

Press any key to start

# Microsoft Office Telemetry




Tracking Your Every Move



Sam Koffman  
U.S. Dept. of the Treasury / SIGTARP

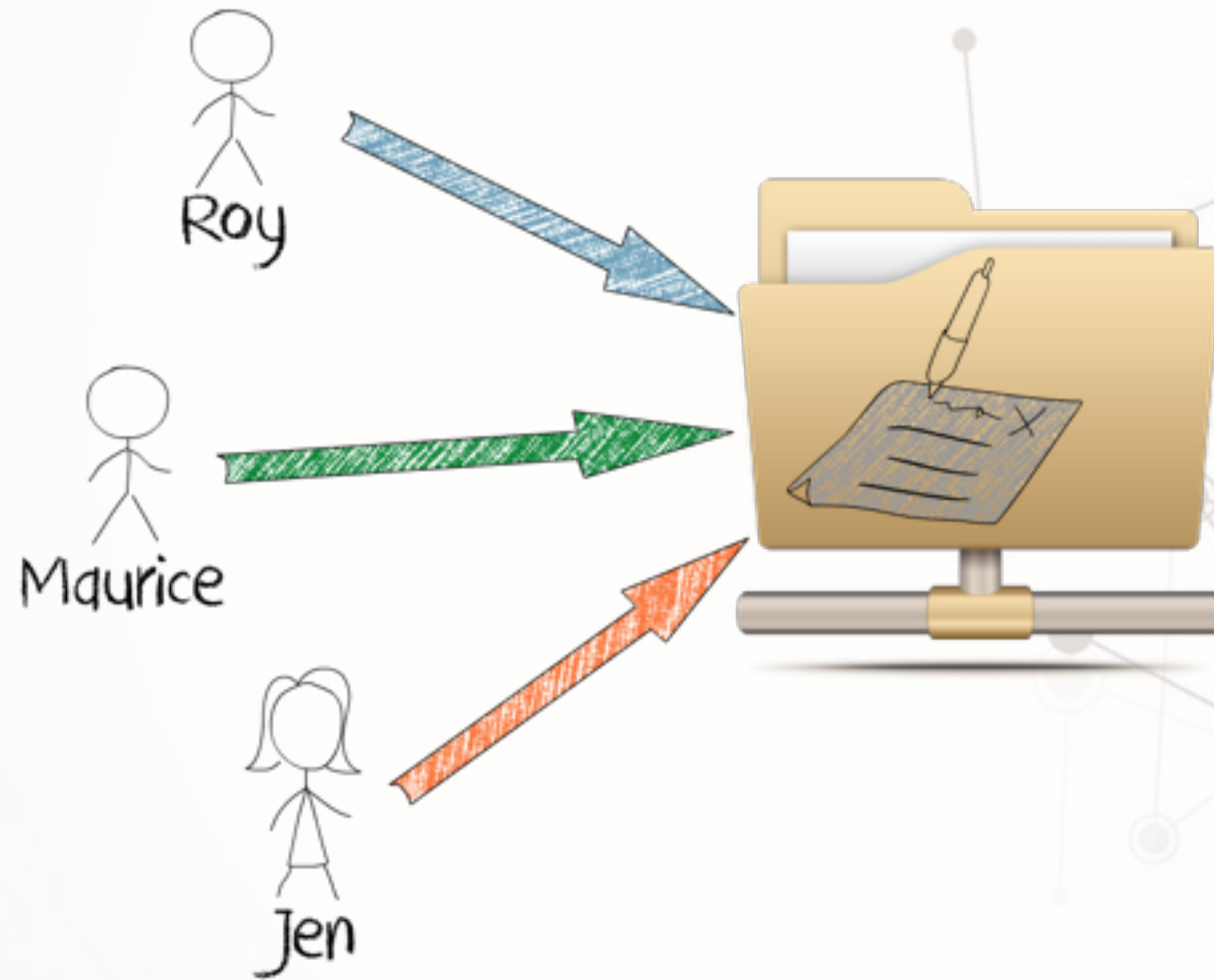
#include lawyers.h

Any reference in this presentation to any person, organization, activities, products, or services do not constitute or imply the endorsement, recommendation, or favoring of the U.S. Government, its subcomponents, or any of its employees or contractors acting on its behalf.



Blah blah blah blah blah  
Blah blah blah blah blah  
Blah blah blah blah blah  
Blah blah blah blah blah

# Scenario



**Which user modified this document at specific date/time?**

- ✓ File system metadata
- ✓ Document metadata / versioning
- ✓ Network traffic

# Scenario

```
43006F00 6E005F00 41006700 65006E00 64006100 2E006400 6F006300 6D000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
61006D00 5C004400 65007300 6B007400 6F007000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 905E0000 09000000 10000000 00000000 02000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000
```

O S D F C o n \_ A g e n d a . d o c m

s e r s \ S a m \ D e s k t o p

S a m

..... ^



# Down the Rabbit Hole



## Compatibility Monitoring Framework

Identify

Test  
compatibility

Check  
performance

# Office Versions



Standard  
Pro Plus  
365 Pro Plus

Included

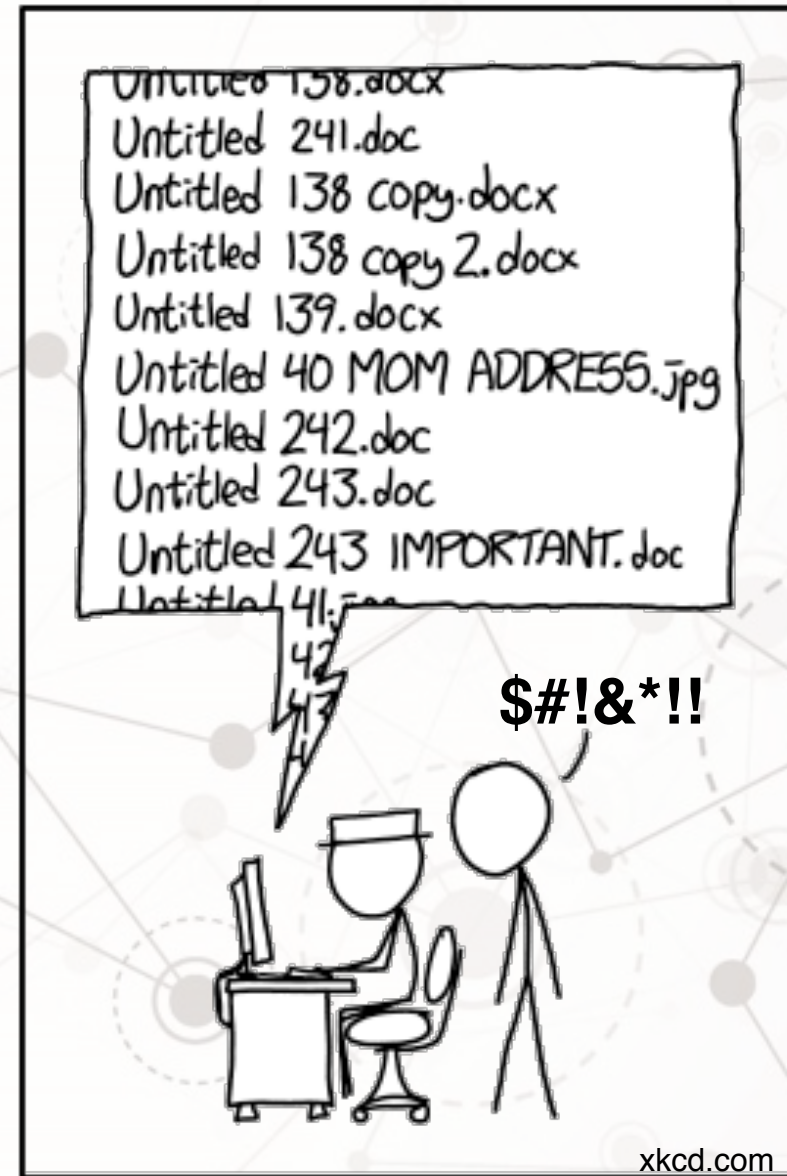


Telemetry Agent Compatible



??????  
?

What does this  
have to do with  
OSDFCon?



\$#!&\*!!

PROTIP: NEVER LOOK IN SOMEONE  
ELSE'S DOCUMENTS FOLDER.



# Data Collected

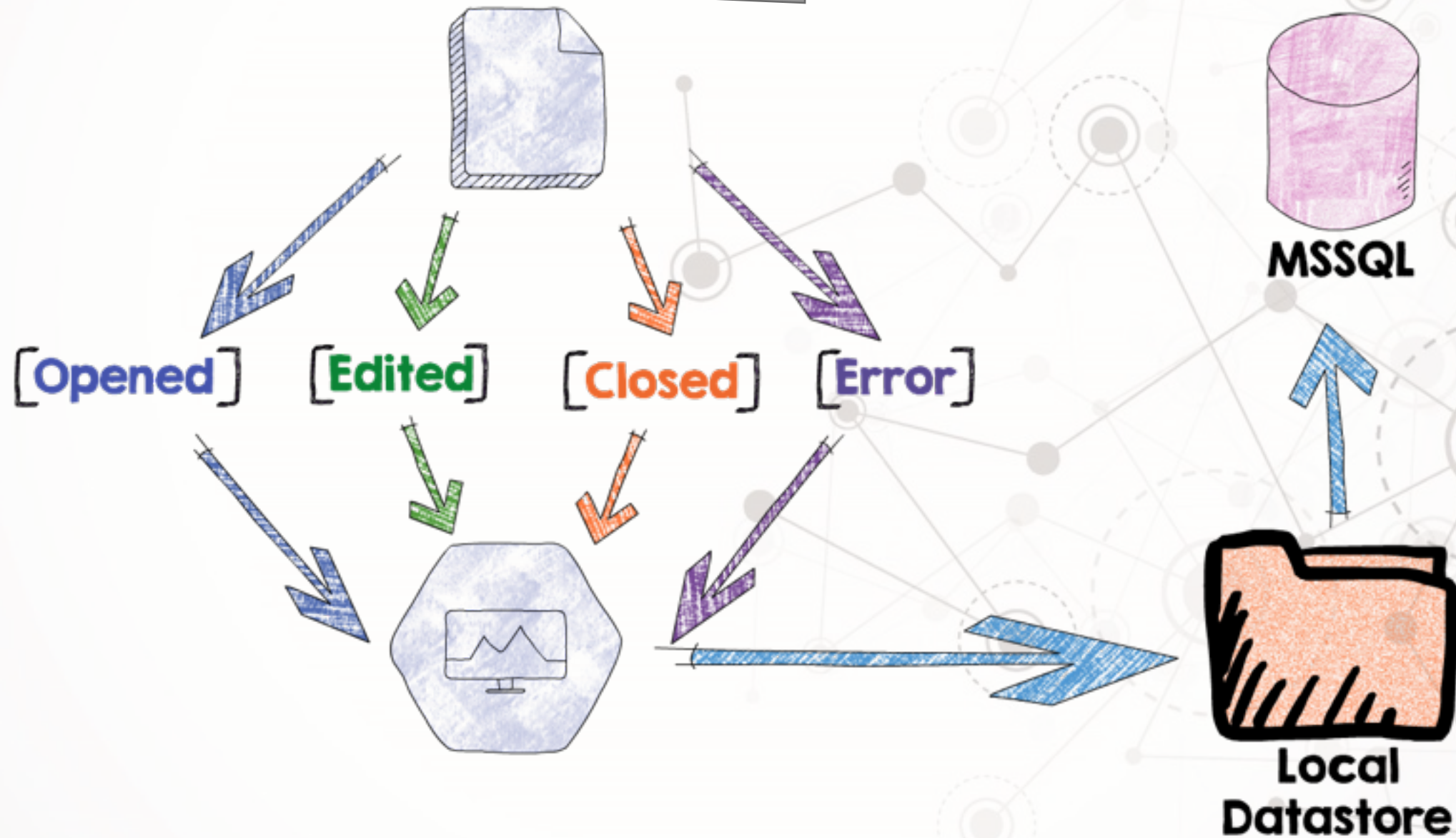
## Document

File name	File format	Event Timestamp	Path	Size	Author	Title
-----------	-------------	--------------------	------	------	--------	-------

## Computer

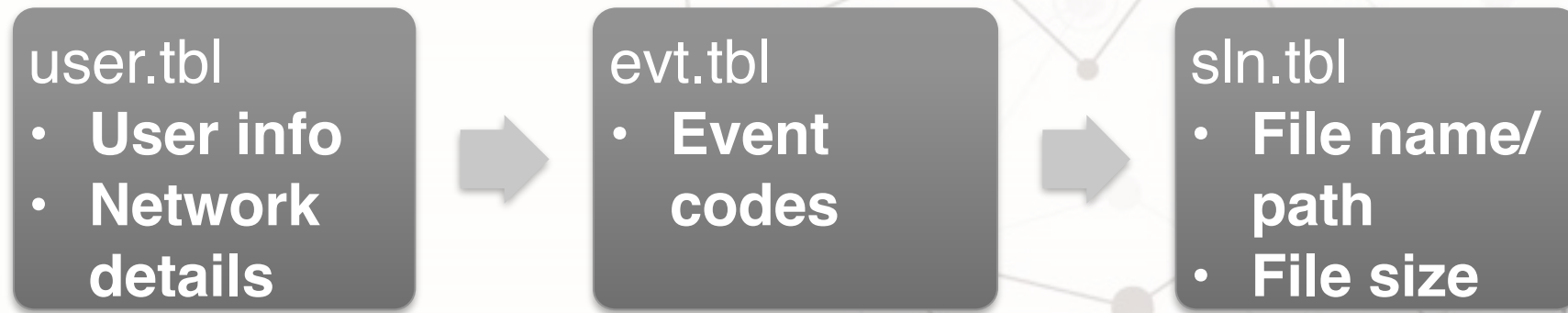
User name	Computer name	Domain	RAM	CPU
-----------	---------------	--------	-----	-----

# Telemetry Process



# Local Datastore

%UserProfile%\AppData\Local\Microsoft\Office\16.0\Telemetry\



## Caveats:

Recently used files  
5MB file size

# Wait, there's code!



MadScientistAssociation / libmsot

Unwatch 2

★ Star 1

Fork

<> Code

Issues 0

Pull requests 0

Projects 0

Wiki

Insights

Settings

Parser for MS Office telemetry files.

Edit

Manage topics

18 commits

1 branch

0 releases

1 contributor

View license

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download



skusa108 Merge pull request #2 from MadScientistAssociation/evt\_parse\_v2

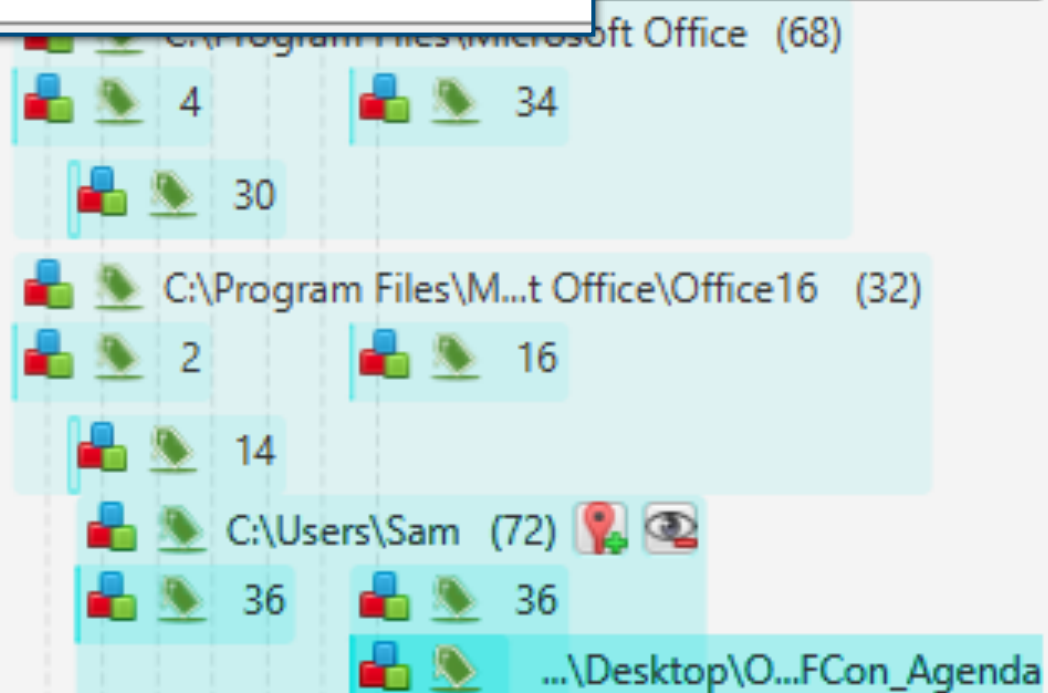
Latest commit ce8b7f9 10 days ago

.gitignore	Added new field to evt_tbl_parse	10 days ago
LICENSE.txt	Initial code commit.	6 months ago
MSOTParser.py	Added new field to evt_tbl_parse	10 days ago
README.md	Initial code commit.	6 months ago
evt_tbl_parse.py	Added new field to evt_tbl_parse	10 days ago
misc_functions.py	Fixed issue with 0 values in timestamps.	4 months ago
sln_tbl_parse.py	Moved common helper functions to misc_functions.py	4 months ago
user_tbl_parse.py	Added user.tbl info into output file.	13 days ago

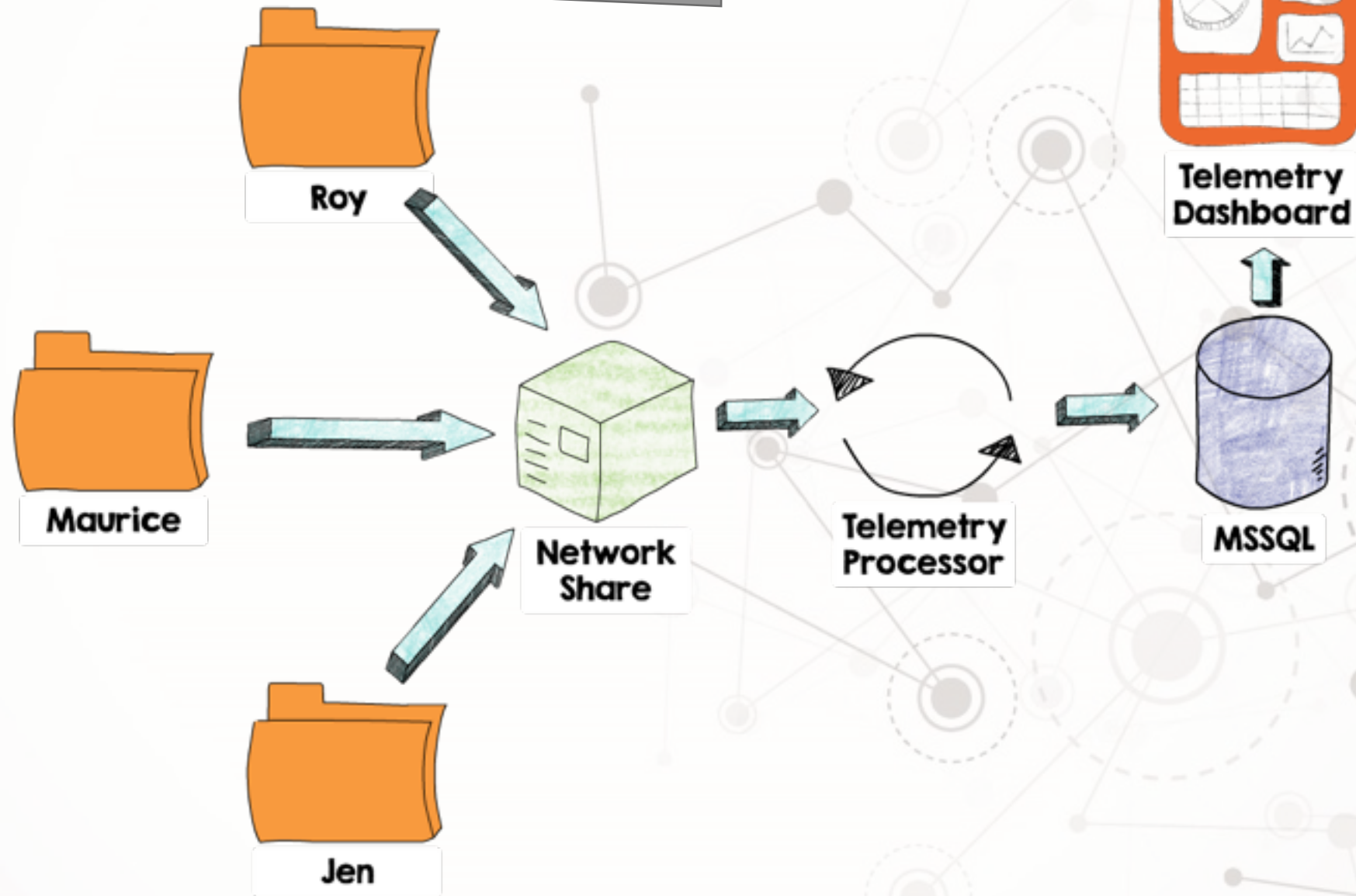


# Push button for evidence

Type	Value
Path	C:\Users\Sam\Desktop\OSDFCon_Agenda.docm
Date/Time	2018-10-11 13:28:39
Comment	Document loaded successfully
Username	sam
Source File Path	/img_MSOT Tester.vhd/vol_vol3/Users/Sam/Desktop/sln.zip/evt.tbl
Artifact ID	-9223372036854775030



# SQL Database

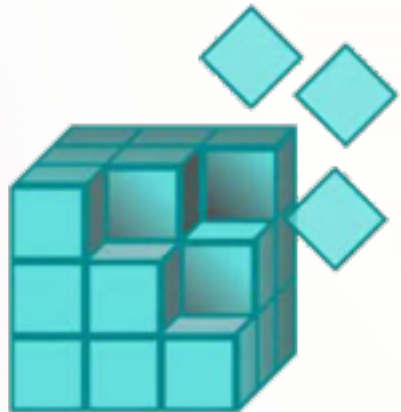


# Registry / GPO

HKEY\_CURRENT\_USER\Software\Microsoft\Office\16.0\OSM

HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Office\16.0\OSM

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



Upload to share

Custom tags

Wait / Random  
delay

Obfuscation

# So What?

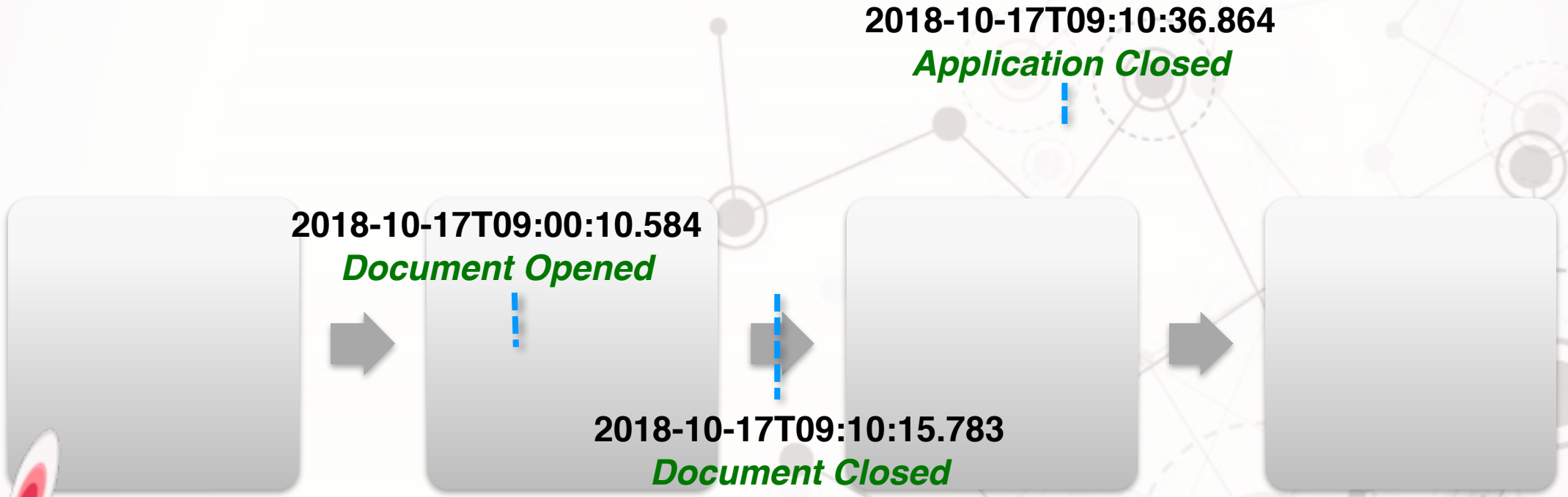
I DON'T KNOW OR CARE WHAT  
DATA *ANYONE* HAS ABOUT ME.

DATA IS IMAGINARY.  
THIS BURRITO IS REAL.





# Timelines



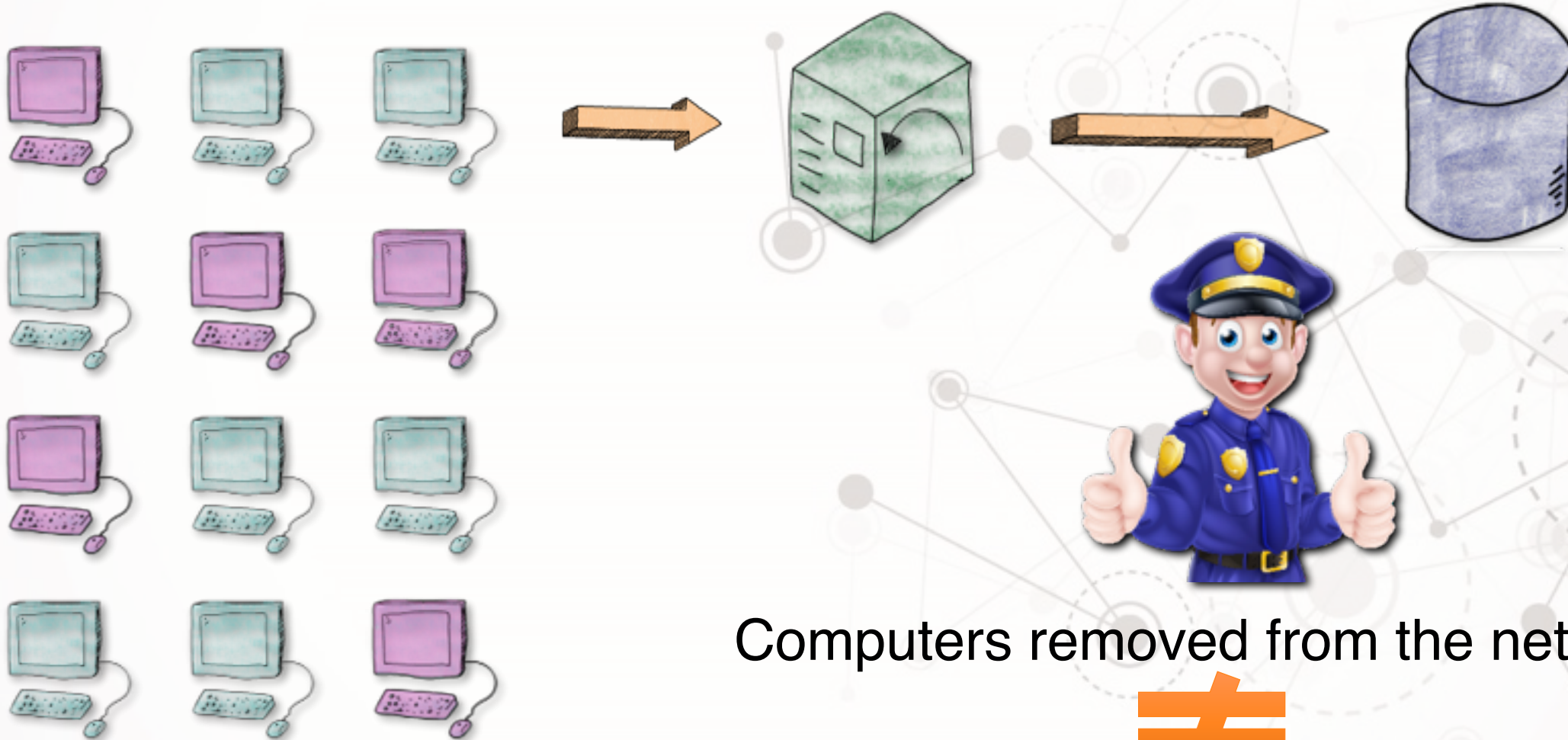
2018-10-17T09:00:00.000  
*Application Opened*

2018-10-17T09:00:10.584  
*Document Opened*

2018-10-17T09:10:15.783  
*Document Closed*

2018-10-17T09:10:36.864  
*Application Closed*

# Enterprise



Computers removed from the network



Entries removed from telemetry DB!

# Cloud-Hosted SQL



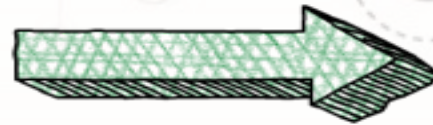
Azure



amazon  
web services



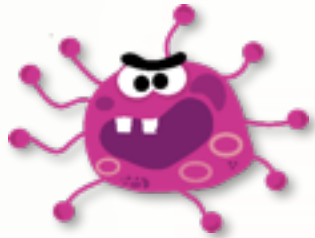
Google  
Cloud Platform



Malicious Code !Detected\_



Attack Vectors



Malicious macros



Custom Javascript  
functions



Dynamic Data Exchange calls



# To Do

- ☐ Test Office attacks
- ☐ Parse more stuff
- ☐ Office 365?
- ☐ Improve Autopsy module

END

Questions? Answers?

**madscientistassociation.org**

**sam@madscientistassociation.org**

Contribution to this project is encouraged!

JOKE'S ON THEM, GATHERING  
ALL THIS DATA ON ME  
AS IF ANYTHING I DO  
MEANS ANYTHING.



xkcd.com