  - Time of last execution for each path
  - Number of times executed
  - (In most cases) files accessed by the application, up to 10

Sources: [8, 9]

© Volexity Inc. 11

11



System Resource Usage Monitor (SRUM)

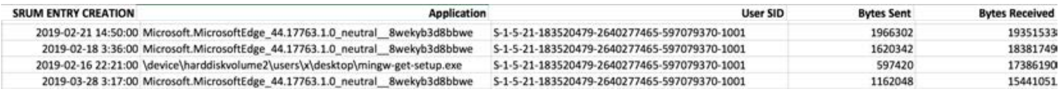
- Windows 8.1+
- An ESEDB at
  - C:\Windows\System32\sru\SRUDB.dat
- Monitors a significant of activity:
  - Network Connectivity
  - Network Data usage
  - Application Resource usage
  - Windows push notifications
  - Energy usage

Sources: [10, 11]

© Volexity Inc. 12

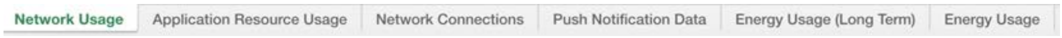
12

Example Network Usage Tracking:



SRUM ENTRY CREATION	Application	User SID	Bytes Sent	Bytes Received
2019-02-21 14:50:00	Microsoft.MicrosoftEdge_44.17763.1.0_neutral__8wekyb3d8bbwe	S-1-5-21-183520479-2640277465-597079370-1001	1966302	19351533
2019-02-18 3:36:00	Microsoft.MicrosoftEdge_44.17763.1.0_neutral__8wekyb3d8bbwe	S-1-5-21-183520479-2640277465-597079370-1001	1620342	18381749
2019-02-16 22:21:00	\device\harddiskvolume2\users\x\desktop\mingw-get-setup.exe	S-1-5-21-183520479-2640277465-597079370-1001	597420	17386190
2019-03-28 3:17:00	Microsoft.MicrosoftEdge_44.17763.1.0_neutral__8wekyb3d8bbwe	S-1-5-21-183520479-2640277465-597079370-1001	1162048	15441051

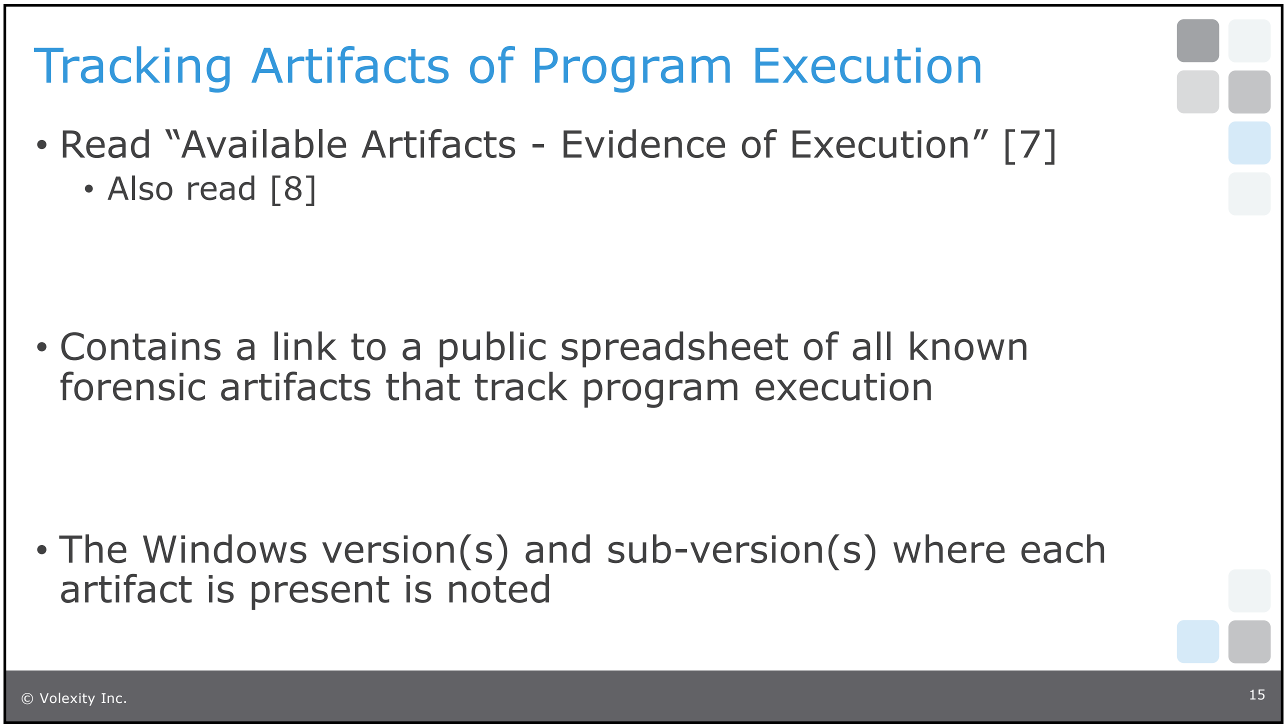
All Tabs Available in Produced Excel Sheet:



Parsed with srum-dump: [34]

Amcache

- Another source of determining what ran on the machine
- Available starting with Windows 8
- Includes (but not limited to):
  - Full path to the file
  - Last modified and created timestamps
  - Product & company name
  - PE file description and size
  - **SHA1 Hash**

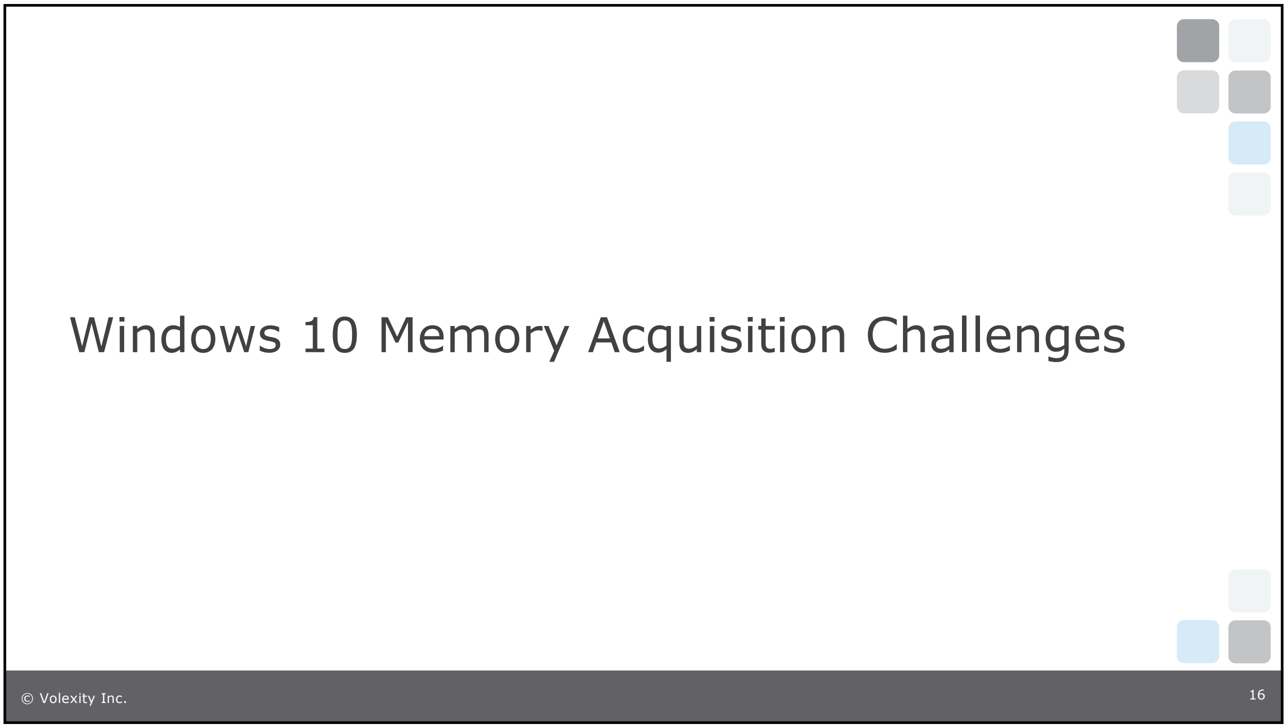


Tracking Artifacts of Program Execution

- Read “Available Artifacts - Evidence of Execution” [7]
  - Also read [8]
- Contains a link to a public spreadsheet of all known forensic artifacts that track program execution
- The Windows version(s) and sub-version(s) where each artifact is present is noted

© Volexity Inc. 15

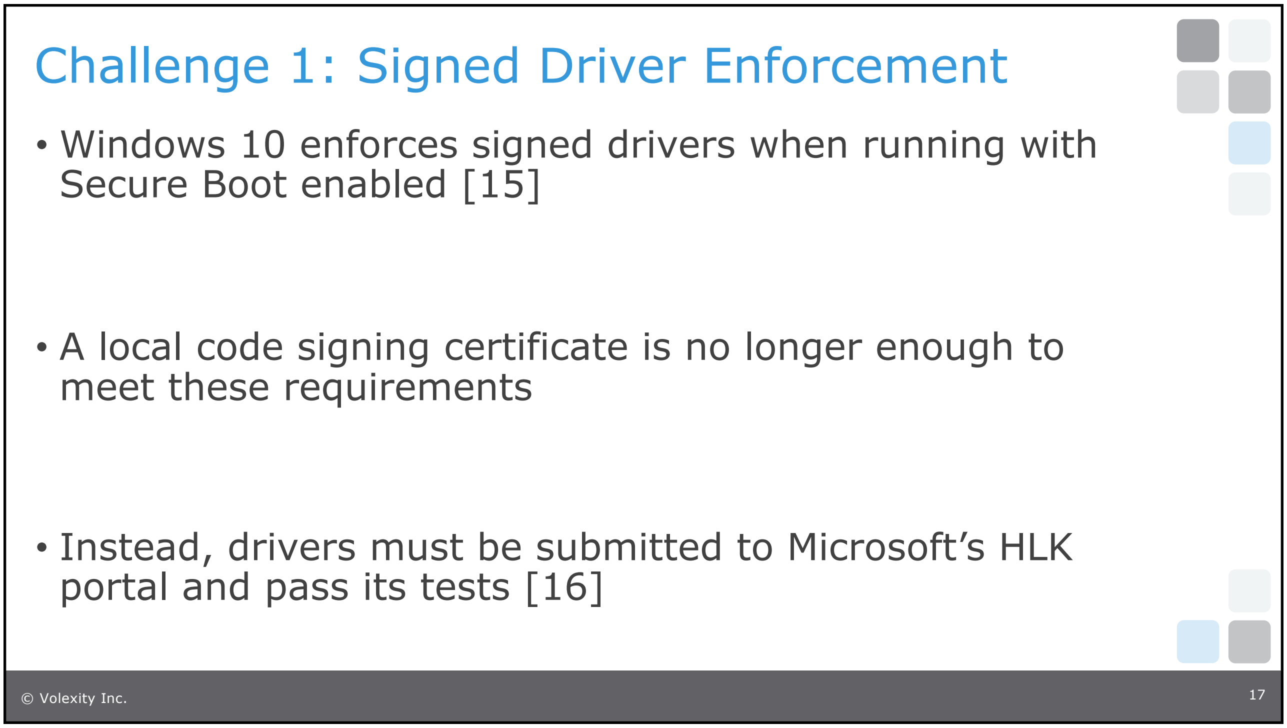
15



Windows 10 Memory Acquisition Challenges

© Volexity Inc. 16

16

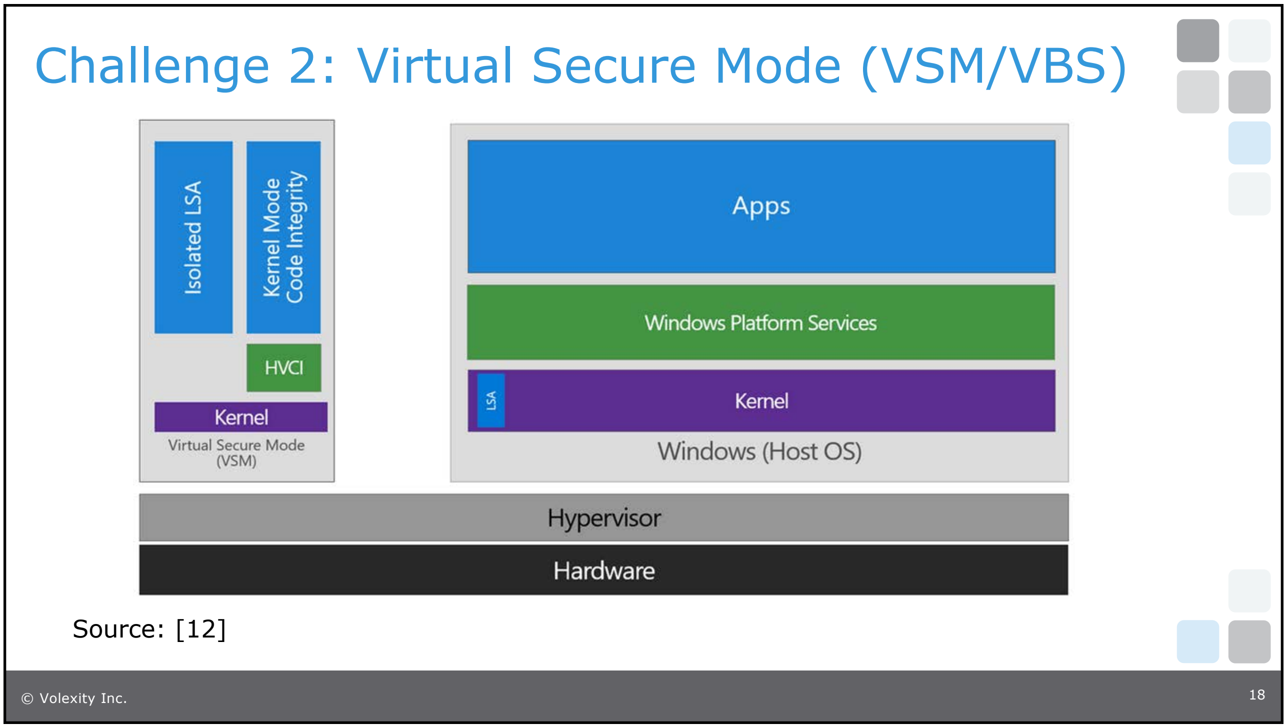


Challenge 1: Signed Driver Enforcement

- Windows 10 enforces signed drivers when running with Secure Boot enabled [15]
- A local code signing certificate is no longer enough to meet these requirements
- Instead, drivers must be submitted to Microsoft's HLK portal and pass its tests [16]

© Volexity Inc. 17

17



Challenge 2: Virtual Secure Mode (VSM/VBS)

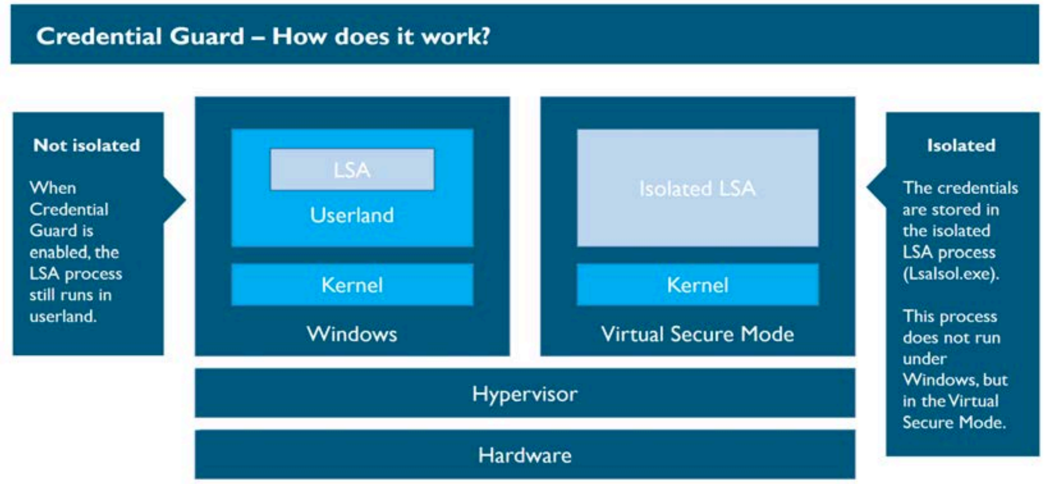
Isolated LSA
Kernel Mode Code Integrity
HVCI
Kernel
Virtual Secure Mode (VSM)
Apps
Windows Platform Services
LSA
Kernel
Windows (Host OS)
Hypervisor
Hardware

Source: [12]

© Volexity Inc. 18

18

Credential Isolation



Credential Guard – How does it work?

Not isolated

When Credential Guard is enabled, the LSA process still runs in userland.

Isolated

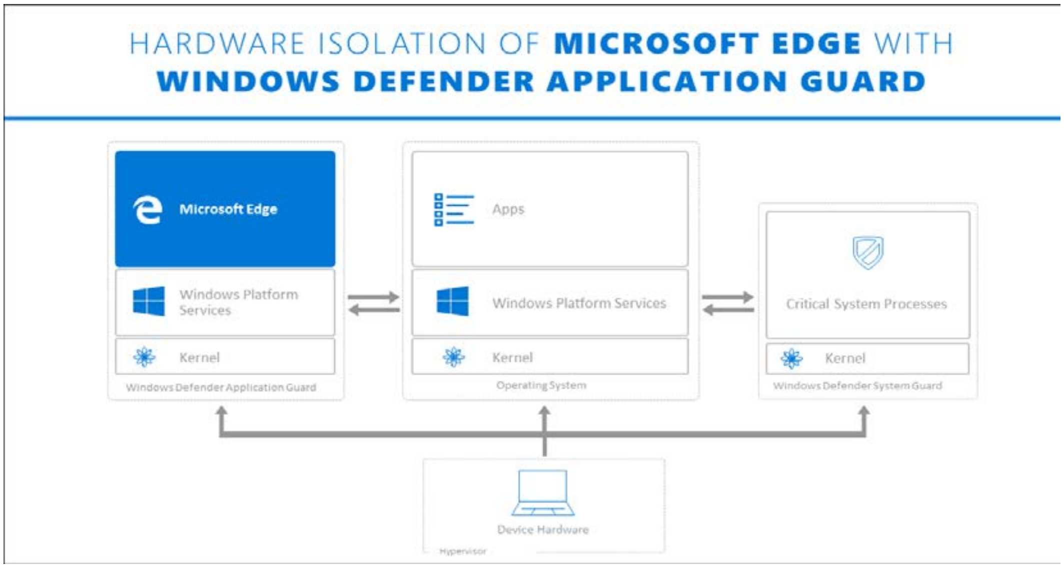
The credentials are stored in the isolated LSA process (Lsalsol.exe).

This process does not run under Windows, but in the Virtual Secure Mode.

Source: [13]

CG Prevents Cached Credential Harvesting

- “Live” credential harvesting still very much possible
- memssp module of Mimikatz [14]
- Any userland keylogger

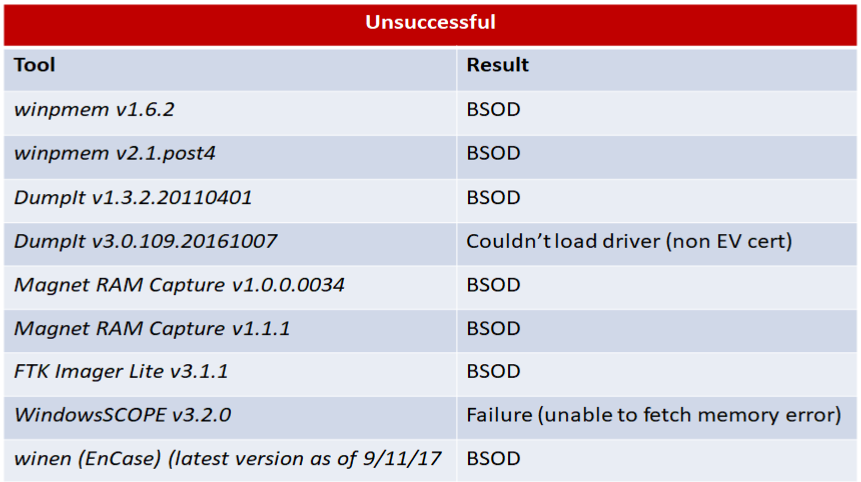


HARDWARE ISOLATION OF **MICROSOFT EDGE** WITH **WINDOWS DEFENDER APPLICATION GUARD**

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

Source: [17]

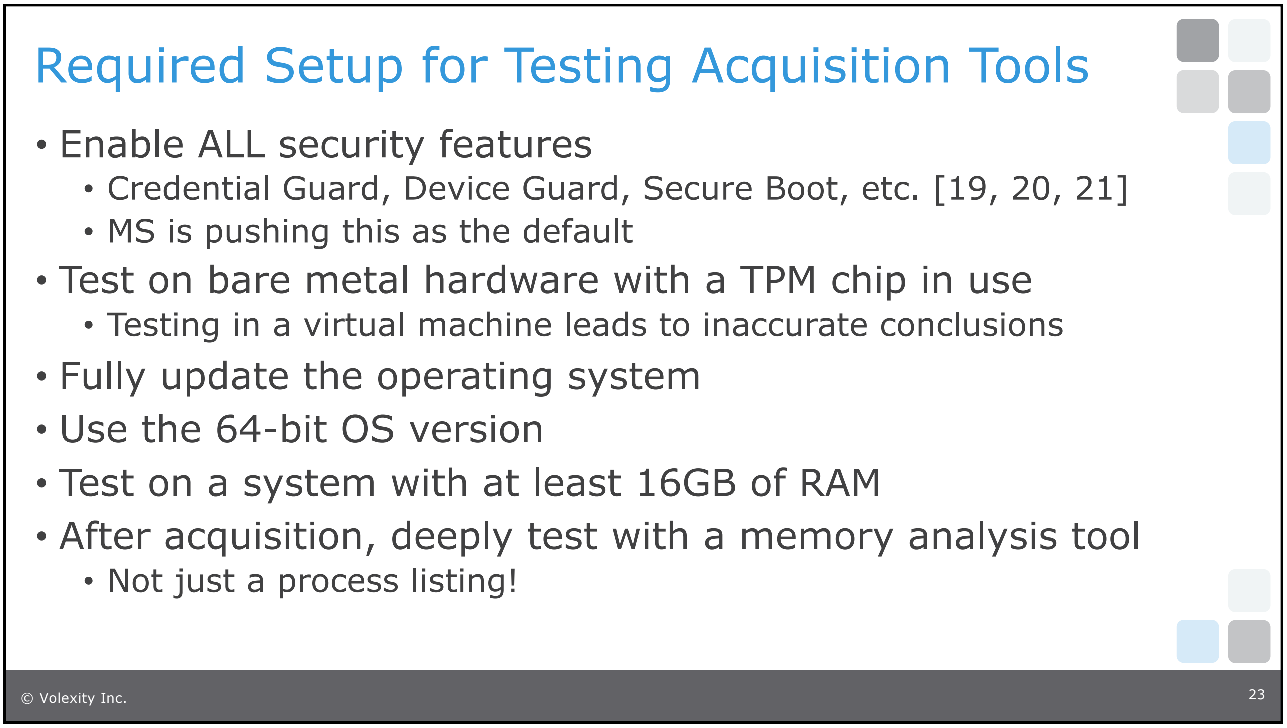
VSM and Acquisition Tools



Unsuccessful

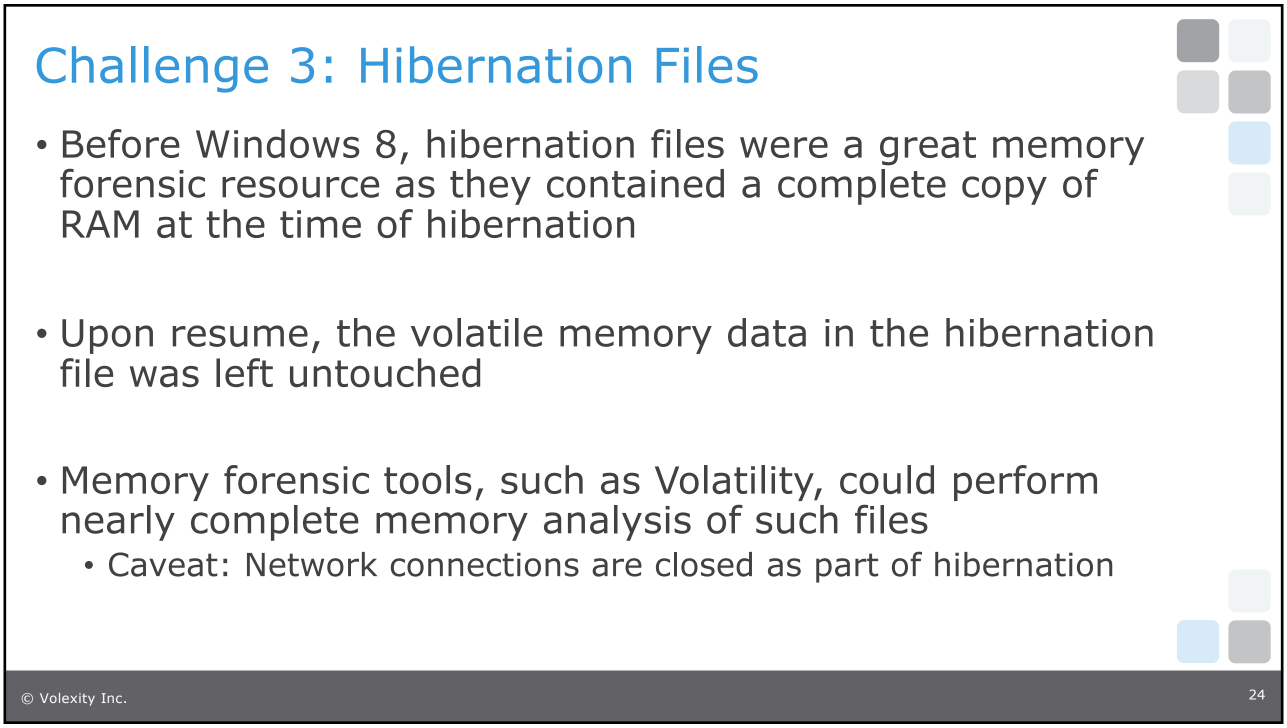
Tool	**Result**
winpmem v1.6.2	BSOD
winpmem v2.1.post4	BSOD
DumpIt v1.3.2.20110401	BSOD
DumpIt v3.0.109.20161007	Couldn't load driver (non EV cert)
Magnet RAM Capture v1.0.0.0034	BSOD
Magnet RAM Capture v1.1.1	BSOD
FTK Imager Lite v3.1.1	BSOD
WindowsSCOPE v3.2.0	Failure (unable to fetch memory error)
winen (EnCase) (latest version as of 9/11/17	BSOD

Source: [18] – Image from July 2017



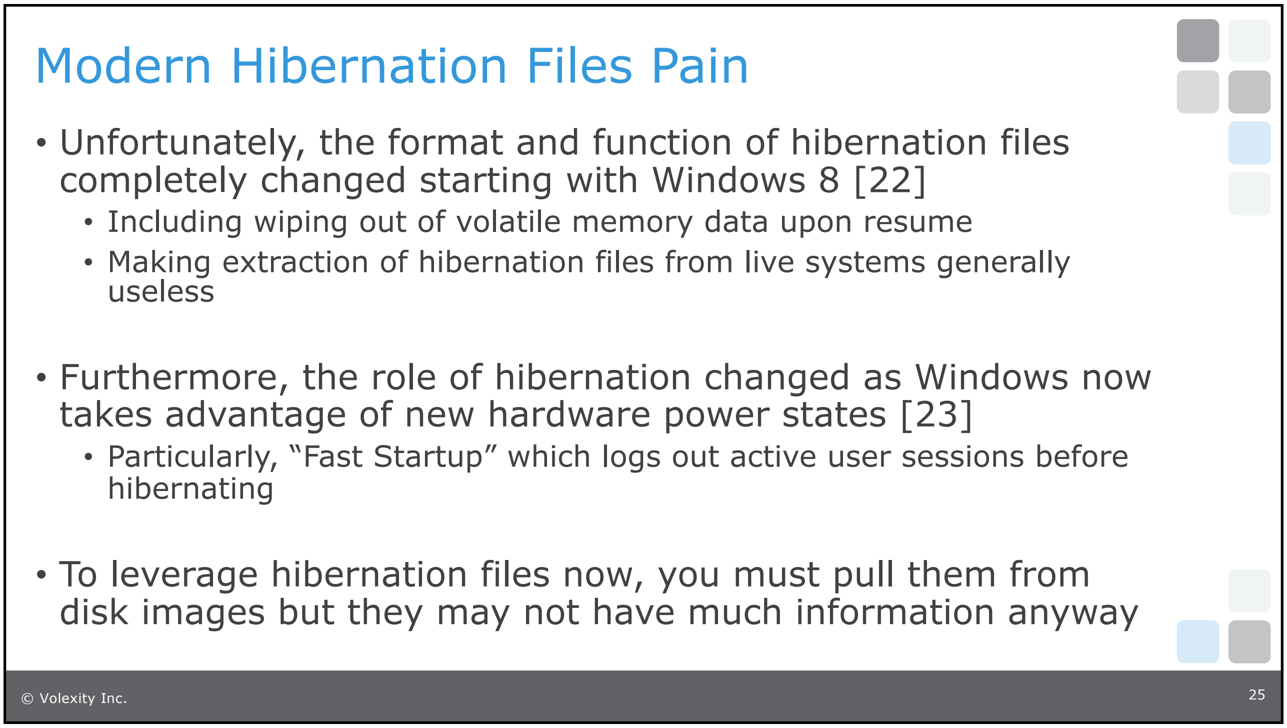
Required Setup for Testing Acquisition Tools

- Enable ALL security features
  - Credential Guard, Device Guard, Secure Boot, etc. [19, 20, 21]
  - MS is pushing this as the default
- Test on bare metal hardware with a TPM chip in use
  - Testing in a virtual machine leads to inaccurate conclusions
- Fully update the operating system
- Use the 64-bit OS version
- Test on a system with at least 16GB of RAM
- After acquisition, deeply test with a memory analysis tool
  - Not just a process listing!



Challenge 3: Hibernation Files

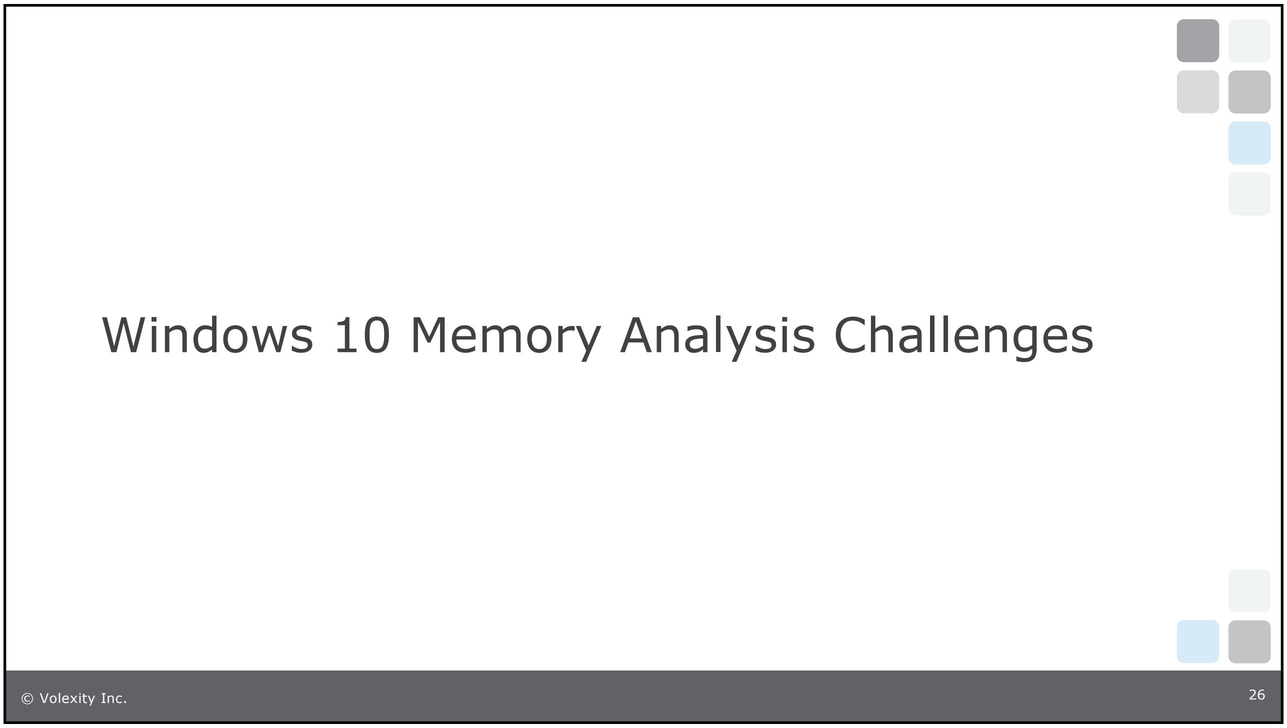
- Before Windows 8, hibernation files were a great memory forensic resource as they contained a complete copy of RAM at the time of hibernation
- Upon resume, the volatile memory data in the hibernation file was left untouched
- Memory forensic tools, such as Volatility, could perform nearly complete memory analysis of such files
  - Caveat: Network connections are closed as part of hibernation



Modern Hibernation Files Pain

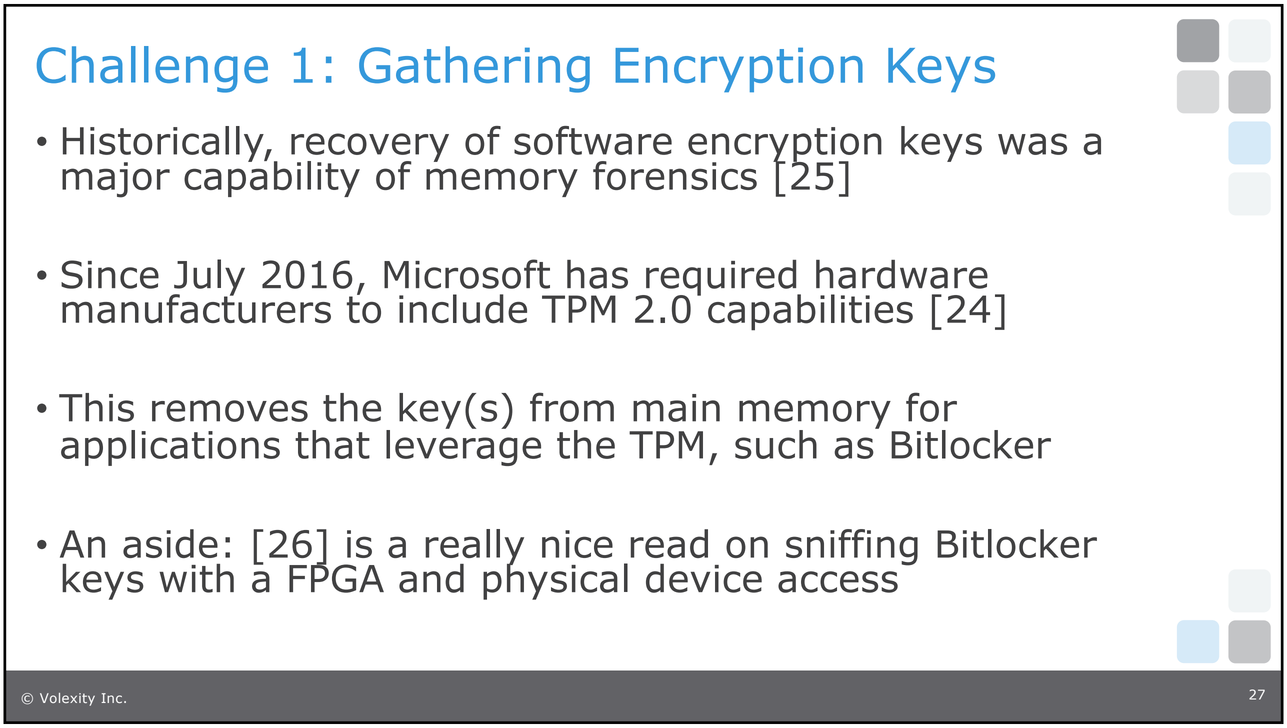
- Unfortunately, the format and function of hibernation files completely changed starting with Windows 8 [22]
  - Including wiping out of volatile memory data upon resume
  - Making extraction of hibernation files from live systems generally useless
- Furthermore, the role of hibernation changed as Windows now takes advantage of new hardware power states [23]
  - Particularly, “Fast Startup” which logs out active user sessions before hibernating
- To leverage hibernation files now, you must pull them from disk images but they may not have much information anyway

25



Windows 10 Memory Analysis Challenges

26

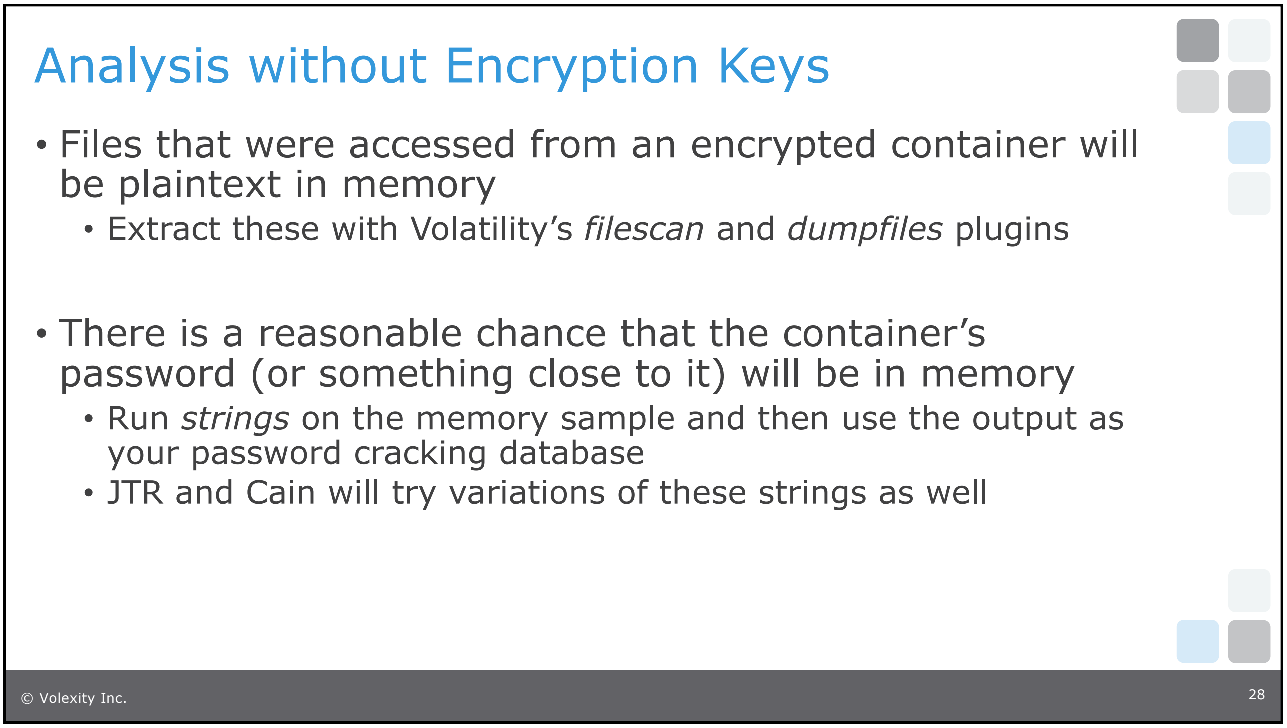


Challenge 1: Gathering Encryption Keys

- Historically, recovery of software encryption keys was a major capability of memory forensics [25]
- Since July 2016, Microsoft has required hardware manufacturers to include TPM 2.0 capabilities [24]
- This removes the key(s) from main memory for applications that leverage the TPM, such as Bitlocker
- An aside: [26] is a really nice read on sniffing Bitlocker keys with a FPGA and physical device access

© Volexity Inc. 27

27

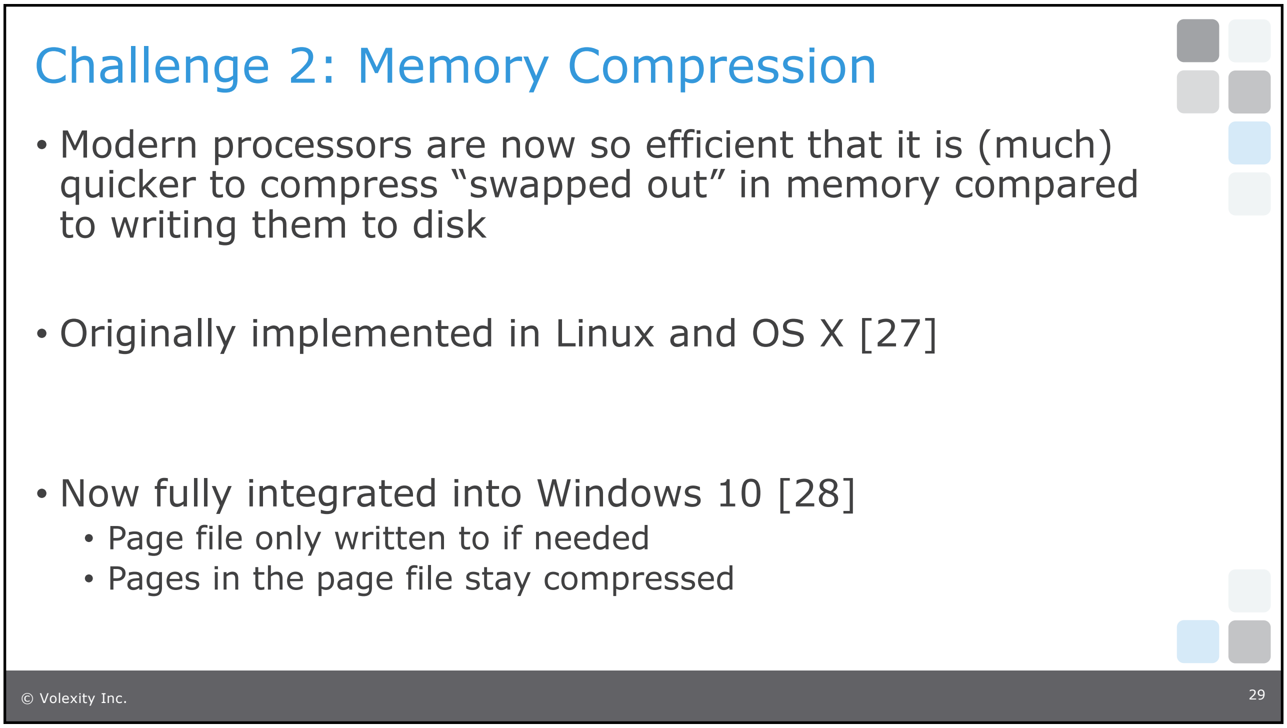


Analysis without Encryption Keys

- Files that were accessed from an encrypted container will be plaintext in memory
  - Extract these with Volatility’s *filescan* and *dumpfiles* plugins
- There is a reasonable chance that the container’s password (or something close to it) will be in memory
  - Run *strings* on the memory sample and then use the output as your password cracking database
  - JTR and Cain will try variations of these strings as well

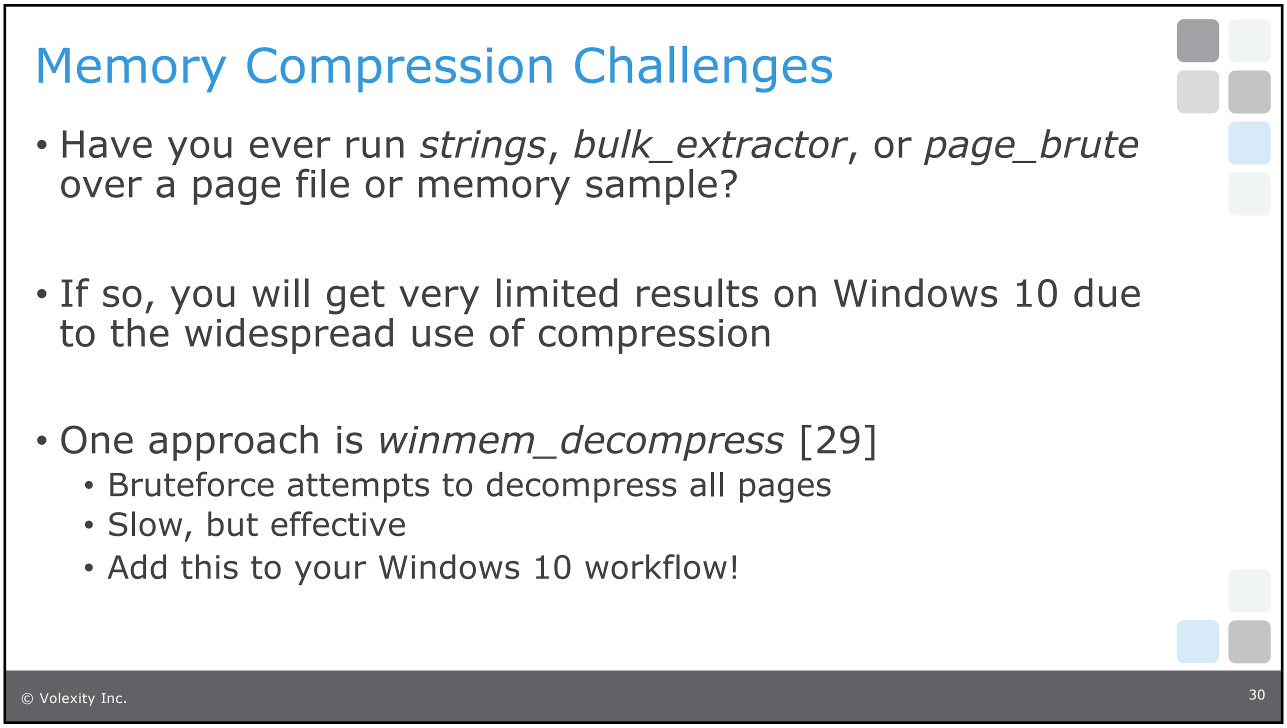
© Volexity Inc. 28

28



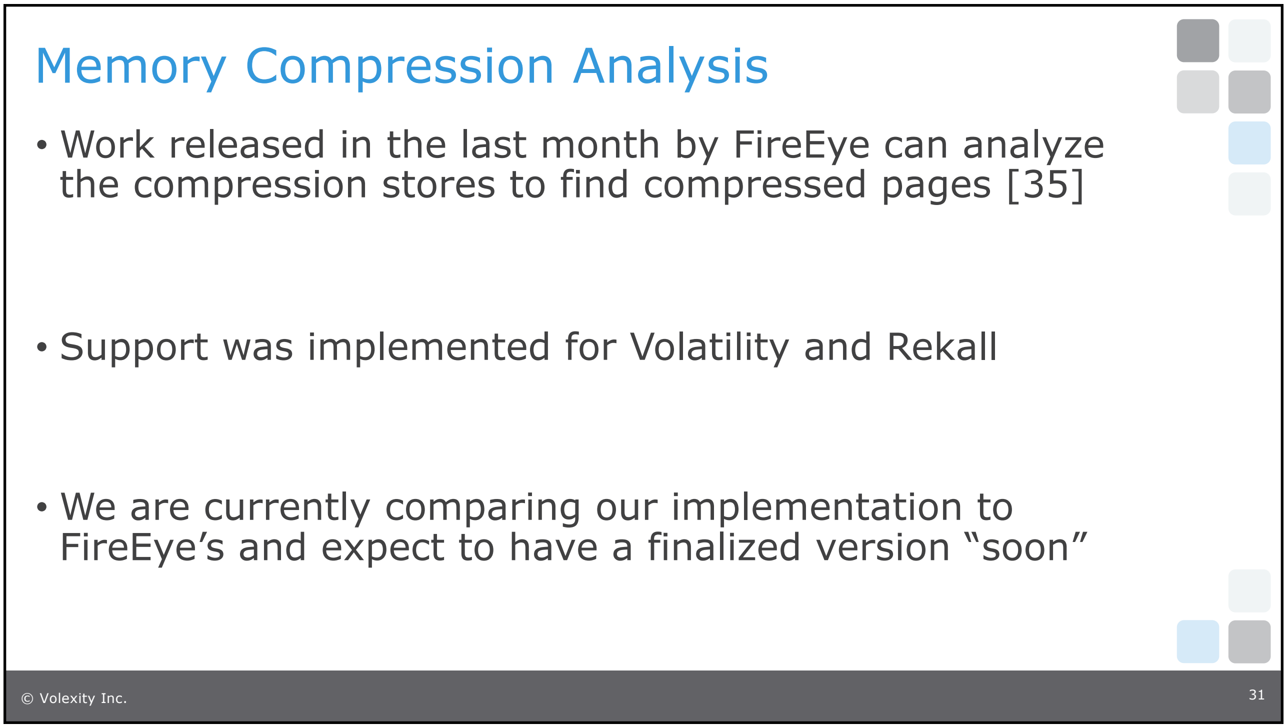
Challenge 2: Memory Compression

- Modern processors are now so efficient that it is (much) quicker to compress "swapped out" in memory compared to writing them to disk
- Originally implemented in Linux and OS X [27]
- Now fully integrated into Windows 10 [28]
  - Page file only written to if needed
  - Pages in the page file stay compressed



Memory Compression Challenges

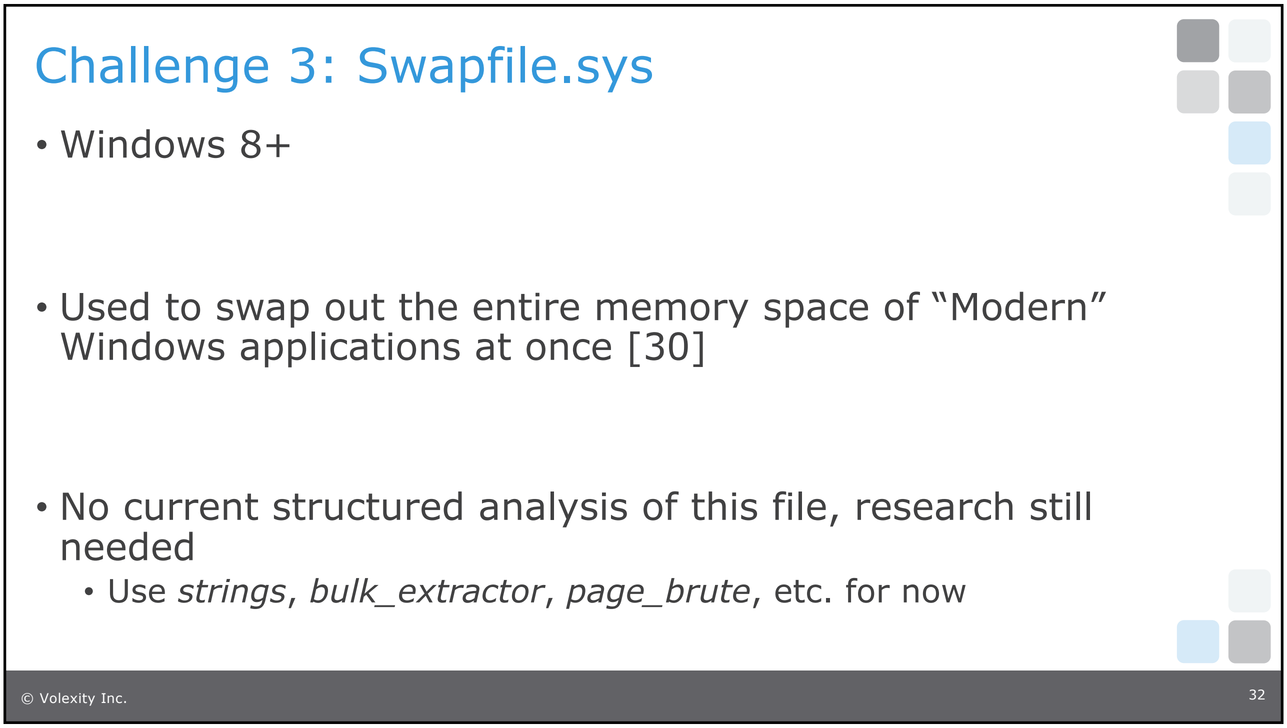
- Have you ever run *strings*, *bulk_extractor*, or *page_brute* over a page file or memory sample?
- If so, you will get very limited results on Windows 10 due to the widespread use of compression
- One approach is *winmem_decompress* [29]
  - Bruteforce attempts to decompress all pages
  - Slow, but effective
  - Add this to your Windows 10 workflow!



Memory Compression Analysis

- Work released in the last month by FireEye can analyze the compression stores to find compressed pages [35]
- Support was implemented for Volatility and Rekall
- We are currently comparing our implementation to FireEye's and expect to have a finalized version "soon"

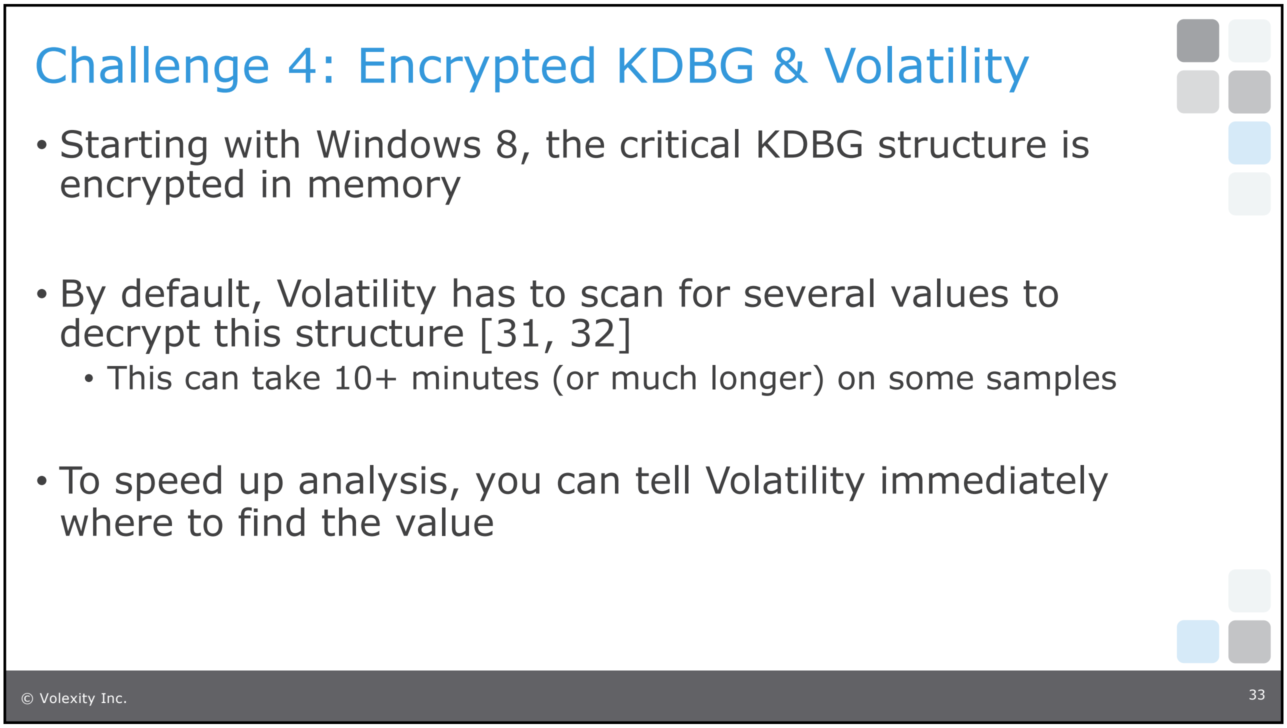
31



Challenge 3: Swapfile.sys

- Windows 8+
- Used to swap out the entire memory space of "Modern" Windows applications at once [30]
- No current structured analysis of this file, research still needed
  - Use *strings*, *bulk_extractor*, *page_brute*, etc. for now

32

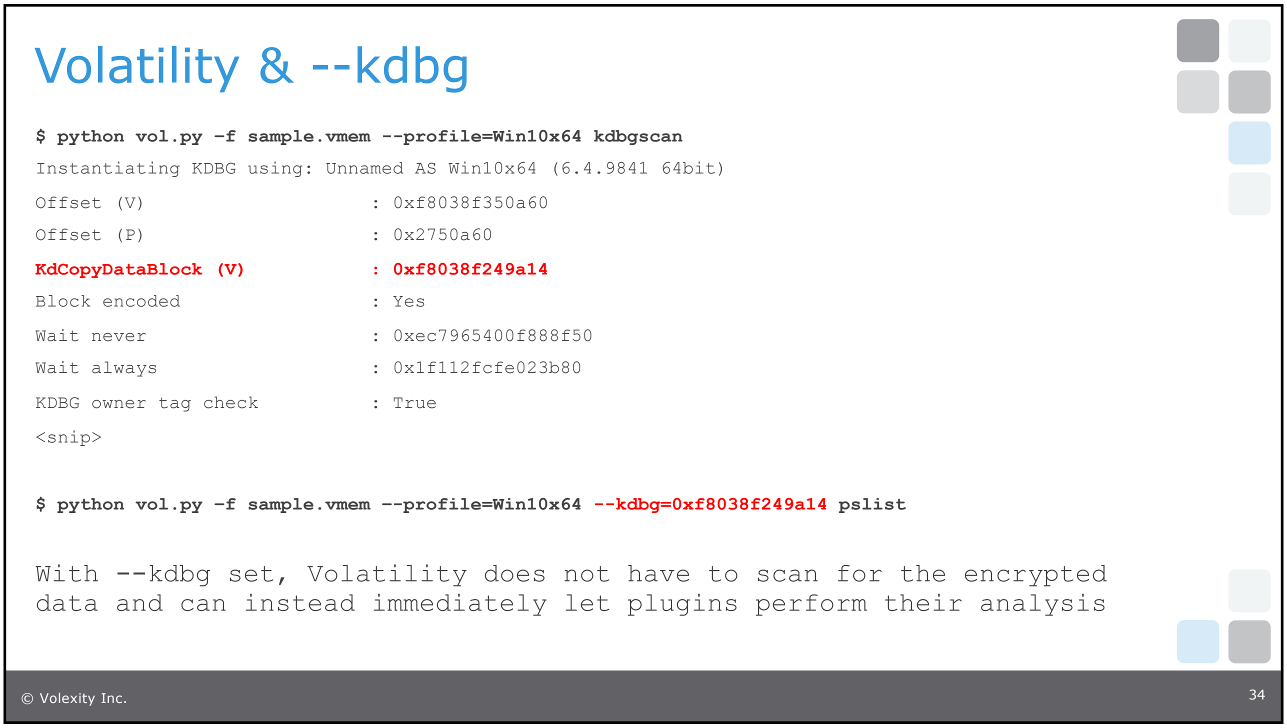


Challenge 4: Encrypted KDBG & Volatility

- Starting with Windows 8, the critical KDBG structure is encrypted in memory
- By default, Volatility has to scan for several values to decrypt this structure [31, 32]
  - This can take 10+ minutes (or much longer) on some samples
- To speed up analysis, you can tell Volatility immediately where to find the value

© Volexity Inc. 33

33



Volatility & --kdbg

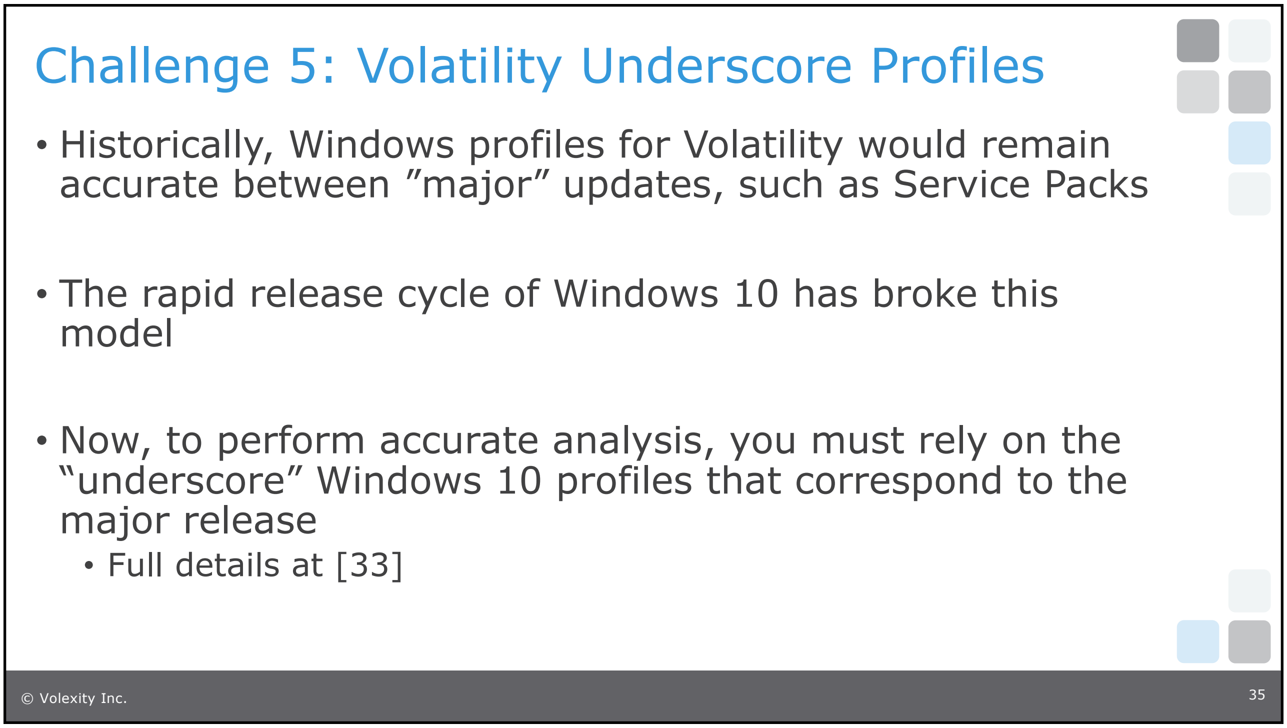
```
$ python vol.py -f sample.vmem --profile=Win10x64 kdbgscan
Instantiating KDBG using: Unnamed AS Win10x64 (6.4.9841 64bit)
Offset (V)                    : 0xf8038f350a60
Offset (P)                    : 0x2750a60
KdCopyDataBlock (V)           : 0xf8038f249a14
Block encoded                 : Yes
Wait never                    : 0xec7965400f888f50
Wait always                   : 0x1f112fcfe023b80
KDBG owner tag check          : True
<snip>

$ python vol.py -f sample.vmem --profile=Win10x64 --kdbg=0xf8038f249a14 pslist
```

With --kdbg set, Volatility does not have to scan for the encrypted data and can instead immediately let plugins perform their analysis

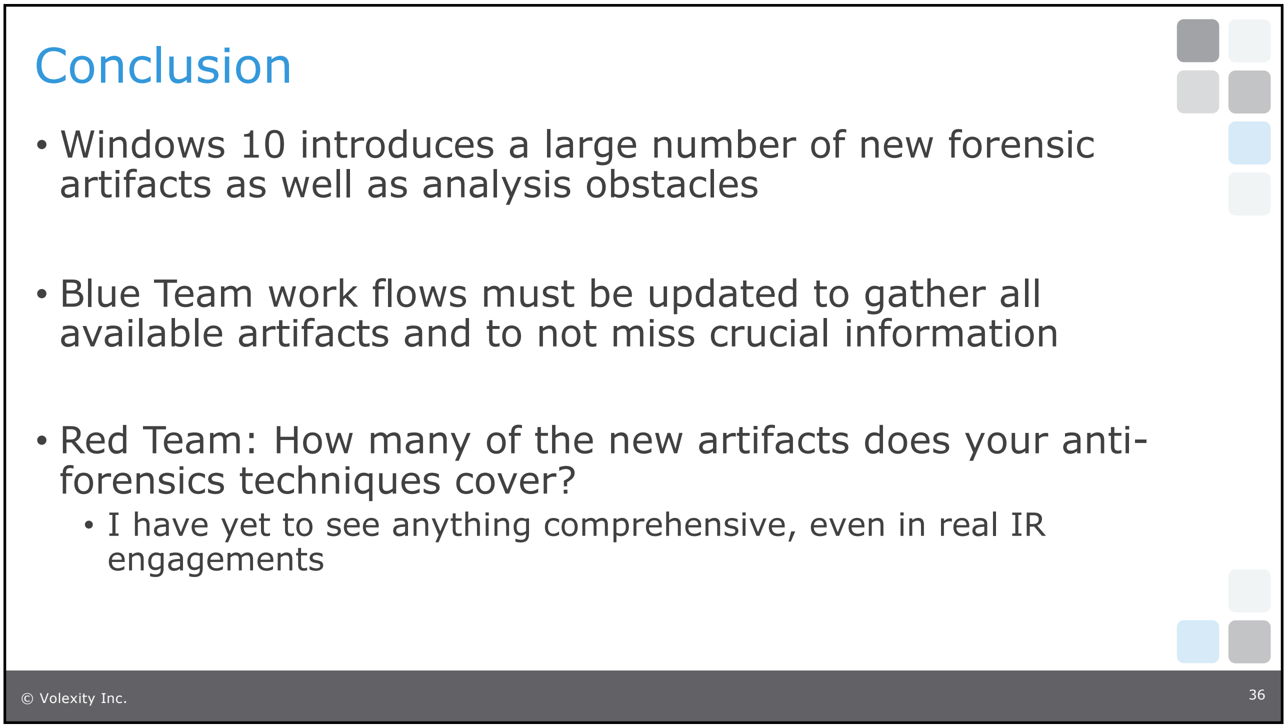
© Volexity Inc. 34

34



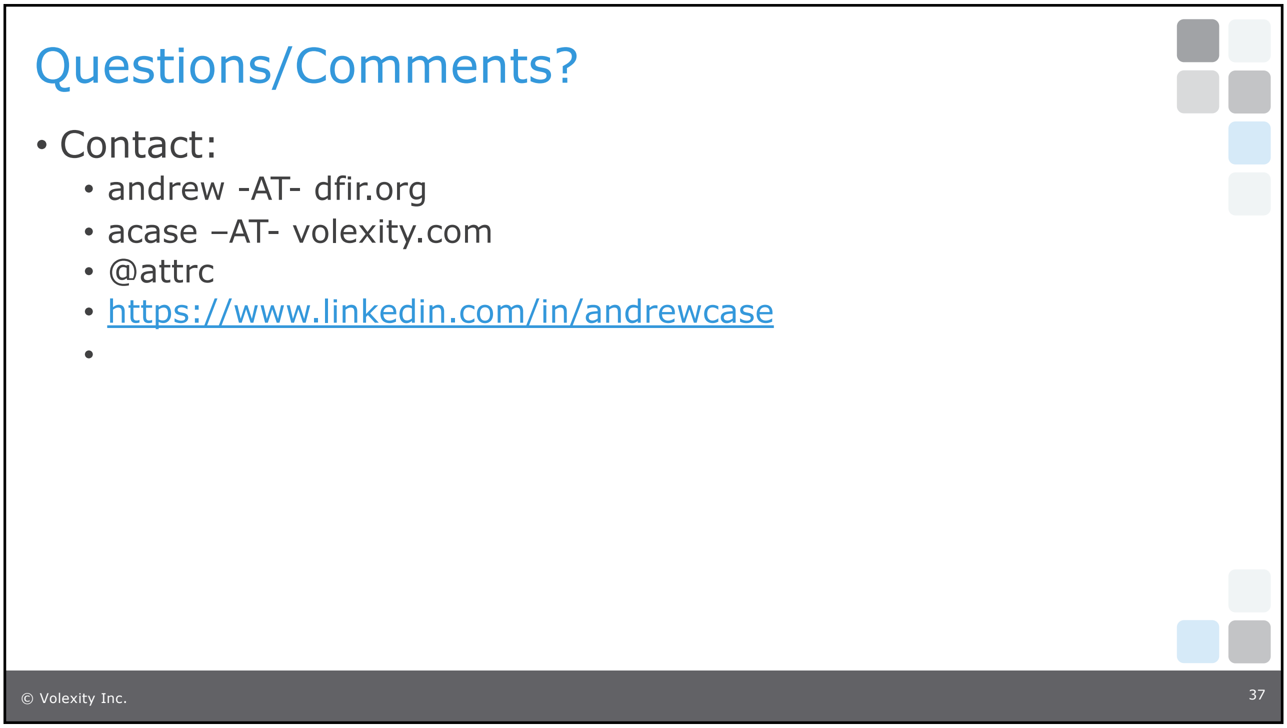
Challenge 5: Volatility Underscore Profiles

- Historically, Windows profiles for Volatility would remain accurate between ”major” updates, such as Service Packs
- The rapid release cycle of Windows 10 has broke this model
- Now, to perform accurate analysis, you must rely on the “underscore” Windows 10 profiles that correspond to the major release
  - Full details at [33]



Conclusion

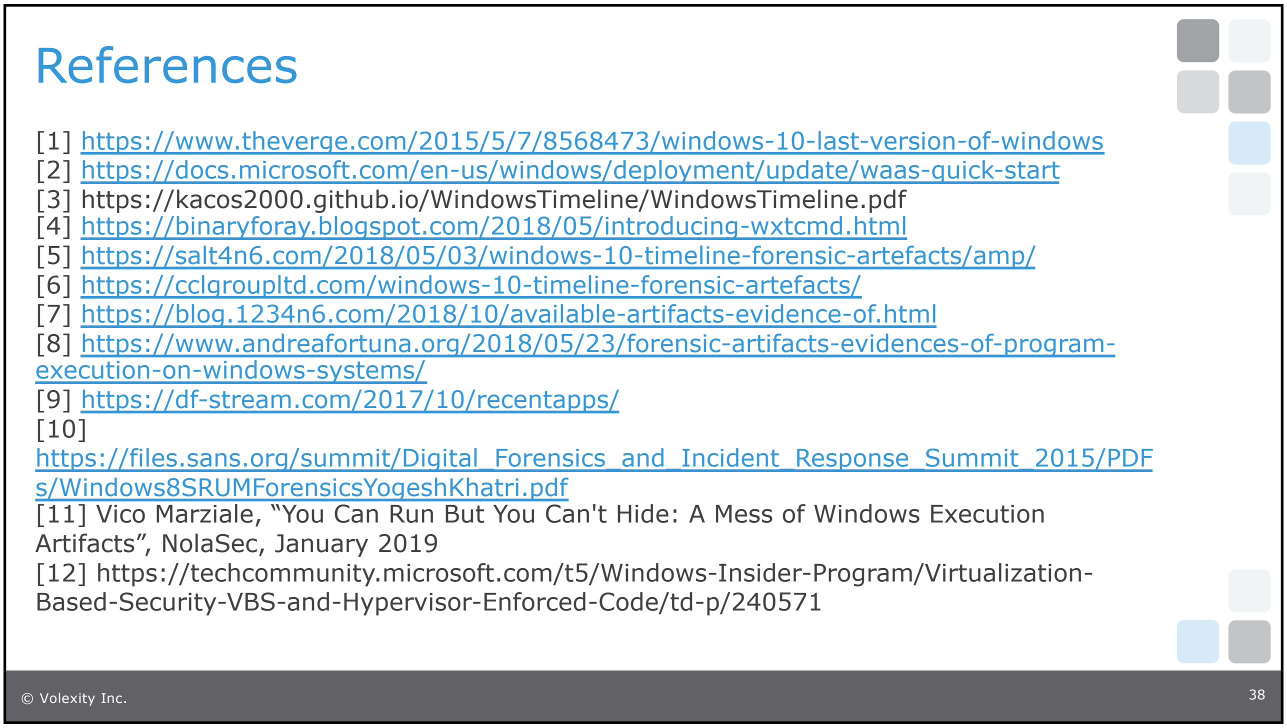
- Windows 10 introduces a large number of new forensic artifacts as well as analysis obstacles
- Blue Team work flows must be updated to gather all available artifacts and to not miss crucial information
- Red Team: How many of the new artifacts does your anti-forensics techniques cover?
  - I have yet to see anything comprehensive, even in real IR engagements



Questions/Comments?

- Contact:
  - andrew -AT- dfir.org
  - acase –AT- volexity.com
  - @attrc
  - https://www.linkedin.com/in/andrewcase
  -

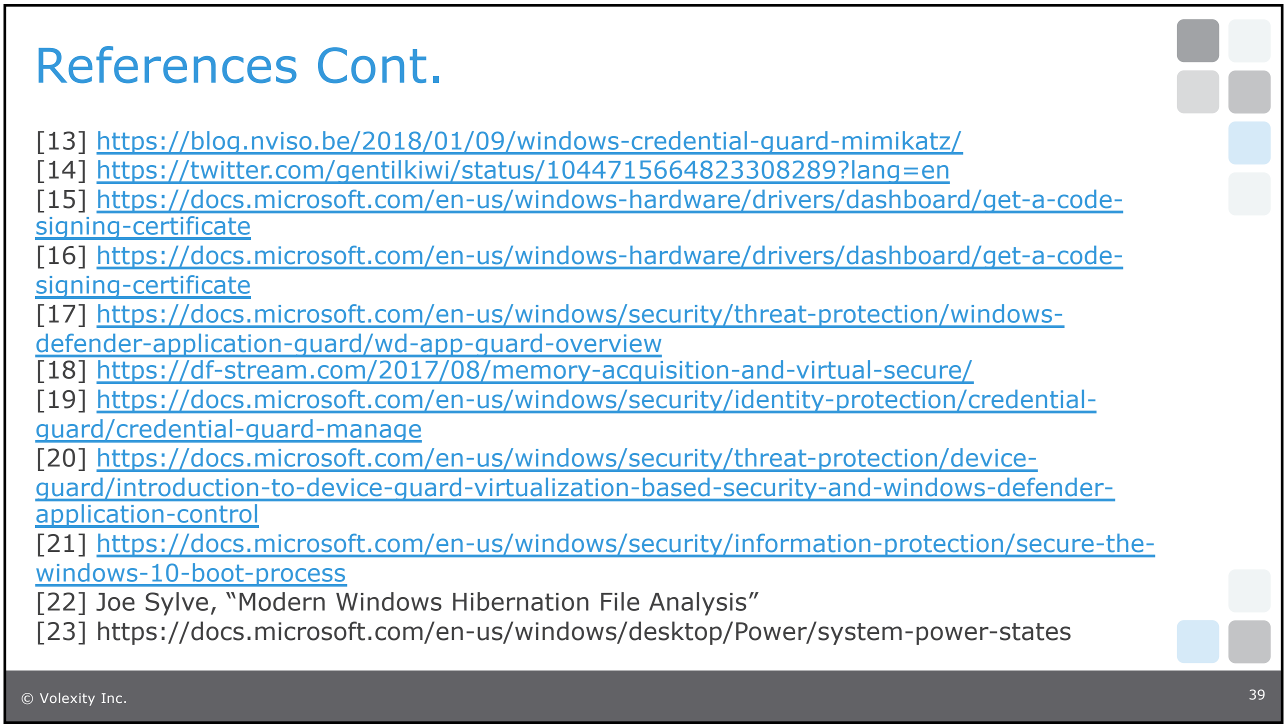
37



References

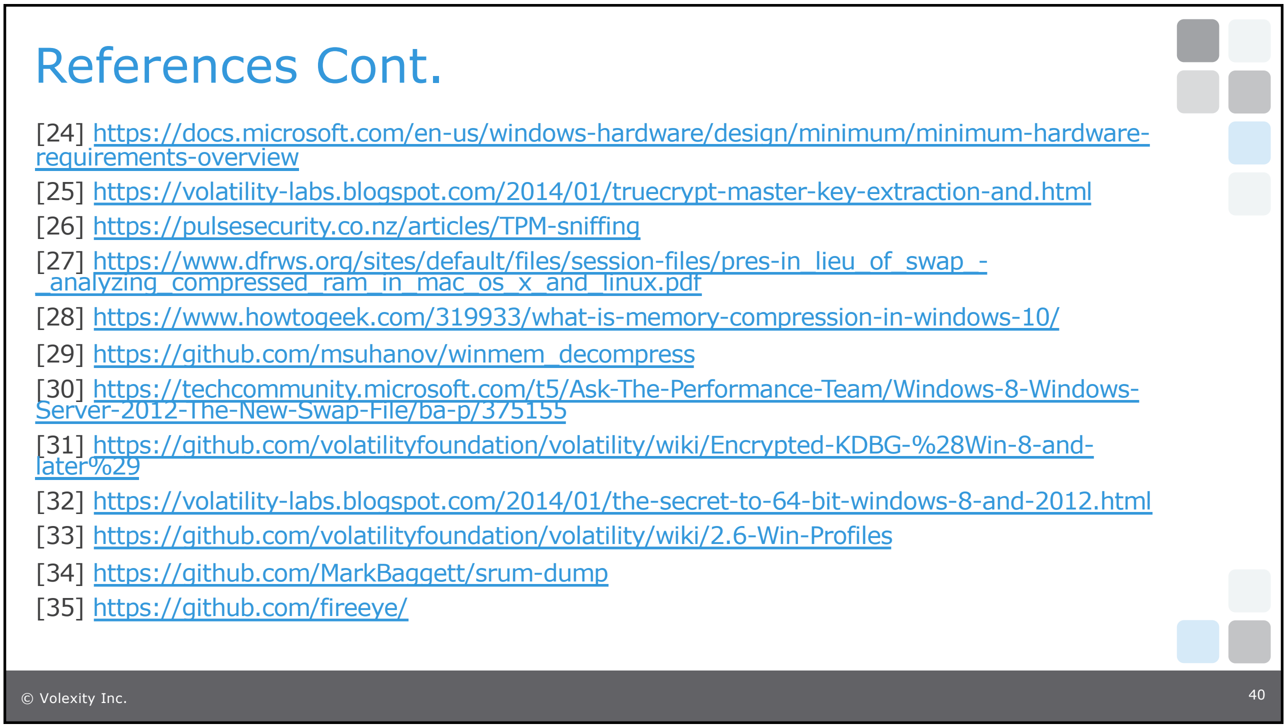
[1] https://www.theverge.com/2015/5/7/8568473/windows-10-last-version-of-windows
[2] https://docs.microsoft.com/en-us/windows/deployment/update/waas-quick-start
[3] https://kacos2000.github.io/WindowsTimeline/WindowsTimeline.pdf
[4] https://binaryforay.blogspot.com/2018/05/introducing-wxtcmd.html
[5] https://salt4n6.com/2018/05/03/windows-10-timeline-forensic-artefacts/amp/
[6] https://cclgroupltd.com/windows-10-timeline-forensic-artefacts/
[7] https://blog.1234n6.com/2018/10/available-artifacts-evidence-of.html
[8] https://www.andreafortuna.org/2018/05/23/forensic-artifacts-evidences-of-program-execution-on-windows-systems/
[9] https://df-stream.com/2017/10/recentapps/
[10] https://files.sans.org/summit/Digital_Forensics_and_Incident_Response_Summit_2015/PDFs/Windows8SRUMForensicsYogeshKhatri.pdf
[11] Vico Marziale, "You Can Run But You Can't Hide: A Mess of Windows Execution Artifacts", NolaSec, January 2019
[12] https://techcommunity.microsoft.com/t5/Windows-Insider-Program/Virtualization-Based-Security-VBS-and-Hypervisor-Enforced-Code/td-p/240571

38



References Cont.

[13] https://blog.nviso.be/2018/01/09/windows-credential-guard-mimikatz/
[14] https://twitter.com/gentilkiwi/status/1044715664823308289?lang=en
[15] https://docs.microsoft.com/en-us/windows-hardware/drivers/dashboard/get-a-code-signing-certificate
[16] https://docs.microsoft.com/en-us/windows-hardware/drivers/dashboard/get-a-code-signing-certificate
[17] https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/wd-app-guard-overview
[18] https://df-stream.com/2017/08/memory-acquisition-and-virtual-secure/
[19] https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
[20] https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control
[21] https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process
[22] Joe Sylve, “Modern Windows Hibernation File Analysis”
[23] https://docs.microsoft.com/en-us/windows/desktop/Power/system-power-states



References Cont.

[24] https://docs.microsoft.com/en-us/windows-hardware/design/minimum/minimum-hardware-requirements-overview
[25] https://volatility-labs.blogspot.com/2014/01/truecrypt-master-key-extraction-and.html
[26] https://pulsesecurity.co.nz/articles/TPM-sniffing
[27] https://www.dfrws.org/sites/default/files/session-files/pres-in_lieu_of_swap_-_analyzing_compressed_ram_in_mac_os_x_and_linux.pdf
[28] https://www.howtogeek.com/319933/what-is-memory-compression-in-windows-10/
[29] https://github.com/msuhanov/winmem_decompress
[30] https://techcommunity.microsoft.com/t5/Ask-The-Performance-Team/Windows-8-Windows-Server-2012-The-New-Swap-File/ba-p/375155
[31] https://github.com/volatilityfoundation/volatility/wiki/Encrypted-KDBG-%28Win-8-and-later%29
[32] https://volatility-labs.blogspot.com/2014/01/the-secret-to-64-bit-windows-8-and-2012.html
[33] https://github.com/volatilityfoundation/volatility/wiki/2.6-Win-Profiles
[34] https://github.com/MarkBaggett/srum-dump
[35] https://github.com/fireeye/