Microsoft Office Telemetry Log (TBL) Format

Summary

Document Information

Author(s):	Sam Koffman sam@madscientistassociation.org
Abstract:	This document contains information about the forensic analysis of the records generated by the Microsoft Office telemetry feature.
Classification:	Public
Keywords:	Microsoft Office, Telemetry, TBL

License

Revision History

Version	Author	Date	Comments
0.1	Sam Koffman	October 2018	Initial Version

1. Overview

The Microsoft Office telemetry agent was first introduced in 2013 with the release of Office 2013. It is used to collect data from various Microsoft Office applications, including Access, Excel, OneNote, Outlook, PowerPoint, Project, Publisher, Visio, and Word. Information collected will depend on the version of Office and the telemetry agent installed, as detailed in section 1.2. Typical data collection will include user name, computer name, filename, document title and author, and last loaded date[1].

Telemetry agent data is initially stored locally the %UserProfile%\AppData\Local\Microsoft\Office\16.0\Telemetry\ folder. Depending on the deployment configuration, it may then be uploaded to a network share and processed into a SQL database.

1.1 Test Version

The following versions of programs were used to test the information in this document:

- Microsoft Windows 10 Professional v. 1803
- Microsoft Windows Server 2012 R2
- Microsoft SQL Server 2016 Standard Service Pack 2
- Microsoft Office Professional Plus 2016

1.2 Timestamps

TBL files store timestamps using the Windows NT (win32 epoch) time format, represented as the number of 100 nanosecond intervals since 01/01/1601 00:00:00 UTC[2]. The timestamps are stored as a 64-bit value.

1.3 Text Encoding

Unless other specified, all text contained in TBL files is encoded as UTF-16 little-endian.

2. File Structure

2.1 Header

TBL files start with a 16-byte signature, divided into two 8-byte segments. The first segment is common across TBL files, while the second defines the TBL as containing either user data (user.tbl), event data (evt.tbl), or solution data (sln.tbl). The header is the *only* section of the TBL file utilizing UTF-8 text encoding.

Offset	Size (b)	Value (hex)	Value (UTF-8)	Description
0	8	2000000053444454	...SDDT	Signature
8	8	0100000052455355	...RESU	user.tbl
8	8	01000000544E5645	...TNVE	evt.tbl
8	8	01000000564E4953	...VNIS	sln.tbl

2.2 user.tbl

The user.tbl file contains information about the user under which the telemetry agent is running, the network to which the machine is joined, and details on the hardware on the underlying machine.

Numeric values in the table below are stored as 16-bit little-endian unsigned integers unless otherwise noted.

Offset	Size (b)	Description
36	8	Timestamp
44	512	User account name (user principal name prefix[3]
558	512	Legacy domain name
1124	30	NetBIOS host name
1156	510	DNS domain name (without hostname)
1668	2	Telemetry agent minor version
1670	2	Telemetry agent major version
1672	2	Telemetry agent version revision
1674	2	Telemetry agent version build
1676	512	Path to network share where telemetry data is uploaded
2196	158	Hardware specifications for local computer
2356	4	Number of logical processors (32-bit unsigned int)
2360	4	Number of physical processors (32-bit unsigned int)
2364	4	CPU architecture (32-bit unsigned int)
2368	4	RAM in MB (32-bit unsigned int)
2372	4	Screen height (32-bit unsigned int)
2376	4	Screen width (32-bit unsigned int)
2380	2	Operating system minor version
2382	2	Operating system major version
2384	2	Operating system product type
2386	2	Operating system version build

Offset	Size (b)	Description
2388	2	Operating system default user interface language ID
2392	2	Operating system default language ID
2396	2	Internet Explorer minor version
2398	2	Internet Explorer major version
2400	2	Internet Explorer version revision
2402	2	Internet Explorer version build

2.3 evt.tbl

The evt.tbl maps each event logged by the telemetry agent to an event type, defined below. Beginning at offset 40, this file consists of 156-byte blocks, each representing a specific event.

2.3.1 Event Codes

Event codes are identified as follows[4]:

ID	Title	Severity	Description
1	Document loaded successfully	None	File opened without any issues
2	Document failed to load	Warning	Application unable to load file
3	Template loaded successfully	None	Template file opened without any issues
4	Template failed to load	Warning	Application unable to load template file
5	Add-in loaded successfully	None	Add-in loaded successfully within the application
6	Add-in failed to load	Critical	Application unable to load add-in
7	Add-in manifest downloaded successfully	None	Host application successfully loaded manifest file for add-in
8	Add-in manifest did not download	Critical	Application unable to load manifest file for add-in from SharePoint catalog, corporate catalog, or the Office Store
9	Add-in manifest could not be parsed	Critical	Application loaded add-in, but could not read the XML
10	Add-in used too much CPU	Critical	Add-in used more than 90% of CPU resources over a finite period of time
11	Application crashed on load	Critical	Application tried to load a document or solution on launch, but problems with the document or solution prevented application launch
12	Application closed due to a problem	Critical	Something caused a critical error in the application and it needed to close

ID	Title	Severity	Description
13	Document closed successfully	None	File closed without any issues
14	Application session extended	None	Application sessions for a document or solution should only last 24 hours, or the application creates a new session
15	Add-in disabled due to string search time-out	None	Outlook e-mail add-ins use regular expressions to search a message subject line and body to determine whether they should be displayed. Outlook disabled the add-in because it timed out repeatedly while trying to match a regular expression
16	Document open when application crashed	Critical	File was opened when application crashed
17	Add-in closed successfully	Informative	Application successfully shut down add-in
18	Application closed successfully	None	Host application successfully closed Office Add-in
19	Add-in encountered runtime error	Critical	Office Add-in had a problem that caused it to fail
20	Add-in failed to verify licensing	Critical	Licensing information for Office Add-in could not be verified

2.3.2 Block Structure

Numeric values in the table below are stored as 32-bit little-endian unsigned integers unless otherwise noted. Offsets are given from the start of the block.

Offset	Size (b)	Description
0	4	Block size
4	4	Entry number
24	8	Timestamp
36	4	Event code
40	16	Document GUID
136	8	Timestamp
144	8	Flags
152	4	Block footer

2.4 sln.tbl

The sln.tbl includes the filename, path, size, and author name, and other metadata for each event logged by the telemetry agent. Beginning at offset 32, this file consists of 2,964-byte blocks, each representing a specific event.

2.4.1 Block Structure

Numeric values in the table below are stored as 32-bit little-endian unsigned integers unless otherwise noted. Offsets are given from the start of the block.

Offset	Size (b)	Description

Offset	Size (b)	Description
0	4	Block size
4	16	Document GUID
24	8	Timestamp
40	8	Timestamp
48	512	Filename of the document or add-in
568	512	Absolute path of the document or add-in
1100	2	Telemetry agent minor revision (16-bit unsigned int)
1102	2	Telemetry agent major revision (16-bit unsigned int)
1106	2	Telemetry agent version build (16-bit unsigned int)
1108	4	Entry type (Application DLL: 0x09000000, Document: 0xFFFFFFFF)
1124	4	Size of document/add-in file (bytes)
1140	2	FileFormat number
1402	256	Document author name
1672	512	Add-in friendly name

3. Detection of Telemetry Agent

The telemetry agent can be enabled in several ways:

1. Using the Telemetry Log application included with Office
2. Keys can be added to the Windows registry
3. Group policy can be pushed to the machine

3.1 Registry Keys

Keys are written to two possible locations in the Windows registry:

1. `HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\OSM` (when enabled through Telemetry Log or manually edited)
2. `HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\OSM` (when enabled by group policy; overrides user settings)`

Value	Type	Description	Values
enablelogging	REG_DWORD	Enable telemetry	0: disable logging and agent (default); 1: enable logging and agent
enableupload	REG_DWORD	Upload telemetry data to shared folder	0: do not upload (default); 1: upload
commonfileshare	REG_SZ	Shared folder for storing telemetry data	UNC path
tagN	REG_SZ	Custom tags for telemetry data, which will show in Telemetry Dashboard	Custom data
enablefileobfuscation	REG_DWORD	Obfuscate file name, path, and title of Office document before uploading data to shared folder	0: do not obfuscate (default); 1: obfuscate
AgentInitWait	REG_DWORD	Time agent waits before scanning a client and uploading data to shared folder	Wait time in seconds; *defaults to 600 if value doesn't exist*

Value	Type	Description	Values
AgentRandomDelay	REG_DWORD	Agent waits between 0 and AgentRandomDelay minutes plus AgentInitWait value before scanning or uploading telemetry data	Wait time in minutes

Additional registry keys may be added to prevent specific applications or solution components from uploading telemetry data. These keys are written to:

`HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\OSM\preventedapplications`

Value	Type	Description	Values
accesssolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
olksolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
onenotesolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
pptsolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
projectsolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
publishersolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
visiosolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
wdsolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting
xlsolution	REG_DWORD	Prevent telemetry reporting for specific Office applications	0: allow reporting (default); 1: prevent reporting

`HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\OSM\preventedsolutiontypes`

Value	Type	Description	Values
agave	REG_DWORD	Prevent telemetry reporting for specific Office solutions. Note that solution types are still reported.	0: allow reporting (default); 1: prevent reporting
appaddins	REG_DWORD	Prevent telemetry reporting for specific Office solutions. Note that solution types are still reported.	0: allow reporting (default); 1: prevent reporting
comaddins	REG_DWORD	Prevent telemetry reporting for specific Office solutions. Note that solution types are still reported.	0: allow reporting (default); 1: prevent reporting
documentfiles	REG_DWORD	Prevent telemetry reporting for specific Office solutions. Note that solution types are still reported.	0: allow reporting (default); 1: prevent reporting
templatefiles	REG_DWORD	Prevent telemetry reporting for specific Office solutions. Note that solution types are still reported.	0: allow reporting (default); 1: prevent reporting

3.2 Group Policies

Office telemetry can also be managed using Windows Group Policy. The following policies may be present if telemetry is configured, and located at:

```
User Configuration\Policies\Administrative Templates\Microsoft Office 2016\Telemetry Dashboard
```

Setting Name	Description
Turn on telemetry data collection	Enable telemetry agent
Turn on data uploading for the Telemetry Agent	Enable the telemetry agent to periodically upload data to a shared folder
Specify the UNC path to store Office telemetry data	Location of shared folder where telemetry agent will upload data
Specify custom tags for Office telemetry data	Add custom tags to data uploaded by the telemetry agent
Turn on privacy settings in Telemetry Agent	Telemetry agent will obfuscate file name, file path, and title of documents when uploading telemetry data
Office applications to exclude from Telemetry Agent reporting	Prevent data from specific applications from being collected
Office solutions to exclude from Telemetry	Prevent data from specific Office solutions from being collected

4. References

[1] Brown, Daniel H. "Data That the Telemetry Agent Collects in Office." Microsoft.com. Dec. 16, 2016. [Online]. Available: https://docs.microsoft.com/en-us/deployoffice/compat/data-that-the-telemetry-agent-collects-in-office. [Accessed Aug. 27, 2018].

[2] Abdulla, Shijaz. “How to convert date/time attributes in Active Directory to standard time format.” Microsoft.com. Jul. 6, 2018. [Online] Available: https://support.microsoft.com/en-us/help/555936. [Accessed Sep. 20, 2018].

[3] Microsoft, “User Naming Attributes.” Microsoft, May 30 2018. [Online] Available: https://docs.microsoft.com/en-us/windows/desktop/ad/naming-properties. [Accessed September 10, 2018].

[4] Narva, Niveditha, and Linda Caputo. "Troubleshooting Office Files and Custom Solutions with the Telemetry Log." Microsoft.com. September 16, 2015. [Online] Available: https://docs.microsoft.com/en-us/office/client-developer/shared/troubleshooting-office-files-and-custom-solutions-with-the-telemetry-log. [Accessed September 13, 2018].

[5] Brown, Daniel H. "Deploy Telemetry Dashboard." Microsoft.com. November 29, 2017. [Online] Available: https://docs.microsoft.com/en-us/deployoffice/compat/deploy-telemetry-dashboard#agentregistry. [Accessed August 27, 2018].