# THE WINDOWS HOUSE OF MIRRORS:

## A ROLLER COASTER TOUR OF THE SUBSYSTEMS YOU USE EVERY DAY.

Stephen Owen

@FoxDeploy

FoxDeploy.com

Automation Engineer

Big Bank

Shaun Cassells

@Cassells

www.shauncassells.com

MVP, Principal Solution Engineer

Jeff Scripter

JPScripter@gmail.com

Application System Engineer

Big Bank

2Pint Software adaptiva vmware 1E DELL Microsoft

| Jeff Scripter | Stephen Owen | Shaun Cassells |
|---|---|---|
| @JeffTheScripter | @FoxDeploy | @cassells |
| IOT Fan | PowerShell is ♡ | Kids in college before age 5 |
| 15 Years | 10 ish years | Forgotten so much |
| Beer, Coffee and Chocolate | Game of Thrones tinfoil | Alfresco and local |

# OUTLINE

- Registry
- COM/DCOM
- WMI
- Component based servicing - SXS
- Telemetry
- DPAPI

# THE REGISTRY

# WHERE DID THIS ALL BEGIN

- In windows 3.1, to organize the COM configuration info.
- In win 95 and NT, Replaced the perfusion of ini files.
- For better performance, the registry was read into memory on boot.
- Allows for permissions to be granularly delegated and give users access.
- Using standard Types (strings, dword, qword, etc)

Hive - Files where the registry data is stored.

Key - sub paths to different settings

Values - the Values

# HOW THE REGISTRY WORKS

- HKLM - Used to store system level settings and configurations.
  - SOFTWARE - Application settings
    - %Systemroot%\system32\config\Software
  - SAM - Security Account manager
    - %Systemroot%\system32\config\SAM
  - SYSTEM - Protocol, services, Drivers
    - %Systemroot%\system32\config\System
    - ControlSet Current - generated for this current boot
      - Set1 - Backups for recovery
  - HARDWARE - Generated on the fly
  - SECURITY  - policies and stored secrets
    - %Systemroot%\system32\config\Security

# HOW THE REGISTRY WORKS

- HKCU - User profile, application and environment settings
  - %userprofile%\NTUser.dat - Kind of
  - This is a session based alias for HKU.

- HKU - All user profiles loaded
  - <SID> - The permanent mounting HKCU for all users
    - %userprofile%\NTUser.dat
  - <SID>_classes - HKCR Permanent mounting location
    - DLL, File Extensions, Defaults
    - %userprofile%\AppData\Local\Microsoft\Windows\usrclass.dat

# HOW THE REGISTRY WORKS

- HKCR - Melding of the user and system settings
  - User settings - HKEY_USERS\<SID>_Classes
  - System settings - HKEY_LOCAL_MACHINE\SOFTWARE\Classes
    - COM object and other DLL registration (CLSID)
    - APPX Registration
    - File extension defaults
    - Shell DLL defaults
    - File icon paths.
  - If there is the same key but different value, the user key wins.

- HKCC
  - Loaded on startup
  - Alias for HKLM\System\CurrentControlSet\HardwareProfiles\Current

# COM/DCOM

# COMPONENT OBJECT MODEL

- This was a way to more easily allow software to interact with each other.
- Mostly for local software interactions, DCOM was added to allow for remote software interactions.
  - Just a COM object with remote access build added.
- COM+ is just the COM but with more bells and whistles (V2)
- Two types:
  - In process – Uses the DLL directly.
  - Out of process – launches and EXE.

# HOW IT WORKS

- Com objects are binary interfaces that are registered in HKR (User or machine)
- DLLs register as a com name and version
  - Com object Interface name
    - Hkey_Classes_root\<Interface>\CLSID
  - CLSID is located
    - Hkey_Classes_Root\CLSID\<CLSID>
- This will locate the binary that can manage the interface.

# PRACTICAL

- There are several applications that can have useful com interfaces like
  - MSI installer
  - windows updates
  - Office
  - RSA soft token

- If you have to troubleshoot errors, The application event log can capture some of the more severe errors.

# WMI

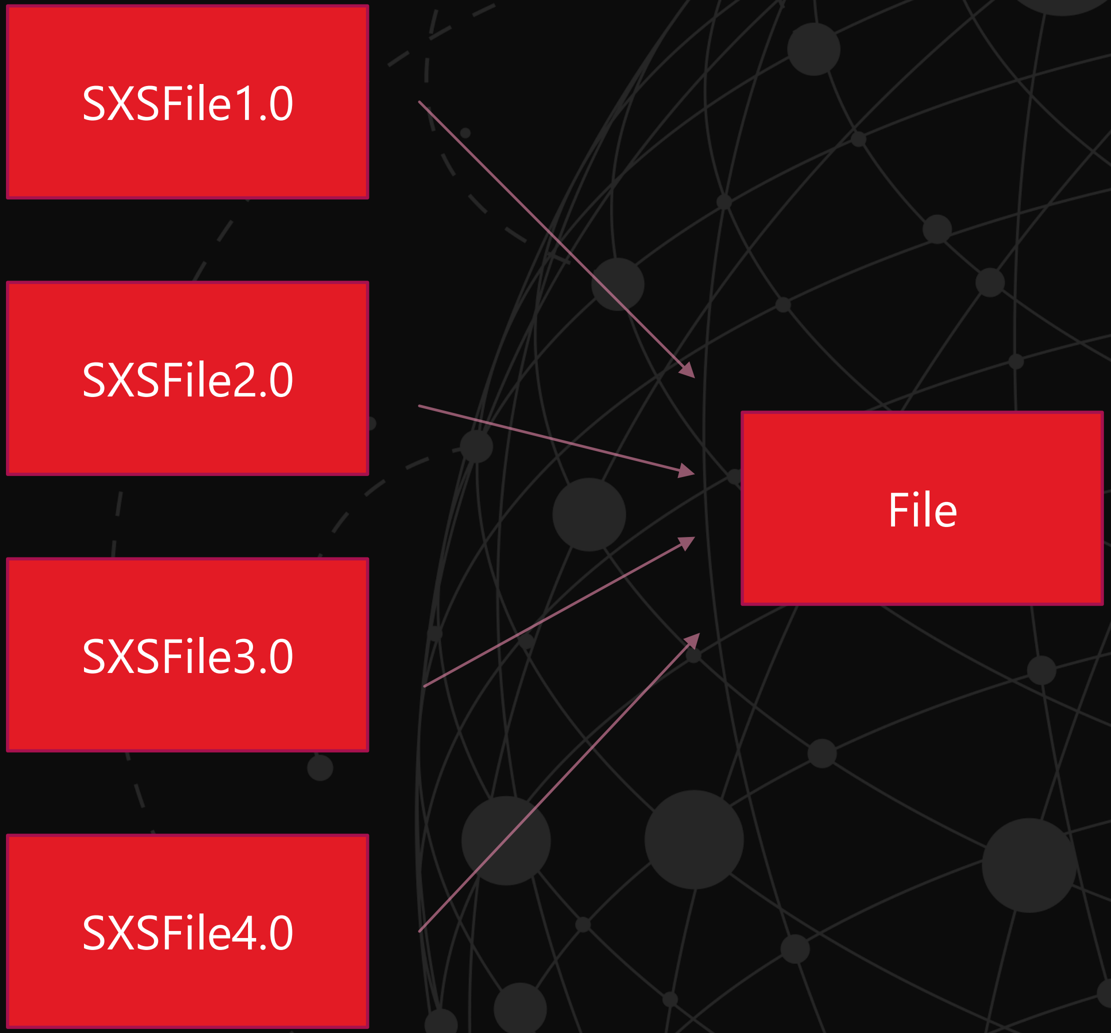
🎺 *T*he skeleton key to basically everything 🎺

# COMPONENT BASED SERVICING

MMS

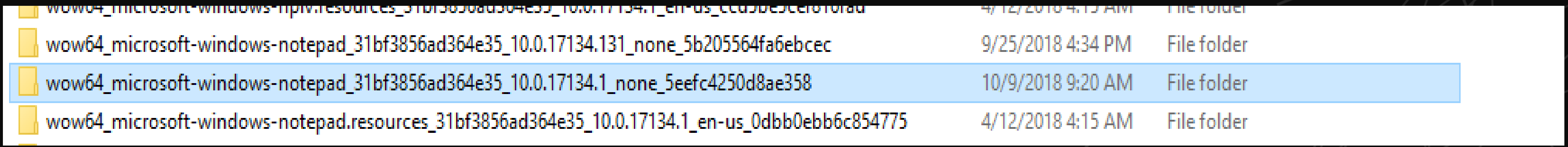
# WHAT IS THE WINDOWS COMPONENT BASED SERVICING

- The subsystem that manages the files for windows.
  - Windows patches
  - MSIs
- Attempts to resolve
  - Missing DLLs
  - DLL Versions
  - Duplicate DLLs
- Where
  - C:\Windows\winsxs
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing

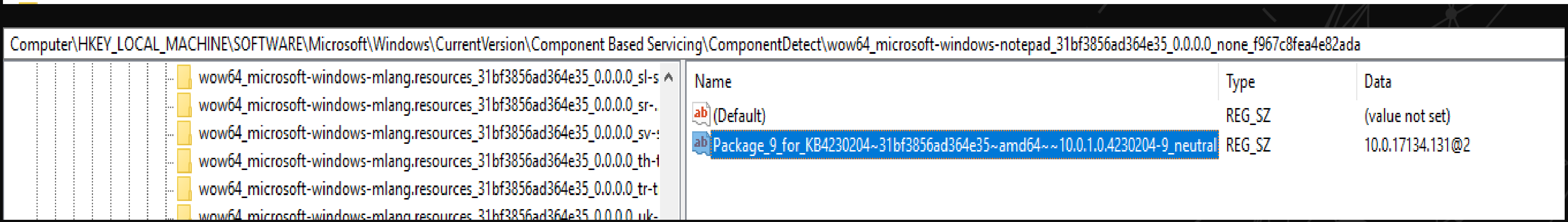


MMS

# TRACING



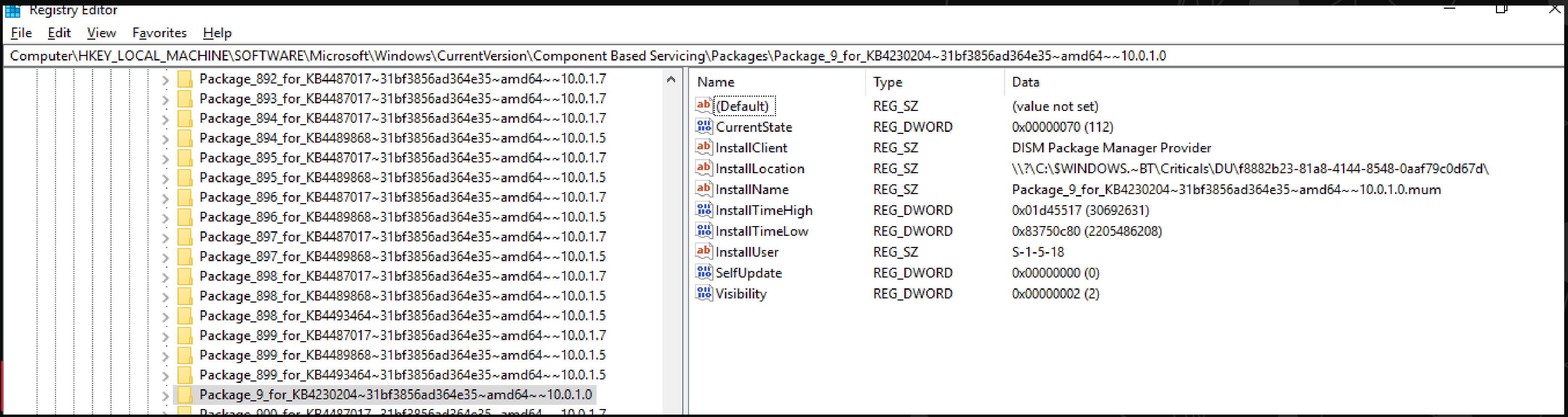
```
wow64_microsoft-windows-npiv.resources_31bf3856ad364e35_10.0.17134.1_en-us_ccd5be5cef6f0fad  4/12/2018 4:15 AM  File folder
wow64_microsoft-windows-notepad_31bf3856ad364e35_10.0.17134.131_none_5b205564fa6ebcec        9/25/2018 4:34 PM  File folder
wow64_microsoft-windows-notepad_31bf3856ad364e35_10.0.17134.1_none_5eefc4250d8ae358          10/9/2018 9:20 AM  File folder
wow64_microsoft-windows-notepad.resources_31bf3856ad364e35_10.0.17134.1_en-us_0dbb0ebb6c854775  4/12/2018 4:15 AM  File folder
```



```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\ComponentDetect\wow64_microsoft-windows-notepad_31bf3856ad364e35_0.0.0.0_none_f967c8fea4e82ada

wow64_microsoft-windows-mlang.resources_31bf3856ad364e35_0.0.0.0_sl-s
wow64_microsoft-windows-mlang.resources_31bf3856ad364e35_0.0.0.0_sr-.
wow64_microsoft-windows-mlang.resources_31bf3856ad364e35_0.0.0.0_sv-
wow64_microsoft-windows-mlang.resources_31bf3856ad364e35_0.0.0.0_th-
wow64_microsoft-windows-mlang.resources_31bf3856ad364e35_0.0.0.0_tr-t
wow64_microsoft-windows-mlang.resources_31bf3856ad364e35_0.0.0.0_uk-

Name                                                                     Type    Data
(Default)                                                                REG_SZ  (value not set)
Package_9_for_KB4230204~31bf3856ad364e35~amd64~~10.0.1.0.4230204-9_neutral  REG_SZ  10.0.17134.131@2
```



```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages\Package_9_for_KB4230204~31bf3856ad364e35~amd64~~10.0.1.0

Package_892_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_893_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_894_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_894_for_KB4489868~31bf3856ad364e35~amd64~~10.0.1.5
Package_895_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_895_for_KB4489868~31bf3856ad364e35~amd64~~10.0.1.5
Package_896_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_896_for_KB4489868~31bf3856ad364e35~amd64~~10.0.1.5
Package_897_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_897_for_KB4489868~31bf3856ad364e35~amd64~~10.0.1.5
Package_898_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_898_for_KB4489868~31bf3856ad364e35~amd64~~10.0.1.5
Package_898_for_KB4493464~31bf3856ad364e35~amd64~~10.0.1.5
Package_899_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7
Package_899_for_KB4489868~31bf3856ad364e35~amd64~~10.0.1.5
Package_899_for_KB4493464~31bf3856ad364e35~amd64~~10.0.1.5
Package_9_for_KB4230204~31bf3856ad364e35~amd64~~10.0.1.0
Package_900_for_KB4487017~31bf3856ad364e35~amd64~~10.0.1.7

Name              Type       Data
(Default)         REG_SZ     (value not set)
CurrentState      REG_DWORD  0x00000070 (112)
InstallClient     REG_SZ     DISM Package Manager Provider
InstallLocation   REG_SZ     \\?\C:\$WINDOWS.~BT\Criticals\DU\f8882b23-81a8-4144-8548-0aaf79c0d67d\
InstallName       REG_SZ     Package_9_for_KB4230204~31bf3856ad364e35~amd64~~10.0.1.0.mum
InstallTimeHigh   REG_DWORD  0x01d45517 (30692631)
InstallTimeLow    REG_DWORD  0x83750c80 (2205486208)
InstallUser       REG_SZ     S-1-5-18
SelfUpdate        REG_DWORD  0x00000000 (0)
Visibility        REG_DWORD  0x00000002 (2)
```

# WHY DOES IT TAKE UP SO MUCH SPACE?

- This allows for easy rollback of patches and software.
- You can clean up the old files, but it prevents uninstalls
  - Cleanup wizard
  - Schedule task
    - \Microsoft\Windows\Servicing – StartComponentCleanup
  - DISM
    - Dism.exe /online /Cleanup-Image /StartComponentcleanup /ResetBase
    - Dism.exe /online /Cleanup-Image /SPSuperseded
- DO NOT DELETE THESE MANUALLY!

# HOW DO I TROUBLESHOOT IT?

- This allows for easy rollback of patches and software.

- You can clean up the old files, but it prevents uninstalls
  - Sxstrace – Exports logging for sxs
  - CheckSur – Win 7 - Integrate checks for sxs
  - Dism – Win 10 - Integrate checks for sxs

- DO NOT DELETE THESE MANUALLY!

MMS

# WINDOWS TELEMETRY

Good data leads to good decisions

Windows Analytics session - https://sched.co/N6fy

# TELEMETRY – HUH WHAT IS IT GOOD FOR?

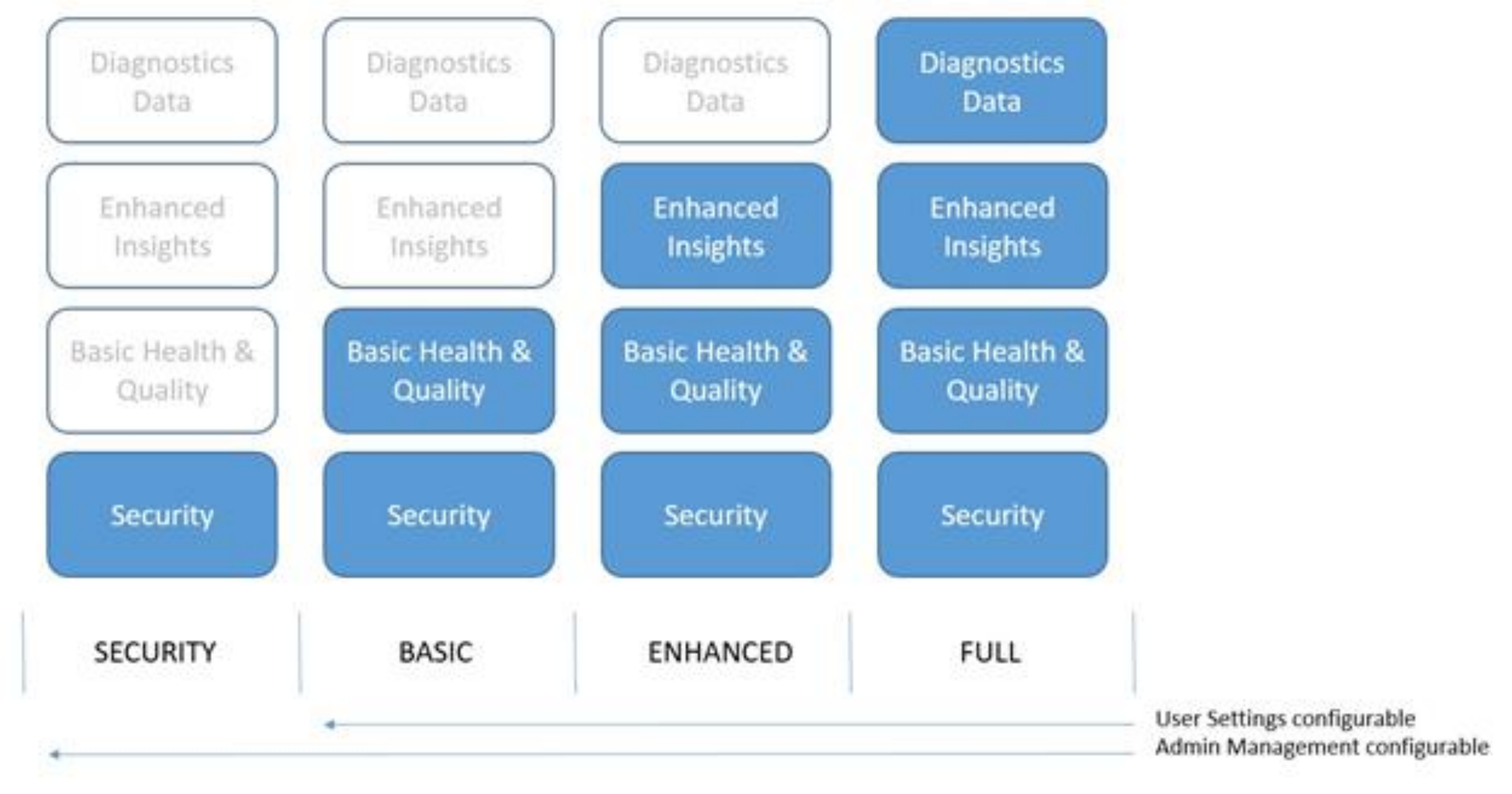
Absolutely EVERYTHING!

What is it?

- Telemetry
- What do I get out of the deal?

MMS

# WINDOWS TELEMETRY



| SECURITY | BASIC | ENHANCED | FULL |
|---|---|---|---|
| Diagnostics Data | Diagnostics Data | Diagnostics Data | Diagnostics Data |
| Enhanced Insights | Enhanced Insights | Enhanced Insights | Enhanced Insights |
| Basic Health & Quality | Basic Health & Quality | Basic Health & Quality | Basic Health & Quality |
| Security | Security | Security | Security |

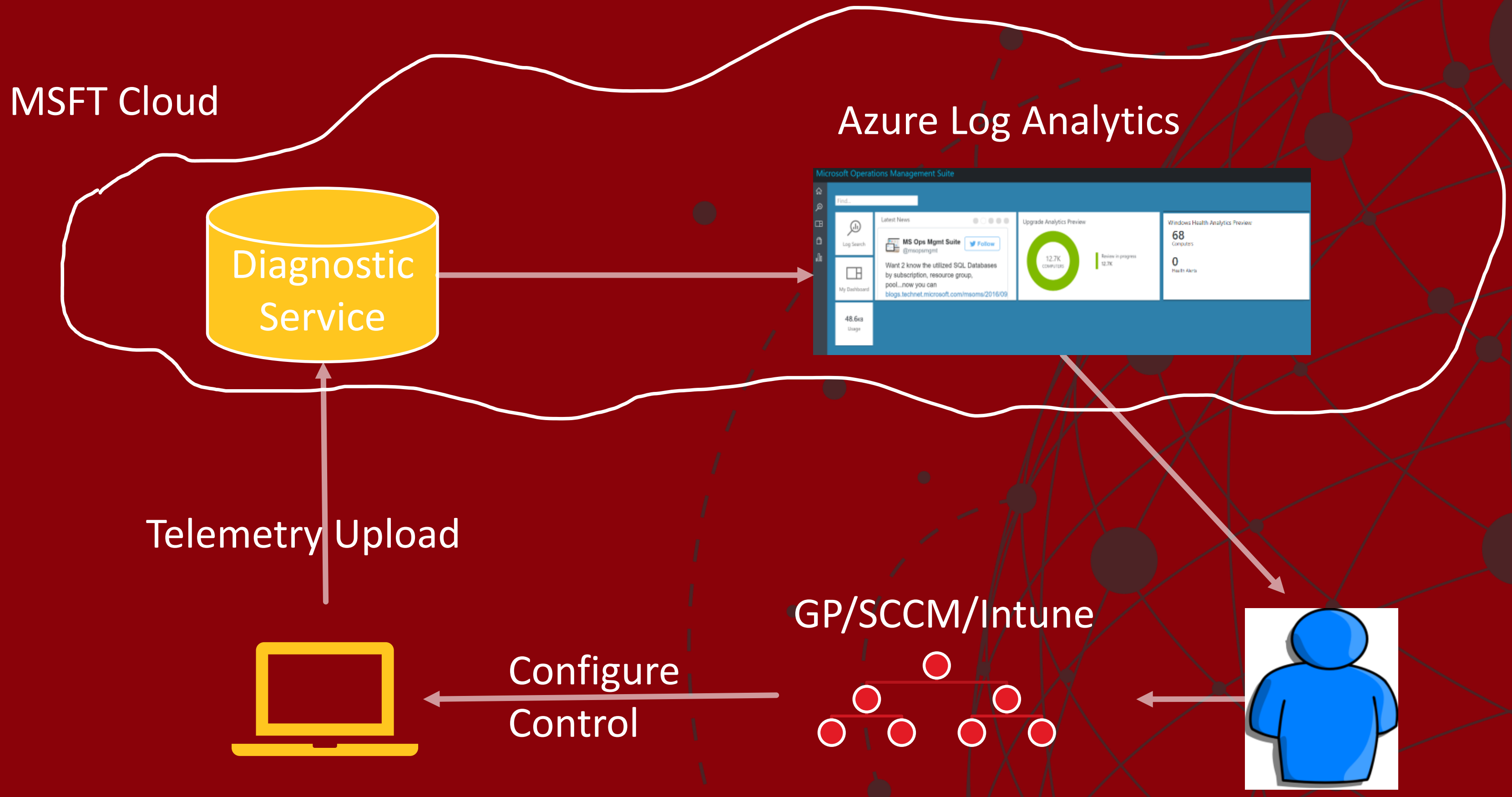
MMS

# Windows Analytics Data Flow

MSFT, as “IT admin” for consumers, uses diagnostic data to ensure OS, app and driver releases land with the right level of quality/health/compat

Windows Analytics gives IT diagnostic-based insights to their devices, exposed via Azure log analytics

IT controls the level of diagnostic data collected, which impacts Analytics availability



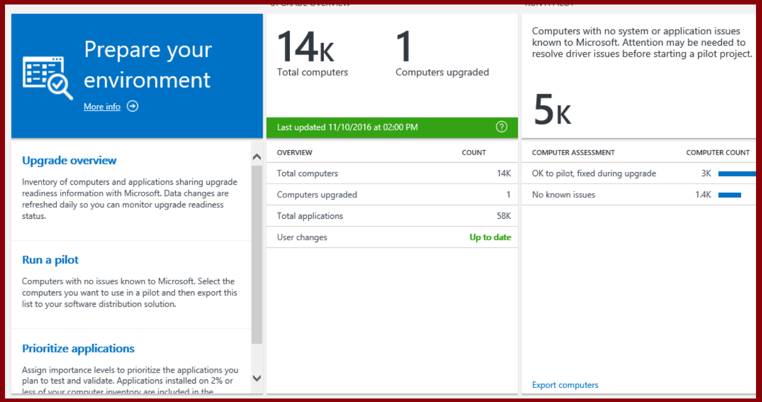
Value to customer: Reduce TCO via proactive insights

Value to MSFT: Diagnostic data helps us improve the product, staying current helps our ecosystem

# WINDOWS ANALYTICS

Data-driven insights to reduce the cost of deploying, servicing, and supporting Windows 10

## Upgrade Readiness



Prepare your environment

More info

**Upgrade overview**

Inventory of computers and applications sharing upgrade readiness information with Microsoft. Data changes are refreshed daily so you can monitor upgrade readiness status.

**Run a pilot**

Computers with no issues known to Microsoft. Select the computers you want to use in a pilot and then export this list to your software distribution solution.

**Prioritize applications**

Assign importance levels to prioritize the applications you plan to test and validate. Applications installed on 2% or less of your computer inventory are included in the

14K Total computers

1 Computers upgraded

Last updated 11/10/2016 at 02:00 PM

| OVERVIEW | COUNT |
|---|---|
| Total computers | 14K |
| Computers upgraded | 1 |
| Total applications | 58K |
| User changes | Up to date |

Computers with no system or application issues known to Microsoft. Attention may be needed to resolve driver issues before starting a pilot project.

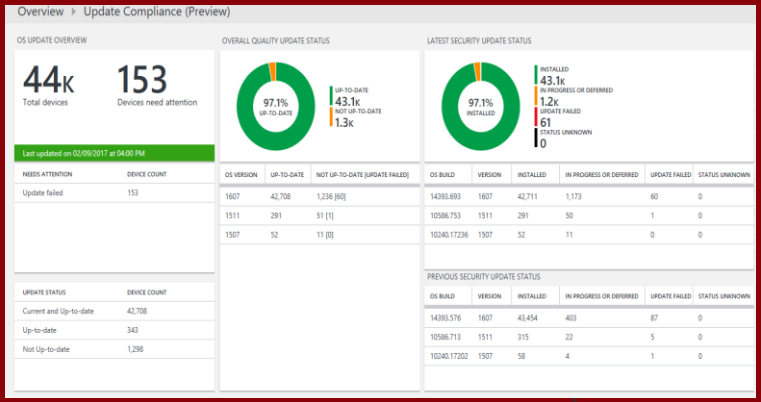
5K

| COMPUTER ASSESSMENT | COMPUTER COUNT |
|---|---|
| OK to pilot, fixed during upgrade | 3K |
| No known issues | 1.4K |

Export computers

**Plan upgrades** by identifying devices that are ready, identify and resolve app and driver compatibility blockers

## Update Compliance



Overview ▸ Update Compliance (Preview)

OS UPDATE OVERVIEW

44K Total devices

153 Devices need attention

Last updated on 02/09/2017 at 04:00 PM

| NEEDS ATTENTION | DEVICE COUNT |
|---|---|
| Update failed | 153 |

| UPDATE STATUS | DEVICE COUNT |
|---|---|
| Current and Up-to-date | 42,708 |
| Up-to-date | 343 |
| Not Up-to-date | 1,298 |

OVERALL QUALITY UPDATE STATUS

UP-TO-DATE 43.1K

NOT UP-TO-DATE 1.3K

| OS VERSION | UP-TO-DATE | NOT UP-TO-DATE [UPDATE FAILED] |
|---|---|---|
| 1607 | 42,708 | 1,236 [60] |
| 1511 | 291 | 51 [1] |
| 1507 | 52 | 11 [0] |

LATEST SECURITY UPDATE STATUS

INSTALLED 43.1K

IN PROGRESS OR DEFERRED 1.2K

UPDATE FAILED 61

STATUS UNKNOWN 0

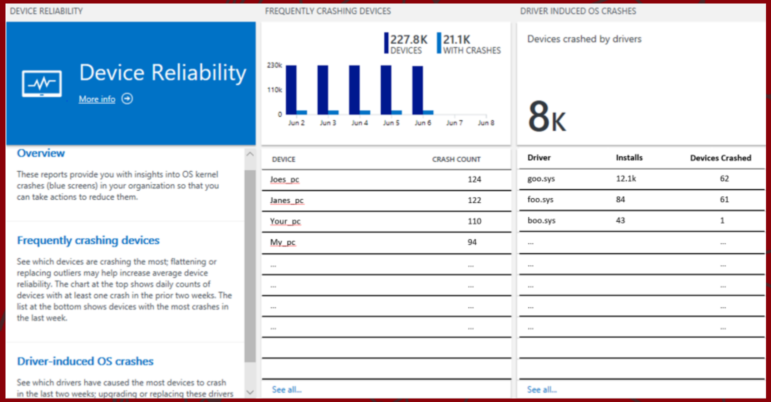
| OS BUILD | VERSION | INSTALLED | IN PROGRESS OR DEFERRED | UPDATE FAILED | STATUS UNKNOWN |
|---|---|---|---|---|---|
| 14393.693 | 1607 | 42,711 | 1,173 | 60 | 0 |
| 10586.753 | 1511 | 291 | 50 | 1 | 0 |
| 10240.17236 | 1507 | 52 | 11 | 0 | 0 |

PREVIOUS SECURITY UPDATE STATUS

| OS BUILD | VERSION | INSTALLED | IN PROGRESS OR DEFERRED | UPDATE FAILED | STATUS UNKNOWN |
|---|---|---|---|---|---|
| 14393.576 | 1607 | 43,454 | 403 | 87 | 0 |
| 10586.713 | 1511 | 315 | 22 | 5 | 0 |
| 10240.17202 | 1507 | 58 | 4 | 1 | 0 |

**Ensure update and antimalware compliance** with timely reports for all your devices (even those on the road)

## Device Health



DEVICE RELIABILITY

Device Reliability

More info

**Overview**

These reports provide you with insights into OS kernel crashes (blue screens) in your organization so that you can take actions to reduce them.

**Frequently crashing devices**

See which devices are crashing the most; flattening or replacing outliers may help increase average device reliability. The chart at the top shows daily counts of devices with at least one crash in the prior two weeks. The list at the bottom shows devices with the most crashes in the last week.

**Driver-induced OS crashes**

See which drivers have caused the most devices to crash in the last two weeks; upgrading or replacing these drivers

FREQUENTLY CRASHING DEVICES

| DEVICE | CRASH COUNT |
|---|---|
| Joes_pc | 124 |
| Janes_pc | 122 |
| Your_pc | 110 |
| My_pc | 94 |
| ... | ... |
| ... | ... |
| ... | ... |
| ... | ... |

See all...

DRIVER INDUCED OS CRASHES

Devices crashed by drivers

8K

| Driver | Installs | Devices Crashed |
|---|---|---|
| goo.sys | 12.1k | 62 |
| foo.sys | 84 | 61 |
| boo.sys | 43 | 1 |
| ... | | ... |
| ... | | ... |
| ... | | ... |
| ... | | ... |
| ... | | ... |

See all...

**Reduce support costs** by pro-actively identifying and remediating top end-user impacting issues

No agents to deploy

Works with your existing infra; AAD or AD, SCCM or Intune, win32 or store apps, ...

No additional cost beyond existing Windows licenses

# WHAT CAN I SEE?

- DDV – Diagnostic Data Viewer
- Windows Feedback Hub – Things that are broken
- Wire Shark - Comms
- Postman - APIs

# TELEMETRY – HUH WHAT IS IT GOOD FOR?

Absolutely EVERYTHING!

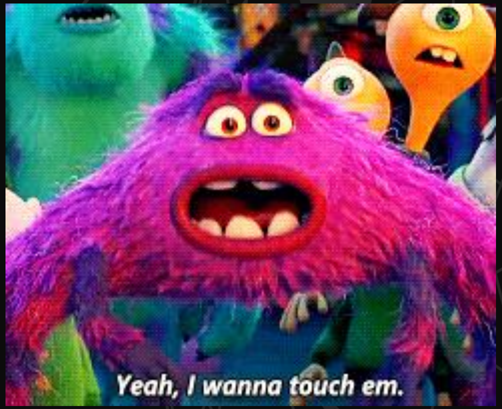
Cloud

- Telemetry
- I get benefits
- I touched it

Can I Gather my own?

The Tale of the Slow Registry

Windows Performance tool Kit



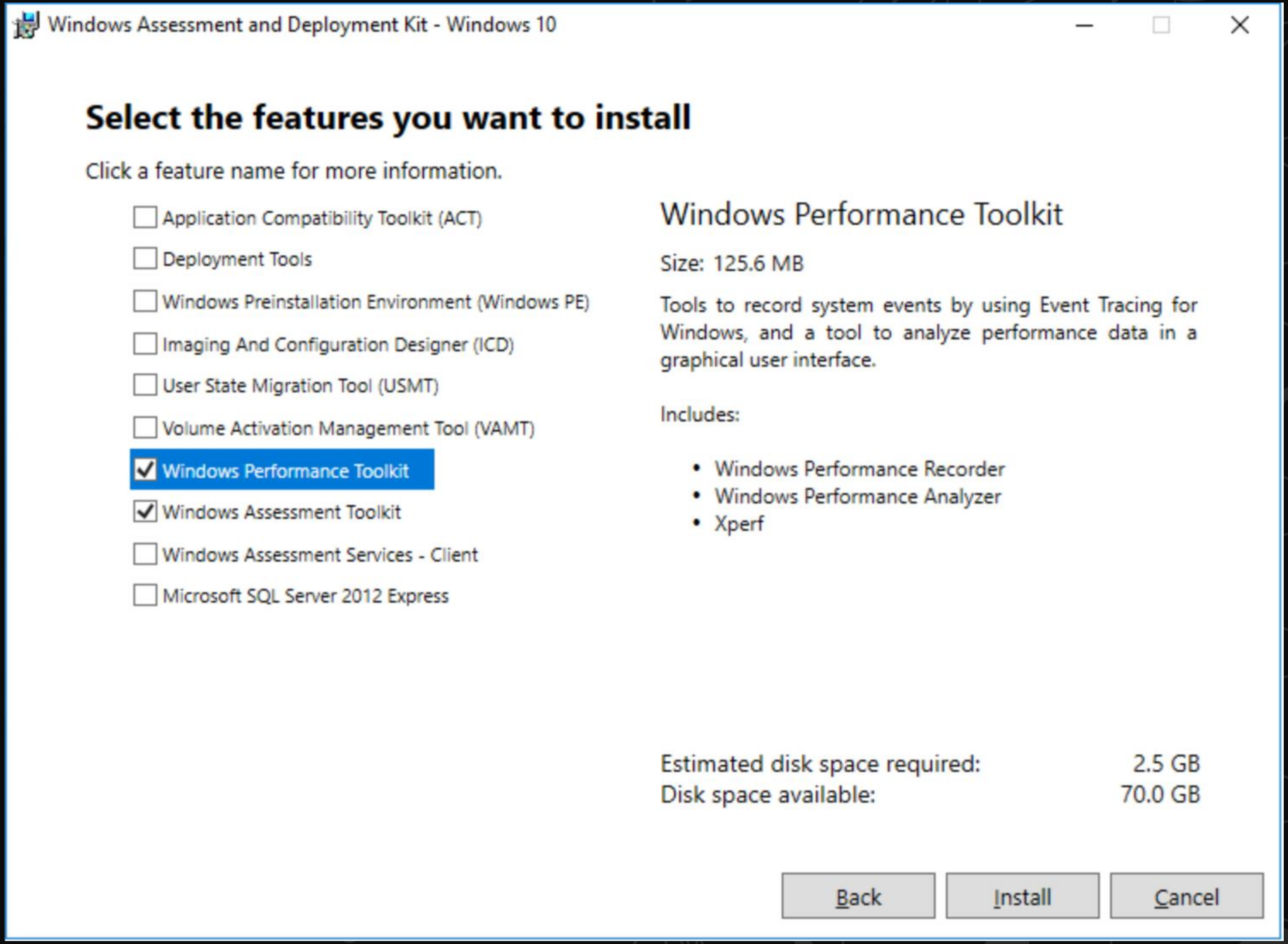
# WHAT IS WPT AND WHERE DO I GET IT?

- Windows Performance Recorder (WPR)
  - Allows you to capture a trace for the problem you want to investigate
  - Get it from the ADK – aka.ms/adk

- Windows Performance Analyzer (WPA)
  - Exposes information about the system and allows you to do performance analysis
  - Get it in the Microsoft STORE!

MMS

# WINDOWS PERFORMANCE TOOLKIT



Windows Assessment and Deployment Kit - Windows 10

## Select the features you want to install

Click a feature name for more information.

- □ Application Compatibility Toolkit (ACT)
- □ Deployment Tools
- □ Windows Preinstallation Environment (Windows PE)
- □ Imaging And Configuration Designer (ICD)
- □ User State Migration Tool (USMT)
- □ Volume Activation Management Tool (VAMT)
- ☑ Windows Performance Toolkit
- ☑ Windows Assessment Toolkit
- □ Windows Assessment Services - Client
- □ Microsoft SQL Server 2012 Express

### Windows Performance Toolkit

Size: 125.6 MB

Tools to record system events by using Event Tracing for Windows, and a tool to analyze performance data in a graphical user interface.

Includes:

- Windows Performance Recorder
- Windows Performance Analyzer
- Xperf

Estimated disk space required: 2.5 GB
Disk space available: 70.0 GB

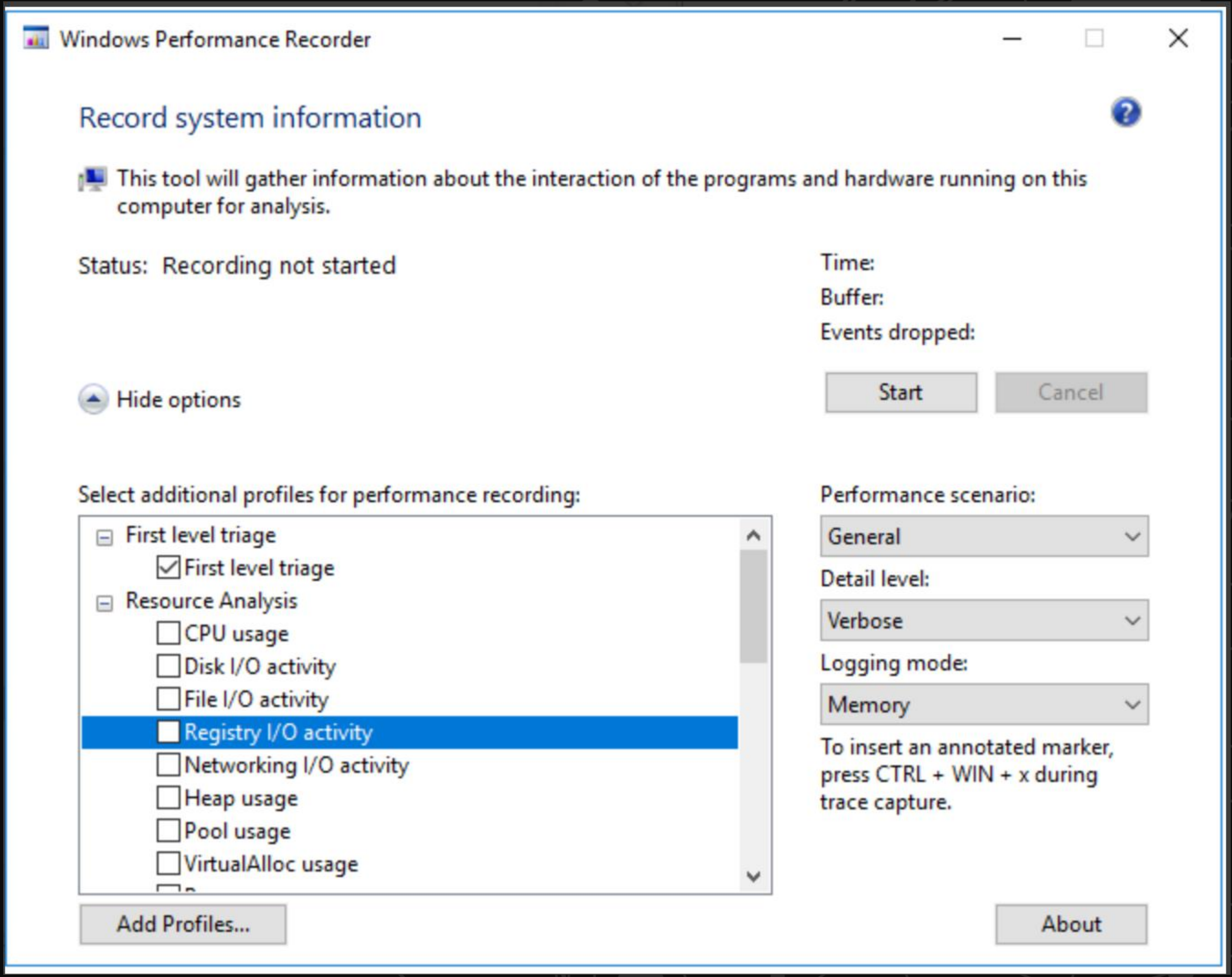
# HOW DO I CAPTURE A TRACE?

- Start Windows Performance Recorder
  - Prior to 1903 index service won't find it ☹
- Once you start **SHOW HIDE OPTIONS**

**Replication!**

- **Windows Metrics Tool kit**

*metrics emptyapp64 RegWriteHKLM -t*



Windows Performance Recorder

Record system information

This tool will gather information about the interaction of the programs and hardware running on this computer for analysis.

Status: Recording not started

Time:
Buffer:
Events dropped:

Hide options

Select additional profiles for performance recording:

- First level triage
  - ☑ First level triage
- Resource Analysis
  - □ CPU usage
  - □ Disk I/O activity
  - □ File I/O activity
  - □ Registry I/O activity
  - □ Networking I/O activity
  - □ Heap usage
  - □ Pool usage
  - □ VirtualAlloc usage

Performance scenario: General

Detail level: Verbose

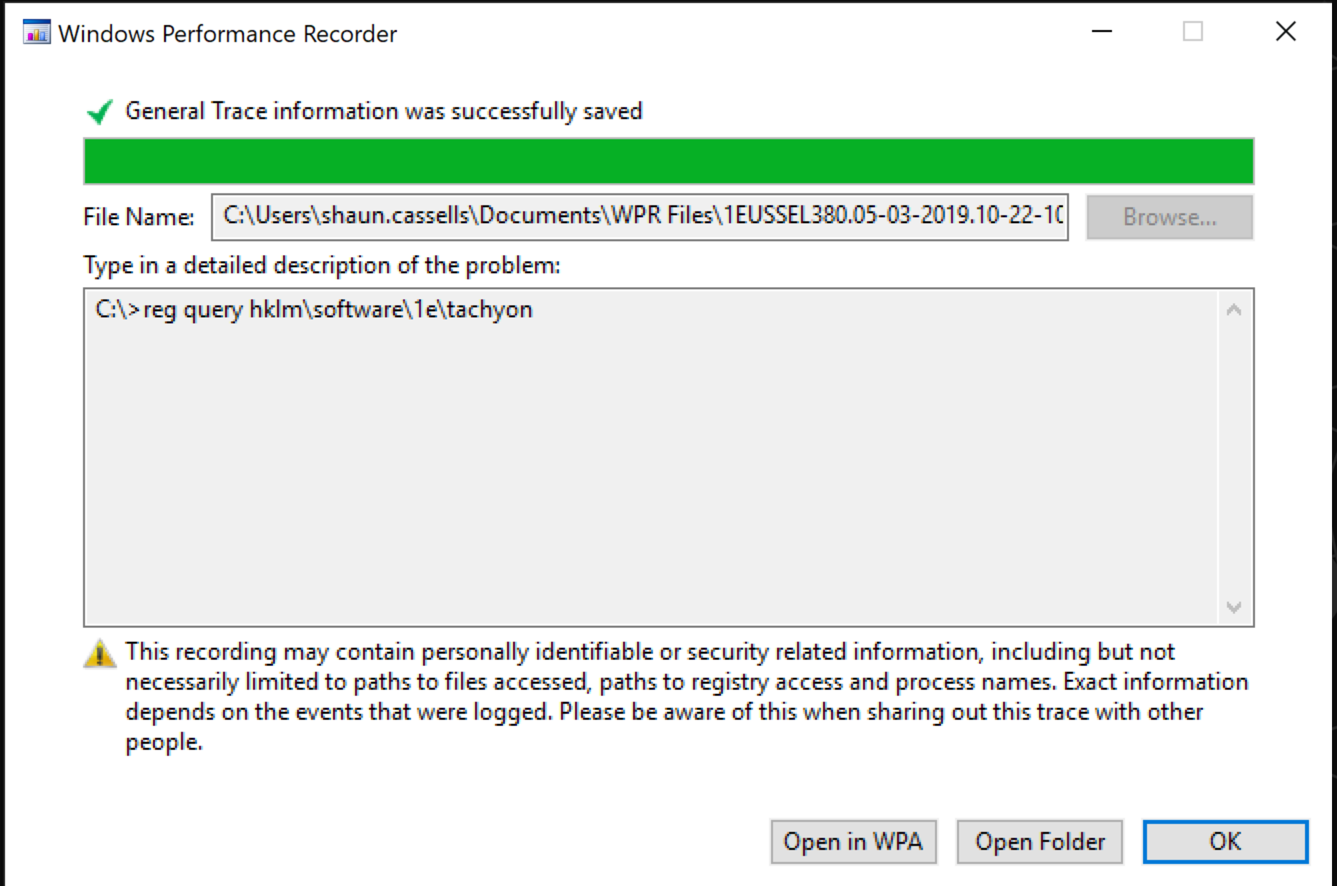
Logging mode: Memory

To insert an annotated marker, press CTRL + WIN + x during trace capture.

MMS

# SAVING

- Get a cuppa this is going to take a minute
- Saves to local Document\WPR Files\ -> If your documents are redirected expect to take longer
- Yea for **Open in WPA**



✓ General Trace information was successfully saved

File Name: C:\Users\shaun.cassells\Documents\WPR Files\1EUSSEL380.05-03-2019.10-22-1(

Type in a detailed description of the problem:

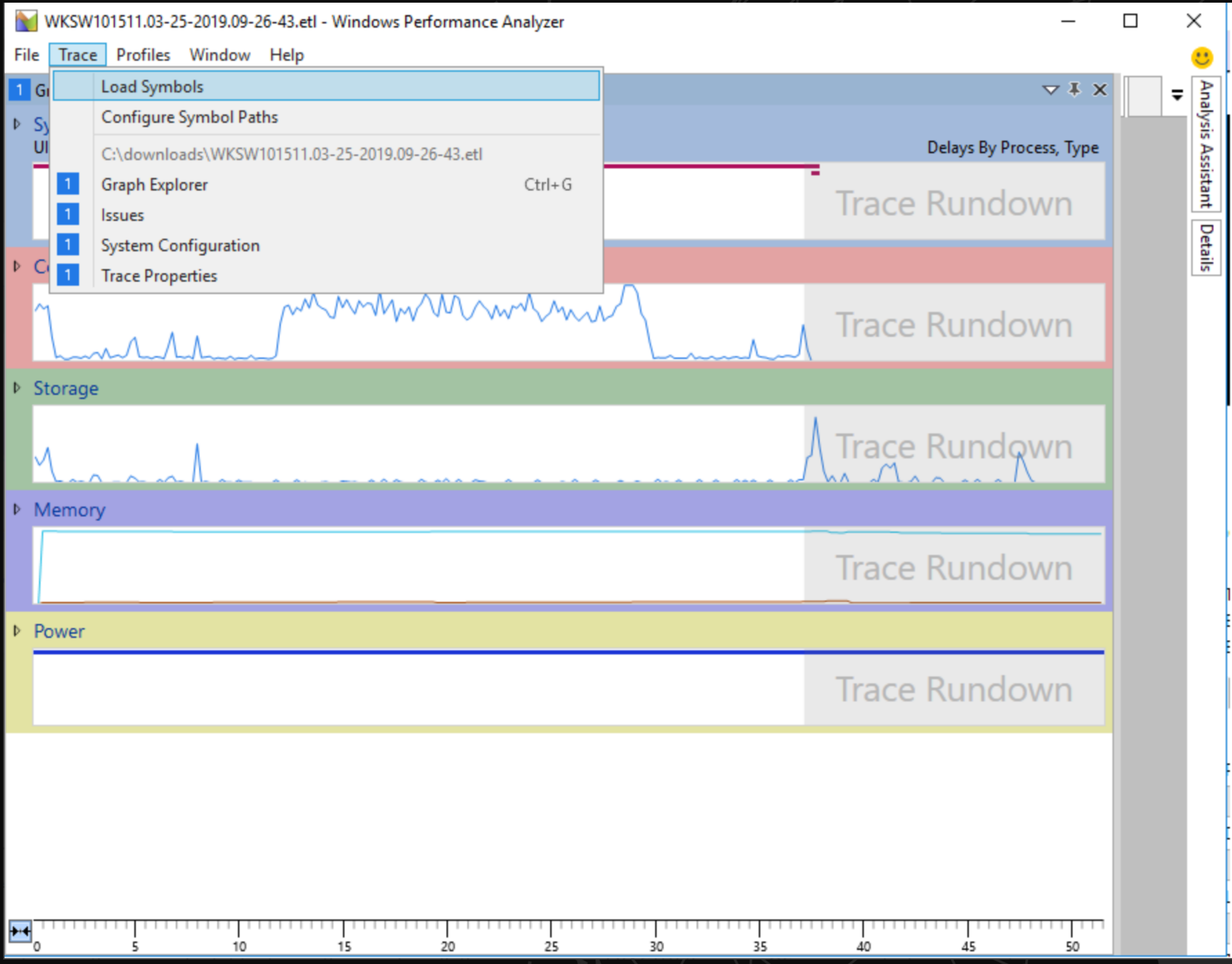
```
C:\>reg query hklm\software\1e\tachyon
```

This recording may contain personally identifiable or security related information, including but not necessarily limited to paths to files accessed, paths to registry access and process names. Exact information depends on the events that were logged. Please be aware of this when sharing out this trace with other people.

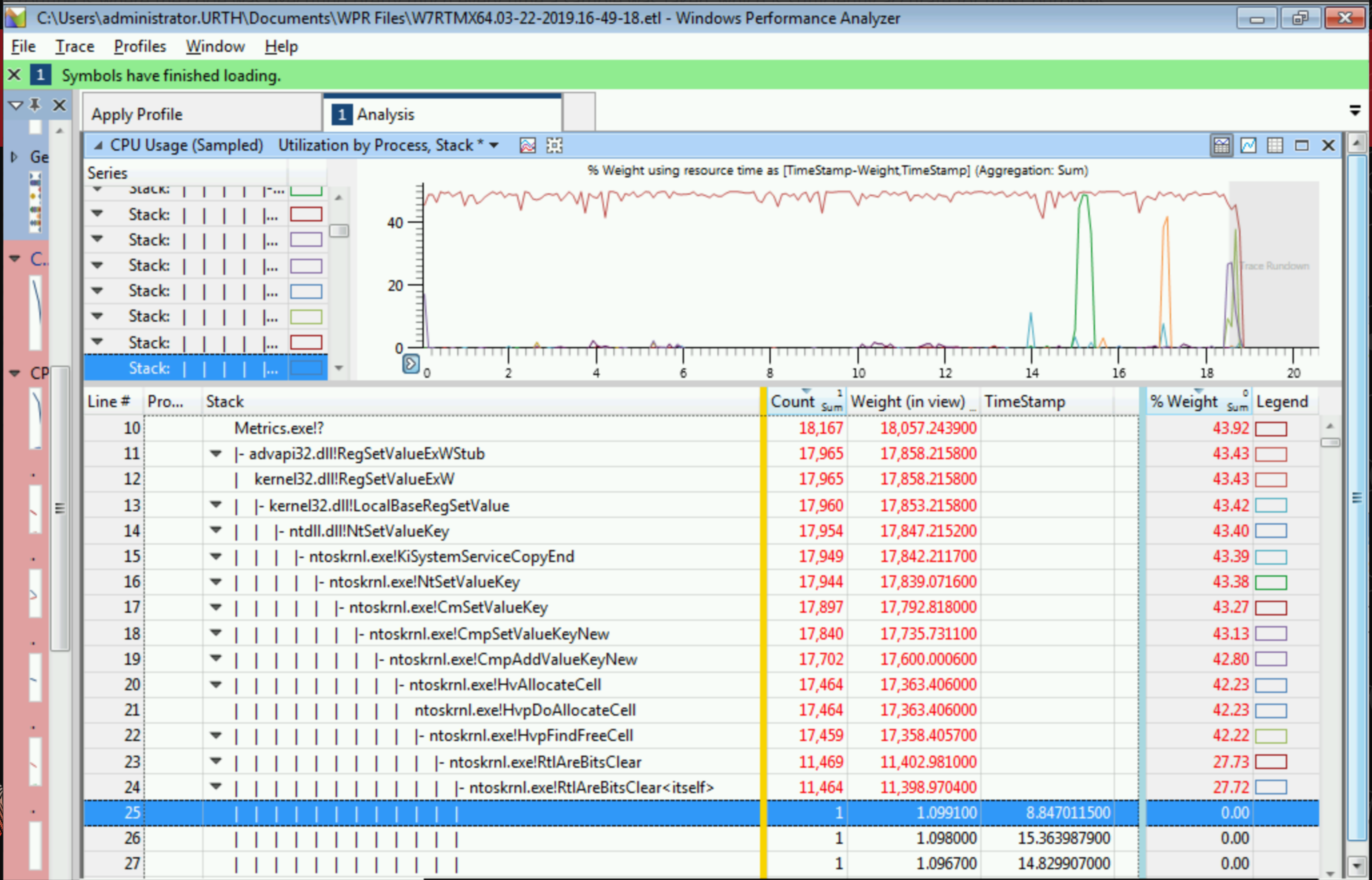
MMS

# OVERVIEW OF WPA

- Load Symbols may take a while
  - More Tea!



MMS



C:\Users\administrator.URTH\Documents\WPR Files\W7RTMX64.03-22-2019.16-49-18.etl - Windows Performance Analyzer

Symbols have finished loading.

<table>
<tr><th>Line #</th><th>Pro...</th><th>Stack</th><th>Count Sum</th><th>Weight (in view)</th><th>TimeStamp</th><th>% Weight Sum</th><th>Legend</th></tr>
<tr><td>10</td><td></td><td>Metrics.exe!?</td><td>18,167</td><td>18,057.243900</td><td></td><td>43.92</td><td>🟥</td></tr>
<tr><td>11</td><td></td><td>▼ |- advapi32.dll!RegSetValueExWStub</td><td>17,965</td><td>17,858.215800</td><td></td><td>43.43</td><td>🟥</td></tr>
<tr><td>12</td><td></td><td>| kernel32.dll!RegSetValueExW</td><td>17,965</td><td>17,858.215800</td><td></td><td>43.43</td><td>🟥</td></tr>
<tr><td>13</td><td></td><td>▼ | |- kernel32.dll!LocalBaseRegSetValue</td><td>17,960</td><td>17,853.215800</td><td></td><td>43.42</td><td>🟦</td></tr>
<tr><td>14</td><td></td><td>▼ | | |- ntdll.dll!NtSetValueKey</td><td>17,954</td><td>17,847.215200</td><td></td><td>43.40</td><td>🟦</td></tr>
<tr><td>15</td><td></td><td>▼ | | | |- ntoskrnl.exe!KiSystemServiceCopyEnd</td><td>17,949</td><td>17,842.211700</td><td></td><td>43.39</td><td>🟦</td></tr>
<tr><td>16</td><td></td><td>▼ | | | | |- ntoskrnl.exe!NtSetValueKey</td><td>17,944</td><td>17,839.071600</td><td></td><td>43.38</td><td>🟩</td></tr>
<tr><td>17</td><td></td><td>▼ | | | | | |- ntoskrnl.exe!CmSetValueKey</td><td>17,897</td><td>17,792.818000</td><td></td><td>43.27</td><td>🟥</td></tr>
<tr><td>18</td><td></td><td>▼ | | | | | | |- ntoskrnl.exe!CmpSetValueKeyNew</td><td>17,840</td><td>17,735.731100</td><td></td><td>43.13</td><td>🟪</td></tr>
<tr><td>19</td><td></td><td>▼ | | | | | | | |- ntoskrnl.exe!CmpAddValueKeyNew</td><td>17,702</td><td>17,600.000600</td><td></td><td>42.80</td><td>🟪</td></tr>
<tr><td>20</td><td></td><td>▼ | | | | | | | | |- ntoskrnl.exe!HvAllocateCell</td><td>17,464</td><td>17,363.406000</td><td></td><td>42.23</td><td>🟦</td></tr>
<tr><td>21</td><td></td><td>| | | | | | | | | ntoskrnl.exe!HvpDoAllocateCell</td><td>17,464</td><td>17,363.406000</td><td></td><td>42.23</td><td>🟦</td></tr>
<tr><td>22</td><td></td><td>▼ | | | | | | | | | |- ntoskrnl.exe!HvpFindFreeCell</td><td>17,459</td><td>17,358.405700</td><td></td><td>42.22</td><td>🟩</td></tr>
<tr><td>23</td><td></td><td>▼ | | | | | | | | | | |- ntoskrnl.exe!RtlAreBitsClear</td><td>11,469</td><td>11,402.981000</td><td></td><td>27.73</td><td>🟥</td></tr>
<tr><td>24</td><td></td><td>▼ | | | | | | | | | | | |- ntoskrnl.exe!RtlAreBitsClear&lt;itself&gt;</td><td>11,464</td><td>11,398.970400</td><td></td><td>27.72</td><td>🟦</td></tr>
<tr><td>25</td><td></td><td>| | | | | | | | | | | |</td><td>1</td><td>1.099100</td><td>8.847011500</td><td>0.00</td><td></td></tr>
<tr><td>26</td><td></td><td>| | | | | | | | | | | |</td><td>1</td><td>1.098000</td><td>15.363987900</td><td>0.00</td><td></td></tr>
<tr><td>27</td><td></td><td>| | | | | | | | | | | |</td><td>1</td><td>1.096700</td><td>14.829907000</td><td>0.00</td><td></td></tr>
</table>

# SLOW REGISTRY WRITE

Registry Write was slow on Windows 7

1. Installed the Windows Performance Toolkit and Windows Performance Analyzer
2. Recorded the action
3. Reviewed the action
4. Found the step with the most delay
5. Bingle FTW!

**Summary**: Fixed in windows 10!

# DTRACE FOR WINDOWS

What is the future?

ETW is so static

DTRACE!!!

Open Source as of 2016

Used in all Insider Builds

- https://techcommunity.microsoft.com/t5/Windows-Kernel-Internals/DTrace-on-Windows/ba-p/362902

- Download https://www.microsoft.com/en-us/download/details.aspx?id=58091

# DPAPI

# DATA PROTECTION API

- A set of Win32 APIs that allow you to encrypt data with great easy.

- The user's password hash encrypts:
    - Old user password hash
    - Current key – refreshed every 90 days

- Used in:
    - IE saved passwords
    - Picture, fingerprint ect authentication
    - ConvertFrom-SecureString
    - Credential manager

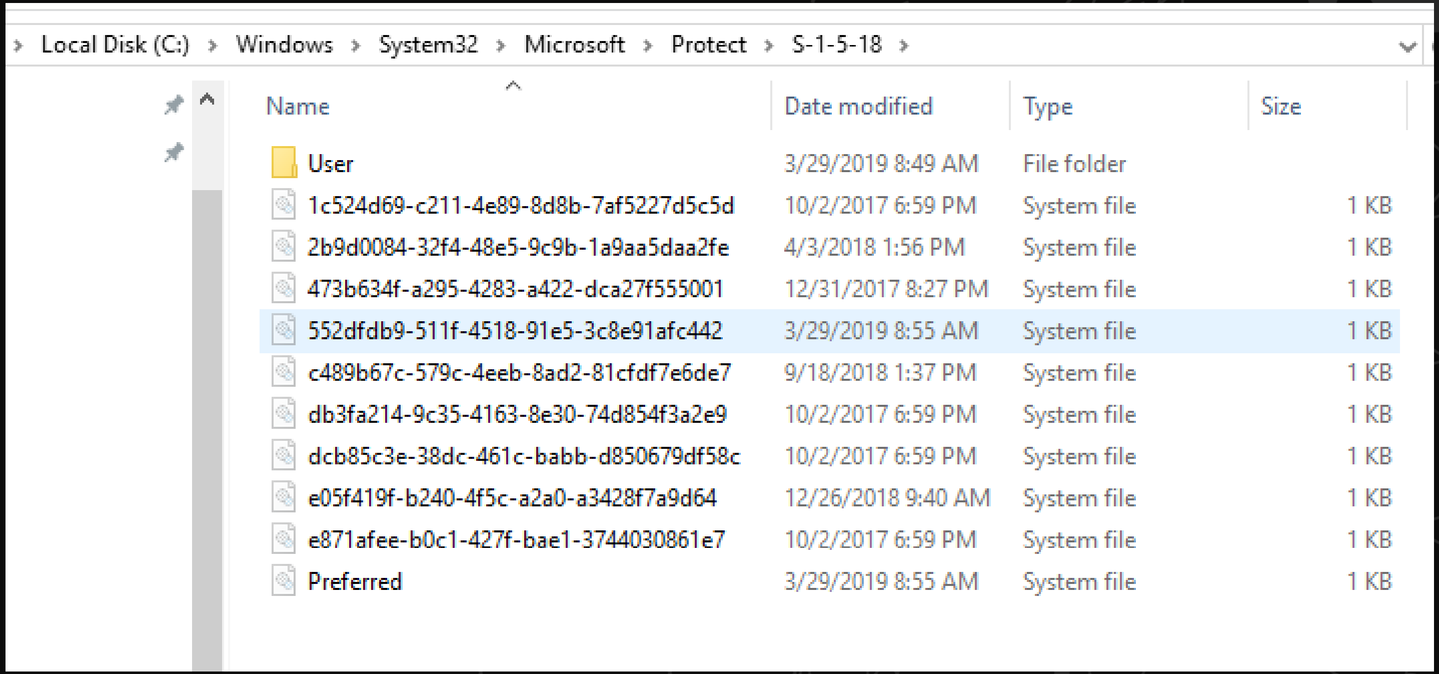
# DPAPI ENCRYPTION - SUBSYSTEM

- Local system

%WINDIR%/System32/Microsoft/Protect

- Current User – Semi Portable

%appdata%\Microsoft\Protect



Local Disk (C:) › Windows › System32 › Microsoft › Protect › S-1-5-18 ›

| Name | Date modified | Type | Size |
|---|---|---|---|
| User | 3/29/2019 8:49 AM | File folder | |
| 1c524d69-c211-4e89-8d8b-7af5227d5c5d | 10/2/2017 6:59 PM | System file | 1 KB |
| 2b9d0084-32f4-48e5-9c9b-1a9aa5daa2fe | 4/3/2018 1:56 PM | System file | 1 KB |
| 473b634f-a295-4283-a422-dca27f555001 | 12/31/2017 8:27 PM | System file | 1 KB |
| 552dfdb9-511f-4518-91e5-3c8e91afc442 | 3/29/2019 8:55 AM | System file | 1 KB |
| c489b67c-579c-4eeb-8ad2-81cfdf7e6de7 | 9/18/2018 1:37 PM | System file | 1 KB |
| db3fa214-9c35-4163-8e30-74d854f3a2e9 | 10/2/2017 6:59 PM | System file | 1 KB |
| dcb85c3e-38dc-461c-babb-d850679df58c | 10/2/2017 6:59 PM | System file | 1 KB |
| e05f419f-b240-4f5c-a2a0-a3428f7a9d64 | 12/26/2018 9:40 AM | System file | 1 KB |
| e871afee-b0c1-427f-bae1-3744030861e7 | 10/2/2017 6:59 PM | System file | 1 KB |
| Preferred | 3/29/2019 8:55 AM | System file | 1 KB |

# DPAPI ENCRYPTION – CREDENTIAL MANAGER

- Is the Credential Manager a good place for Passwords:
  - It depends
  - The API for Credential manager is standard and easy to use and an obvious spot for hackers
  - Most implementation skip adding entropy

https://github.com/davotronic5000/PowerShell_Credential_Manager

# OTHER CRAZY TOPICS

- What part of windows surprised you when you learned how it worked?
- Any suggestions for future topics?

MMS

# Extended Q&A

| | |
|---|---|
| Stephen Owen | @FoxDeploy |
| Shaun Cassels | @Cassells |
| Jeff Scripter | @JeffTheScripter |

2Pint Software

adaptiva

vmware®

1E

DELL

Microsoft

Kollective

Parallels®

Patch My PC
PATCH MANAGEMENT MADE EASY

Recast Software

LogicDS
SwImage

Lenovo.

ivanti

# RESOURCES / LINKS

| | |
|---|---|
| Comprehensive guide to WMI – LogicMonitor | http://bit.ly/wmiguide |
| There’s something about WMI – SANS DFIR | http://bit.ly/wmi4evil |
| PowerShell History – Snover | http://bit.ly/poshhistory |

# TELEMETRY RESOURCES

- Windows Analytics - http://aka.ms/WAGetStarted
- Diagnostic Data Viewer - https://bit.ly/2Y6CV13
- Windows Insider Flight Hub - https://docs.microsoft.com/en-us/windows-insider/flight-hub/
- Windows ADK - https://aka.ms/adk
- Windows Performance Toolkit - https://docs.microsoft.com/en-us/windows-hardware/test/wpt/
- Windows Performance Analyzer - https://bit.ly/2vANA7Q
- DTrace For Windows - https://www.microsoft.com/en-us/download/details.aspx?id=58091

MMS

RADISSON BLU · MALL OF AMERICA

MMS