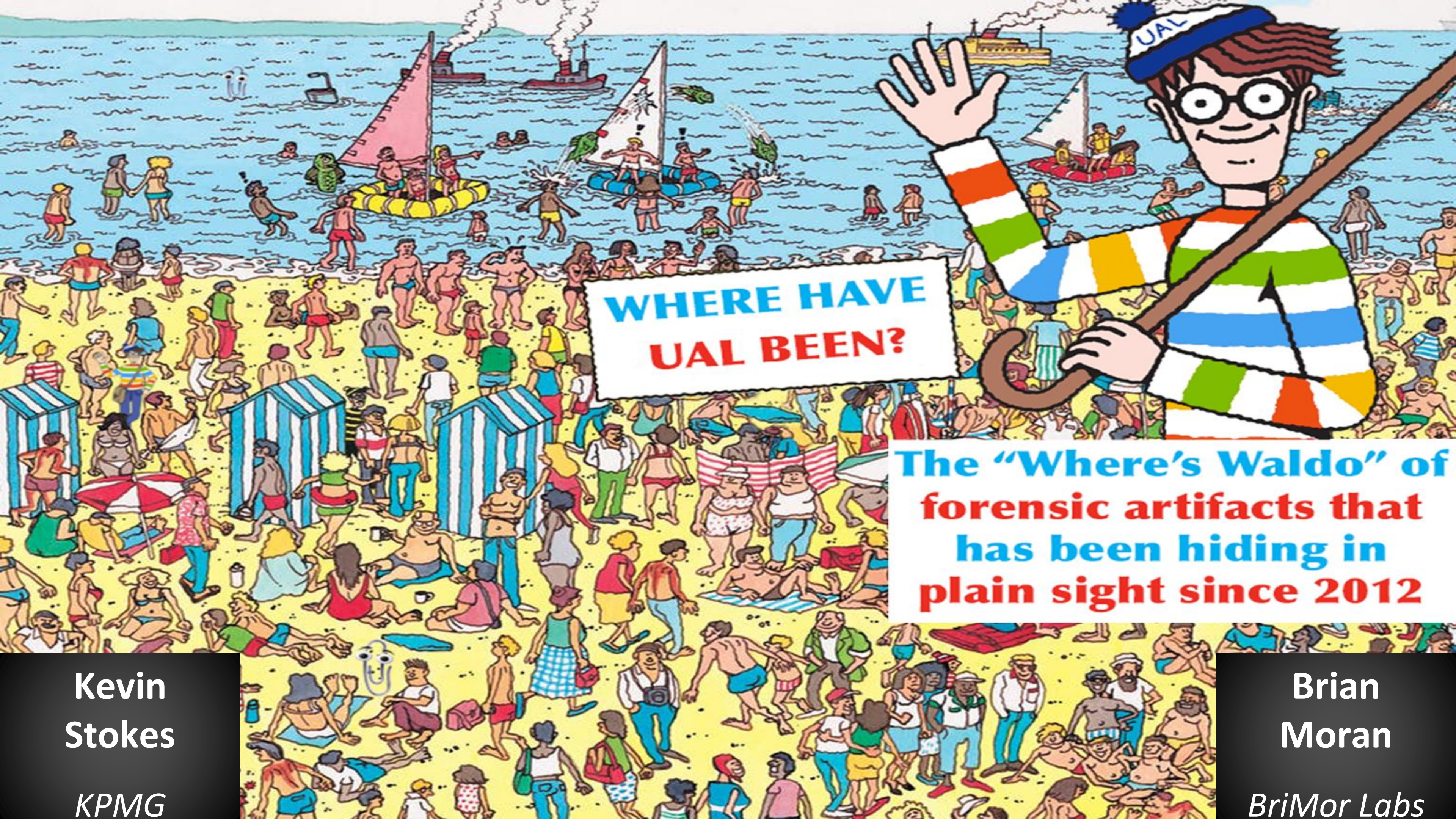


WHERE HAVE UAL BEEN?

The “Where’s Waldo” of forensic artifacts that has been hiding in plain sight since 2012

Kevin Stokes
KPMG

Brian Moran
BriMor Labs

KStokes@KPMG:~$ whoami

Hi, my name is Kevin Stokes

Cyber Response Services @ KPMG

8+ years of DFIR experience

Random fact about me:

Played trombone in a community band years ago

BMoran@BML:~$ whoami

Hello, my name is Brian Moran

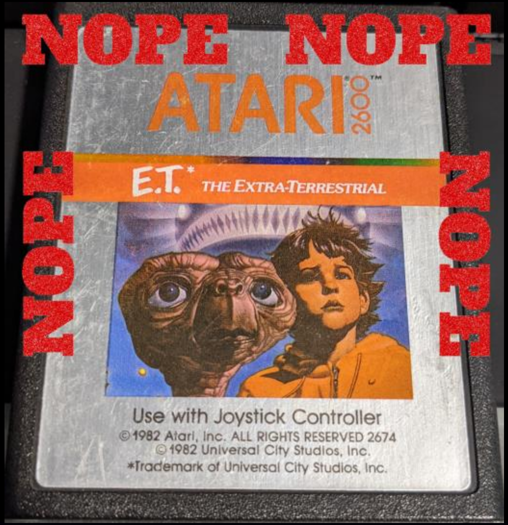
13+ years Air Force career

- Almost 20 years (gasp!) mobile exploitation/DFIR focus

Started BriMor Labs back in 2014

Random fact about me: Proud owner of an Atari 2600 E.T. cartridge

- Reminds me to never, ever make E.T.


NOPE NOPE
NOPE
NOPE
ATARI 2600™
E.T.* THE EXTRA-TERRESTRIAL
Use with Joystick Controller
©1982 Atari, Inc. ALL RIGHTS RESERVED 2674
©1982 Universal City Studios, Inc.
*Trademark of Universal City Studios, Inc.

2012

Some Things That Happened in 2012

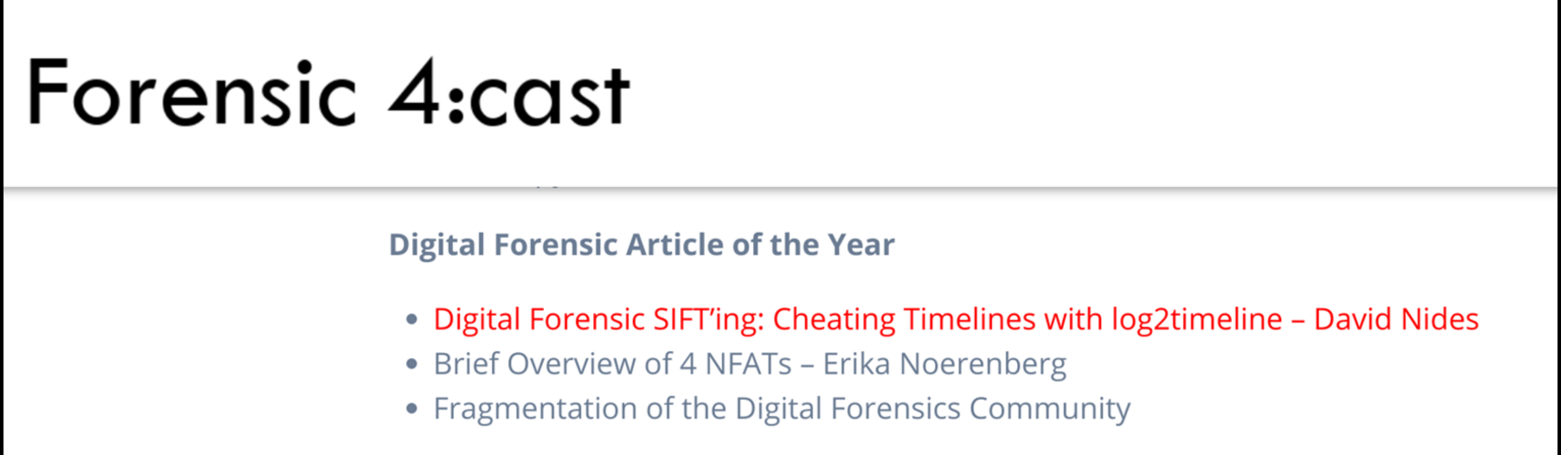
Marvel released *"The Avengers"*

Some Things That Happened in 2012

Felix Baumgartner jumped from 128,000 feet AND broke the sound barrier without any machine assistance

Some Things That Happened in 2012

David Nides (KPMG) won Forensic 4:Cast award
“Digital Forensics Article of the Year” for
“Digital Forensics SIFT’ing: Cheating Timelines with log2timeline”



Forensic 4:cast

Digital Forensic Article of the Year

- Digital Forensic SIFT’ing: Cheating Timelines with log2timeline – David Nides
- Brief Overview of 4 NFATs – Erika Noerenberg
- Fragmentation of the Digital Forensics Community

Some Things That Happened in 2012

Microsoft released a new version of Server OS

Some Things That Happened in 2012

Brent Forman guest wrote, on Ed Wilson's blog, about the new User Access Logging in Windows Server 2012:

https://devblogs.microsoft.com/scripting/powershell-and-user-access-logging

Those Things Happened in 2012

Quote of the Day

“This service is intended for administrators only”
Brent Forman - 09/17/2012

Presentation Objectives

Share our own research/information about User Access Logging (UAL)

Discuss additional research shared by others in community

Demonstrate how to:

- Access UAL data
- Parse UAL data

Provide additional resources

What is This Thing?

User Access Logging (UAL)

- A.K.A., “No no, the OTHER UAL logs”

Aggregates client usage by role and products

Allows admins additional resource usage visibility

Used for licensing management

First implemented in Windows Server 2012

Windows Servers Only

- 2012/2016/2019
- Appears in Windows Server 2022 Preview, as well!

Why Should You Care?

Logs Client Access Requests

- Can glean additional information to “what” happened
- May be helpful to see additional access if the event logs have rolled over

Including (historical) System Names, User Names, and IP Addresses

- Do you need to know what system had IP ###.###.##.## 18 months ago? Now, you can!

2+ years of data is a LONG time (lets face it, you probably won’t discover an incident within the first 24 hours)

UAL Basics

Where can I find these server logs?

%SYSTEMROOT%\Windows\System32\LogFiles\Sum

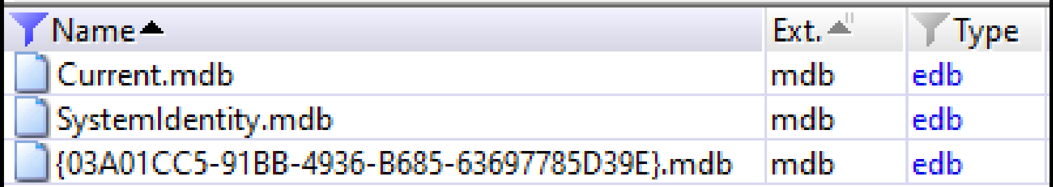
(NOTE: 'Sum' is likely an acronym for "Software Usage Metrics")

What are some files of interest in the Sum folder?

Current.mdb

SystemIdentity.mdb

{GUID}.mdb



Name	Ext.	Type
Current.mdb	mdb	edb
SystemIdentity.mdb	mdb	edb
{03A01CC5-91BB-4936-B685-63697785D39E}.mdb	mdb	edb

Do I need Microsoft Access Database software for these?

Nope! They are actually ESE (Extensible Storage Engine) databases

Stay tuned for more on this!

UAL File Overview

What are the Current.mdb and {GUID}.mdb files?

These files contain the same data, though the Current database (by default) records the current year, including the last 24 hours

{GUID} database files are aggregated backups of the Current.mdb file, up to two years (usually beginning January 1)

- Thus, potential for up to 3 years of data, per server, among all these files
  - If present, check Volume Shadow Copies for these, as well

Depending on server role, there may be extra data on some servers. For example, a DNS server may have an extra table for DNS data

UAL File Overview

Other files in this Sum folder

SystemIdentity.mdb

- Maintains a list of GUID archive files (CHAINED_DATABASES)
- Role_IDS table has GUIDs for server roles that are tracked by UAL
- SYSTEM_IDENTITY table shows details about the system

ESE essential files:

- Several other files exist here that are used by ESE
- Transaction Log Files, Temp DBs, Checkpoint Files
- For more info check this this link:

https://docs.microsoft.com/en-us/windows/win32/extensible-storage-engine/extensible-storage-engine-files

UAL Database Tables

Database	Tables	Description
Current.mdb {GUID}.mdb	CLIENTS	First and Last Access time and date for a user Access count and day of the year of access Including assigned IP address in the timeframe
	DNS*	Last date and time a host utilized DNS from the server Includes IP address of host at the time of last access. * Present if DNS role is applied to server
	ROLE_ACCESS	First and last date and time particular roles were accessed
	VIRTUALMACHINES	Information about Hyper-V VMs logged by UAL * We have not seen this populated yet
SystemIdentity.mdb	CHAIN_DATABASES	Keeps track of the {GUID} database utilized by UAL, shows the year of associated data
	ROLE_IDS	Main list of RoleGuids and associated product name and role name
	SYSTEM_IDENTITY	Information about the server resources and OS

UAL Database Table Columns

Column Name	Database (.mdb)	Table	Description
FirstSeen	Current | {GUID}	ROLE_ACCESS	Earliest date and time the role is seen
HostName	Current | {GUID}	DNS	Host name of the client
LastSeen	Current | {GUID}	DNS | ROLE_ACCESS	Last date and time seen for the role or DNS client record
ProductName	SystemIdentity	ROLE_IDS	Name of the software parent product, or product line, that is providing UAL data.
RoleGuid	Current | {GUID}	CLIENTS | ROLE_ACCESS	UAL assigned, or registered, GUID representing the server role, or installed product
	SystemIdentity	ROLE_IDS	
RoleName	SystemIdentity	ROLE_IDS	Name of the role, component, or sub-product that is providing UAL data
TenantId	Current | {GUID}	CLIENTS	GUID for a tenant client of an installed role or product For ADDS this is the AD InvocationID attribute
TotalAccesses	Current | {GUID}	CLIENTS	Incremental count of device accesses for a particular client device
InsertDate	Current | {GUID}	CLIENTS	First date and time seen for the client record
LastAccess	Current | {GUID}	CLIENTS	Last date and time seen for the client record
Address	Current | {GUID}	CLIENTS | DNS	IP address of a client device
AuthenticatedUserName	Current | {GUID}	CLIENTS	User name of the client that accompanies the UAL entry
ClientName	Current | {GUID}	CLIENTS	Does not appear to be utilized, currently
Day### Columns	Current | {GUID}	CLIENTS	Count of accesses for the day of the year
FileName	Current | {GUID}	CHAIN_DATABASES	Name of the {GUID} databases tracked by UAL
Year	Current | {GUID}	CHAIN_DATABASES	Year associated with the {GUID} databases tracked by UAL

UAL related PowerShell Commands

PowerShell	Description
Disable-Ual	Disables UAL at the next restart.
Enable-Ual	Enables UAL at the next restart
Get-Ual	Gets the startup status for UAL
Get-UalDailyAccess	Provides both client device and user access data for each day of the year.
Get-UalDailyDeviceAccess	Provides client device access data for each day of the year.
Get-UalDailyUserAccess	Provides client user access data for each day of the year.
Get-UalDeviceAccess	Provides client device access data for each role or product installed on the local or targeted server.
Get-UalDns	Provides DNS client specific data of the local or targeted DNS server.
Get-UalHyperV	Provides Hyper-V VM data relevant to the local or targeted server.
Get-UalOverview	Provides UAL related details and history of installed products and roles.
Get-UalServerDevice	Provides client device access data for the local or targeted server.
Get-UalServerUser	Provides client user access data for the local or targeted server.
Get-UalSystemId	Provides system specific data to uniquely identify the local or targeted server.
Get-UalUserAccess	Provides client user access data for each role or product installed on the local or targeted server.
Start-Service ualsvc	Starts the UAL service
Stop-Service ualsvc	Stops the UAL service

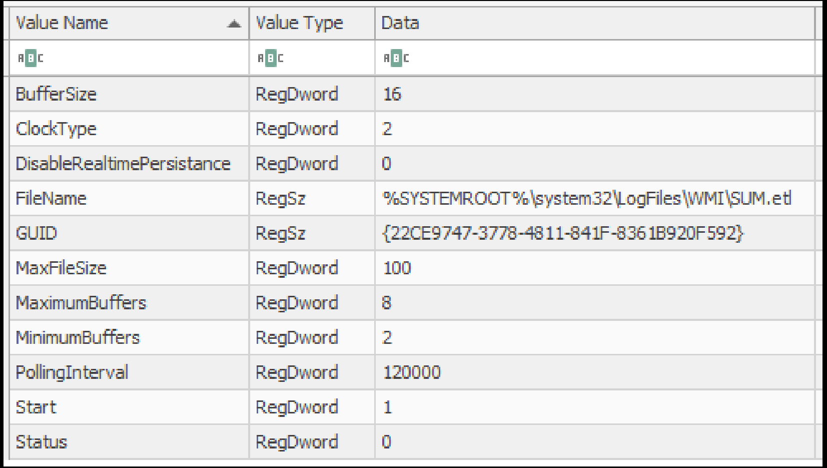
UAL in the Registry

SYSTEM\ControlSet*\Control\WMI\Autologger\SUM

PollingInterval can be adjusted
Default is 24 hours

```
REG ADD
HKLM\System\CurrentControlSet\Control
\WMI
\AutoLogger\Sum /v PollingInterval /t
REG_DWORD /d 120000 /F
```

Minimum is 60 seconds (60000), here it is set to 2 minutes.

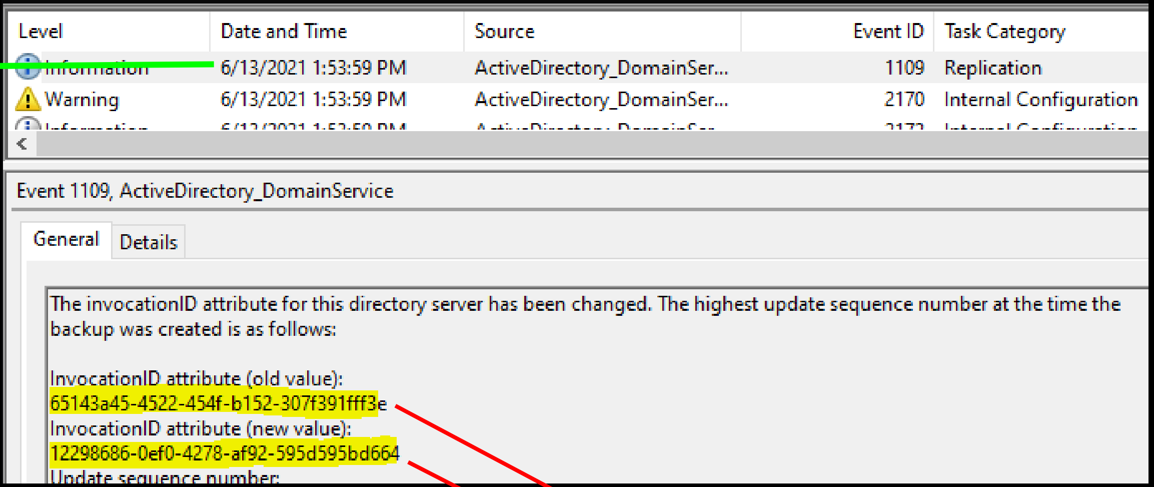


Value Name	Value Type	Data
BufferSize	RegDword	16
ClockType	RegDword	2
DisableRealtimePersistance	RegDword	0
FileName	RegSz	%SYSTEMROOT%\system32\LogFiles\WMI\SUM.etl
GUID	RegSz	{22CE9747-3778-4811-841F-8361B920F592}
MaxFileSize	RegDword	100
MaximumBuffers	RegDword	8
MinimumBuffers	RegDword	2
PollingInterval	RegDword	120000
Start	RegDword	1
Status	RegDword	0

TenantID Research

InvocationID attributes, for ADDS, relate to the version of the Active Directory database associated with the domain controller

The “Domain Service” event log will show the update of the InvocationID (EID 1109)

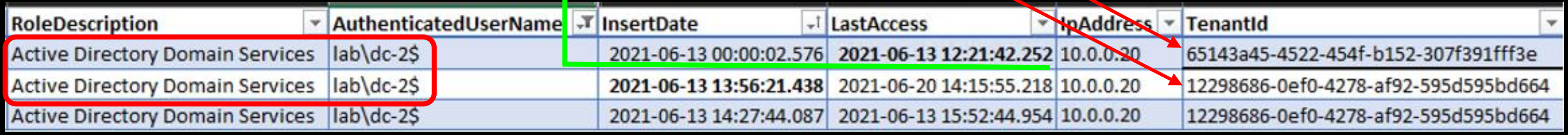


Level	Date and Time	Source	Event ID	Task Category
Information	6/13/2021 1:53:59 PM	ActiveDirectory_DomainSer...	1109	Replication
Warning	6/13/2021 1:53:59 PM	ActiveDirectory_DomainSer...	2170	Internal Configuration
Information	6/13/2021 1:53:59 PM	ActiveDirectory_DomainSer...	2172	Internal Configuration

Event 1109, ActiveDirectory_DomainService

The invocationID attribute for this directory server has been changed. The highest update sequence number at the time the backup was created is as follows:

InvocationID attribute (old value):
65143a45-4522-454f-b152-307f391fff3e
InvocationID attribute (new value):
12298686-0ef0-4278-af92-595d595bd664
Update sequence number:



RoleDescription	AuthenticatedUserName	InsertDate	LastAccess	IpAddress	TenantId
Active Directory Domain Services	lab\dc-2$	2021-06-13 00:00:02.576	2021-06-13 12:21:42.252	10.0.0.20	65143a45-4522-454f-b152-307f391fff3e
Active Directory Domain Services	lab\dc-2$	2021-06-13 13:56:21.438	2021-06-20 14:15:55.218	10.0.0.20	12298686-0ef0-4278-af92-595d595bd664
Active Directory Domain Services	lab\dc-2$	2021-06-13 14:27:44.087	2021-06-13 15:52:44.954	10.0.0.20	12298686-0ef0-4278-af92-595d595bd664

InvocationId attribute information: *https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-ada1/3ac24cae-9ec7-4ba7-9878-21fd42a0371b*

Previous Mentions of UAL

(Aforementioned) Brent Forman on Ed Wilson’s blog:
https://devblogs.microsoft.com/scripting/powershell-and-user-access-logging

Kevin Stokes: KPMG blog post:
https://advisory.kpmg.us/blog/2021/digital-forensics-incident-response.html

Zach Stanford (@svch0st):
https://svch0st.medium.com/windows-user-access-logs-ual-9580f1100635

Microsoft Japan blog (Kenichi Maruyama) :
https://jpwinsup.github.io/blog/2020/10/13/UserInterfaceAndApps/ServerManagement/garbled_file_on_sum_folder/

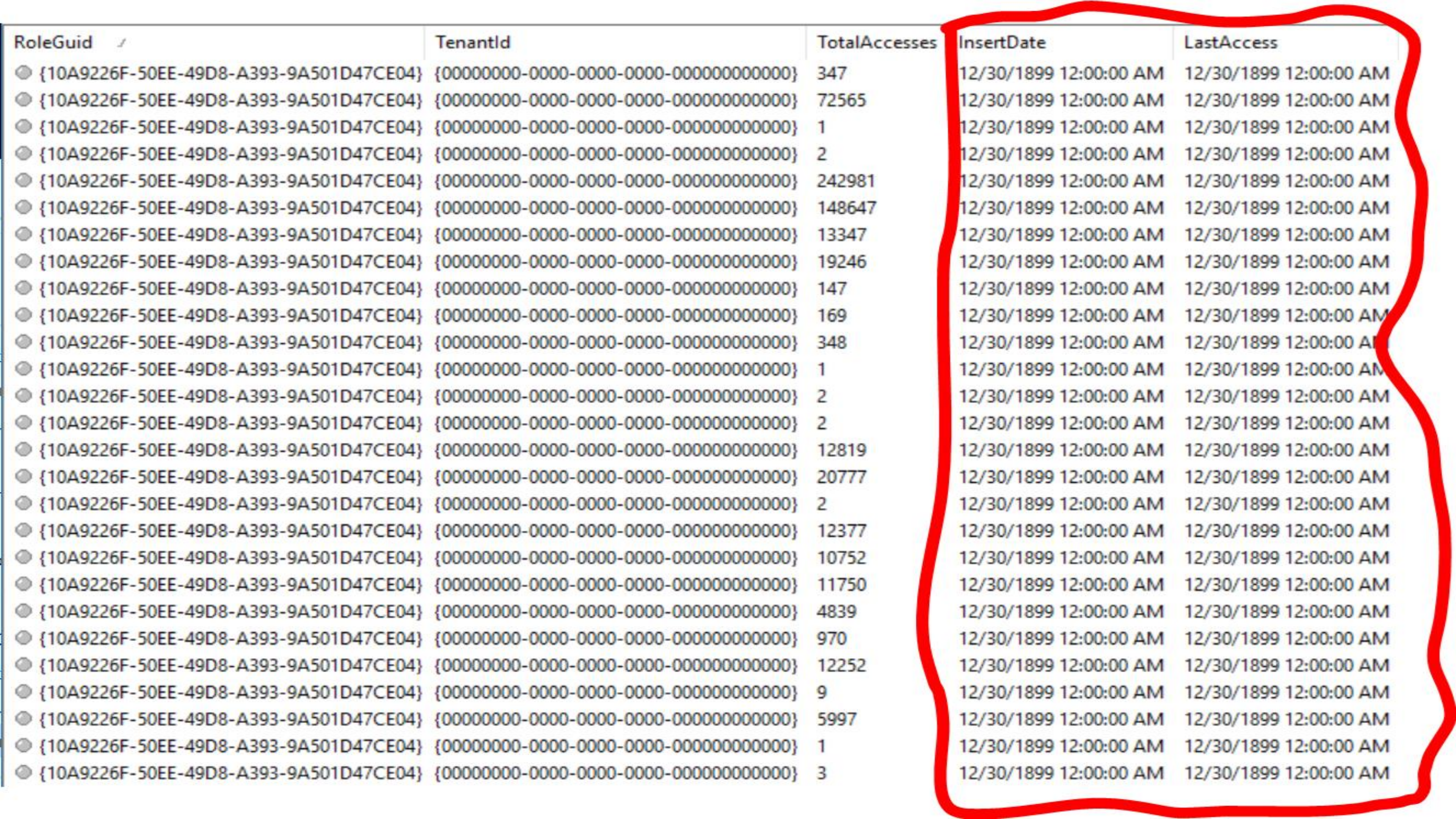
Patrick Bennett: Magnet Virtual Summit 2021:
https://www.magnetforensics.com/resources/mvs-recording-no-logs-no-problem-leveraging-user-access-logging-on-windows-server-systems/

CrowdStrike Blog Post (also Patrick Bennett):
https://www/crowdstrike.com/blog/user-access-logging-ual-overview/

UAL Data Parsing

Found that as we performed keyword searches across multiple systems, hits kept appearing in files with .mdb file extension

- Determined they were ESE databases -- tried to open with Nirsoft ESEDatabaseView
- Unfortunately, timestamp was obviously incorrect, and the GUIDs were not parsed properly (among other things)



RoleGuid	TenantId	TotalAccesses	InsertDate	LastAccess
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	347	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	72565	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	1	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	2	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	242981	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	148647	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	13347	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	19246	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	147	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	169	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	348	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	1	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	2	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	2	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	12819	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	20777	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	2	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	12377	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	10752	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	11750	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	4839	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	970	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	12252	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	9	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	5997	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	1	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM
{10A9226F-50EE-49D8-A393-9A501D47CE04}	{00000000-0000-0000-0000-000000000000}	3	12/30/1899 12:00:00 AM	12/30/1899 12:00:00 AM

UAL Data Parsing

Obviously, that is not right. At all

Highlighted the need to create SOMETHING that parsed everything correctly

UAL Data Parsing

We spent about two weeks trying to gain an understanding of the fields, data structures, etc, of the UAL files

Researched the formatting/structures of GUIDs/MAC addresses, etc

- Thank you Microsoft documentation!

Continued to make refinements of data output to make it more “human consumable”

UAL Data Parsing

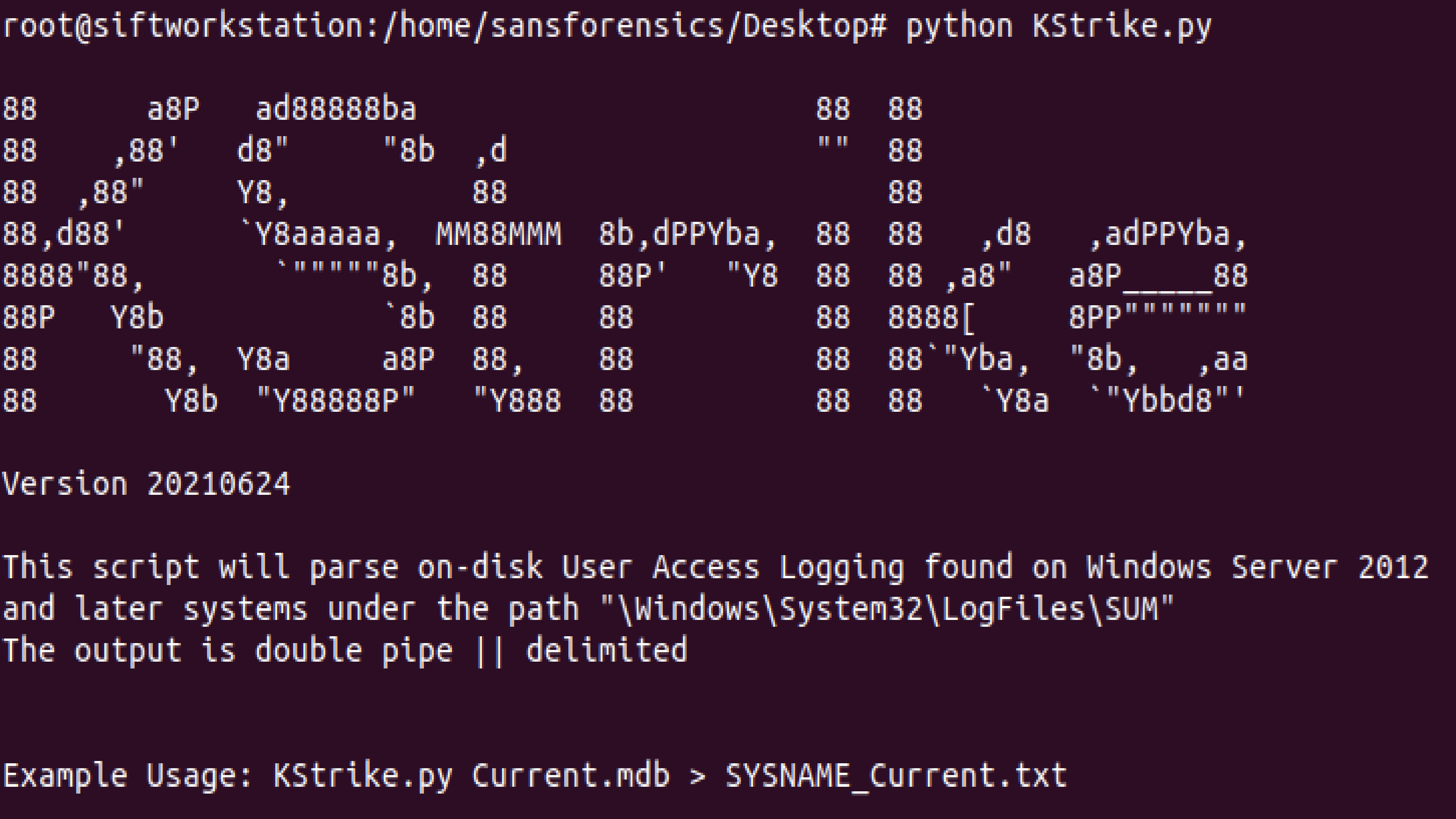
Enter KStrike

https://github.com/brimorlabs/KStrike

Development began January 30, 2021

Subsequent updates:

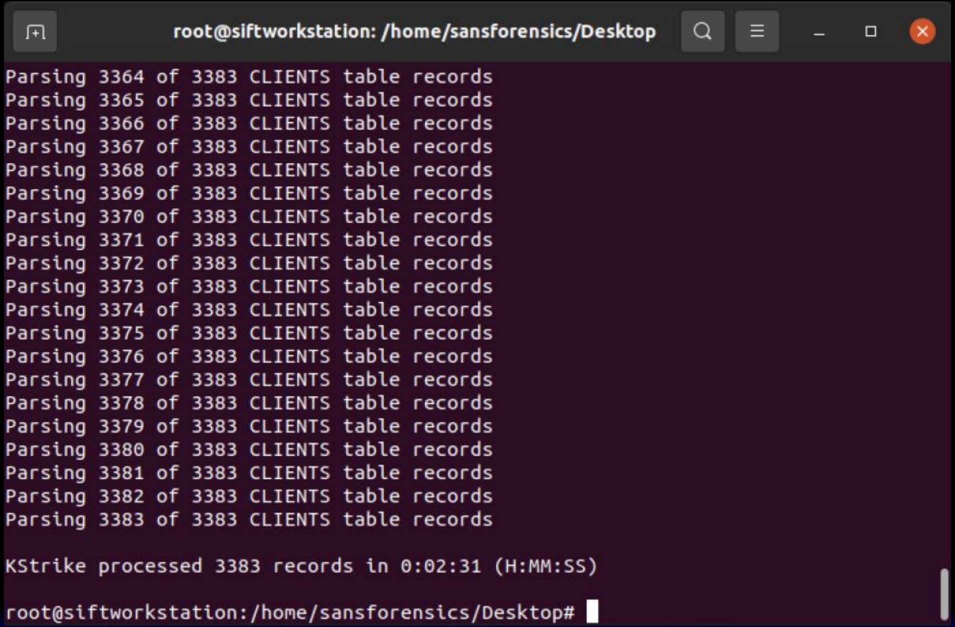
- Added hostname correlation from DNS table (if available)
- Included support (& best guessing) for multi-year entries -- yes, they can occur
- Additional GUID correlation (thanks Mark McKinnon!)
- … and, most recently, Python 3 support
  - runs automagically on Py2/Py3 -- and on SIFT workstation!!



```
root@siftworkstation:/home/sansforensics/Desktop# python KStrike.py

88      a8P   ad88888ba                      88  88
88    ,88'   d8"     "8b  ,d                 ""  88
88  ,88"     Y8,          88                     88
88,d88'      `Y8aaaaa,  MM88MMM  8b,dPPYba,  88  88   ,d8   ,adPPYba,
8888"88,       `"""""8b,  88     88P'   "Y8  88  88 ,a8"   a8P_____88
88P   Y8b            `8b  88     88          88  8888[     8PP"""""""
88     "88,  Y8a     a8P  88,    88          88  88`"Yba,  "8b,   ,aa
88       Y8b  "Y88888P"   "Y888  88          88  88   `Y8a  `"Ybbd8"'

Version 20210624

This script will parse on-disk User Access Logging found on Windows Server 2012
and later systems under the path "\Windows\System32\LogFiles\SUM"
The output is double pipe || delimited


Example Usage: KStrike.py Current.mdb > SYSNAME_Current.txt
```

KStrike Raw Output

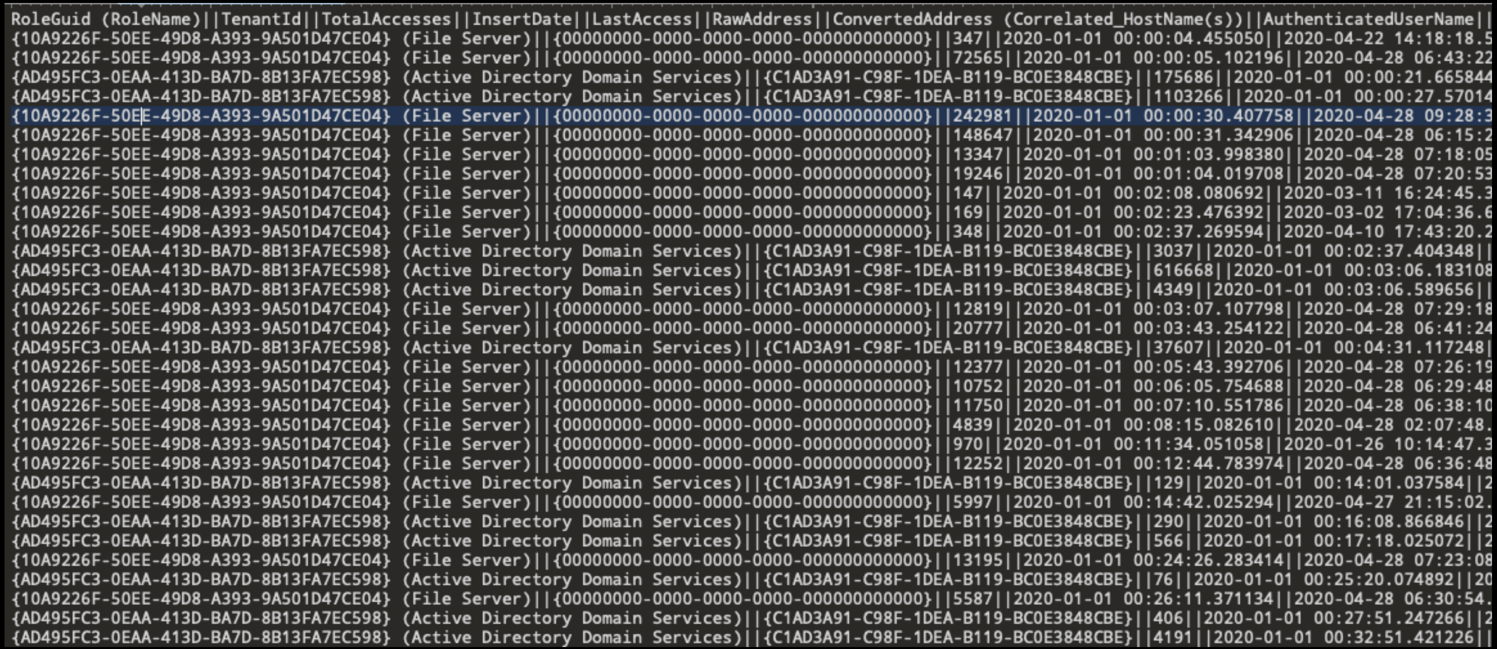
KStrike writes processing details/information to STDERR
KStrike writes formatted data to STDOUT (for redirection to a text file)



```
Parsing 3364 of 3383 CLIENTS table records
Parsing 3365 of 3383 CLIENTS table records
Parsing 3366 of 3383 CLIENTS table records
Parsing 3367 of 3383 CLIENTS table records
Parsing 3368 of 3383 CLIENTS table records
Parsing 3369 of 3383 CLIENTS table records
Parsing 3370 of 3383 CLIENTS table records
Parsing 3371 of 3383 CLIENTS table records
Parsing 3372 of 3383 CLIENTS table records
Parsing 3373 of 3383 CLIENTS table records
Parsing 3374 of 3383 CLIENTS table records
Parsing 3375 of 3383 CLIENTS table records
Parsing 3376 of 3383 CLIENTS table records
Parsing 3377 of 3383 CLIENTS table records
Parsing 3378 of 3383 CLIENTS table records
Parsing 3379 of 3383 CLIENTS table records
Parsing 3380 of 3383 CLIENTS table records
Parsing 3381 of 3383 CLIENTS table records
Parsing 3382 of 3383 CLIENTS table records
Parsing 3383 of 3383 CLIENTS table records

KStrike processed 3383 records in 0:02:31 (H:MM:SS)

root@siftworkstation:/home/sansforensics/Desktop# 
```

KStrike Raw Output

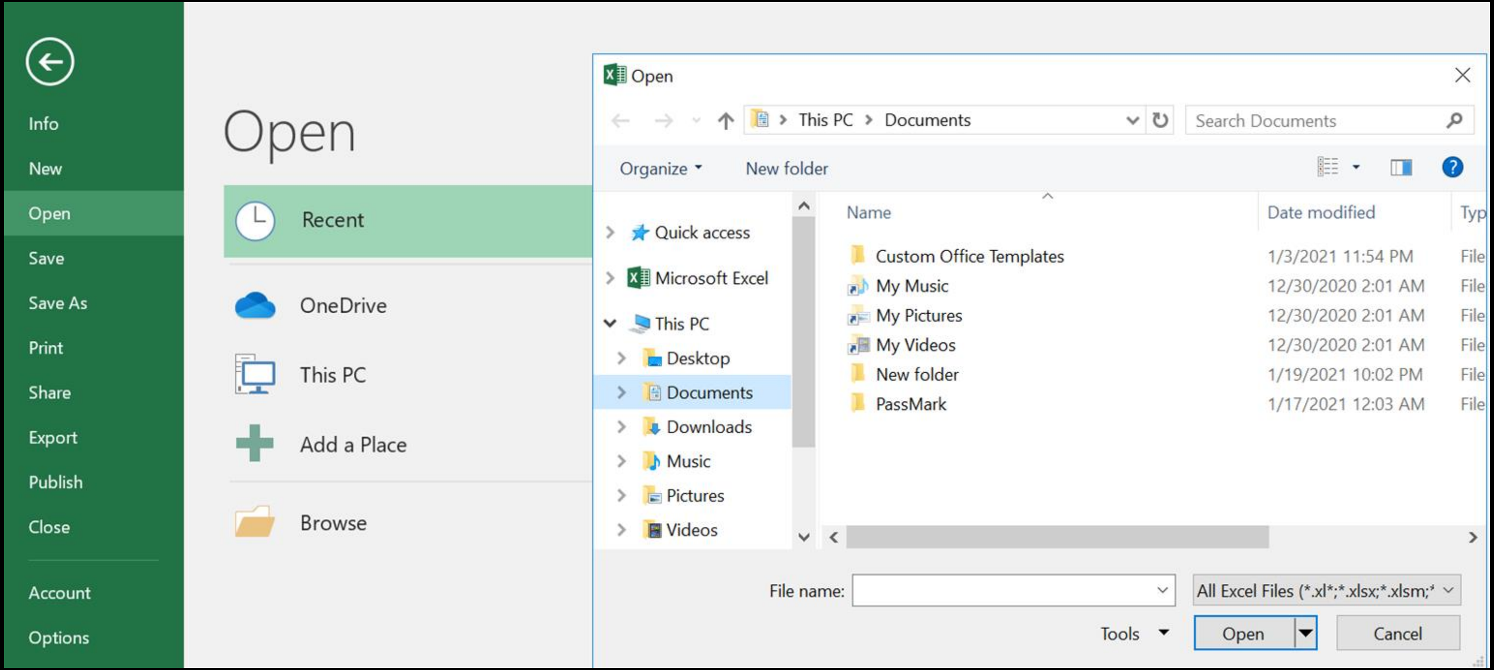
KStrike output is UTF-8 encoded text, easy Excel import!!



```
RoleGuid (RoleName)||TenantId||TotalAccesses||InsertDate||LastAccess||RawAddress||ConvertedAddress (Correlated_HostName(s))||AuthenticatedUserName||
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||347||2020-01-01 00:00:04.455050||2020-04-22 14:18:18.5
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||72565||2020-01-01 00:00:05.102196||2020-04-28 06:43:22
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||175686||2020-01-01 00:00:21.665844
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||1103266||2020-01-01 00:00:27.57014
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||242981||2020-01-01 00:00:30.407758||2020-04-28 09:28:3
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||148647||2020-01-01 00:00:31.342906||2020-04-28 06:15:2
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||13347||2020-01-01 00:01:03.998380||2020-04-28 07:18:05
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||19246||2020-01-01 00:01:04.019708||2020-04-28 07:20:53
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||147||2020-01-01 00:02:08.080692||2020-03-11 16:24:45.3
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||169||2020-01-01 00:02:23.476392||2020-03-02 17:04:36.6
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||348||2020-01-01 00:02:37.269594||2020-04-10 17:43:20.2
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||3037||2020-01-01 00:02:37.404348||
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||616668||2020-01-01 00:03:06.183108
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||4349||2020-01-01 00:03:06.589656||
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||12819||2020-01-01 00:03:07.107798||2020-04-28 07:29:18
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||20777||2020-01-01 00:03:43.254122||2020-04-28 06:41:24
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||37607||2020-01-01 00:04:31.117248|
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||12377||2020-01-01 00:05:43.392706||2020-04-28 07:26:19
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||10752||2020-01-01 00:06:05.754688||2020-04-28 06:29:48
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||11750||2020-01-01 00:07:10.551786||2020-04-28 06:38:10
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||4839||2020-01-01 00:08:15.082610||2020-04-28 02:07:48.
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||970||2020-01-01 00:11:34.051058||2020-01-26 10:14:47.3
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||12252||2020-01-01 00:12:44.783974||2020-04-28 06:36:48
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||129||2020-01-01 00:14:01.037584||2
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||5997||2020-01-01 00:14:42.025294||2020-04-27 21:15:02.
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||290||2020-01-01 00:16:08.866846||2
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||566||2020-01-01 00:17:18.025072||2
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||13195||2020-01-01 00:24:26.283414||2020-04-28 07:23:08
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||76||2020-01-01 00:25:20.074892||20
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0000-000000000000}||5587||2020-01-01 00:26:11.371134||2020-04-28 06:30:54.
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||406||2020-01-01 00:27:51.247266||2
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||{C1AD3A91-C98F-1DEA-B119-BC0E3848CBE}||4191||2020-01-01 00:32:51.421226||
```

Important Excel Import - Windows

First, choose to open the text file with the KStrike output:



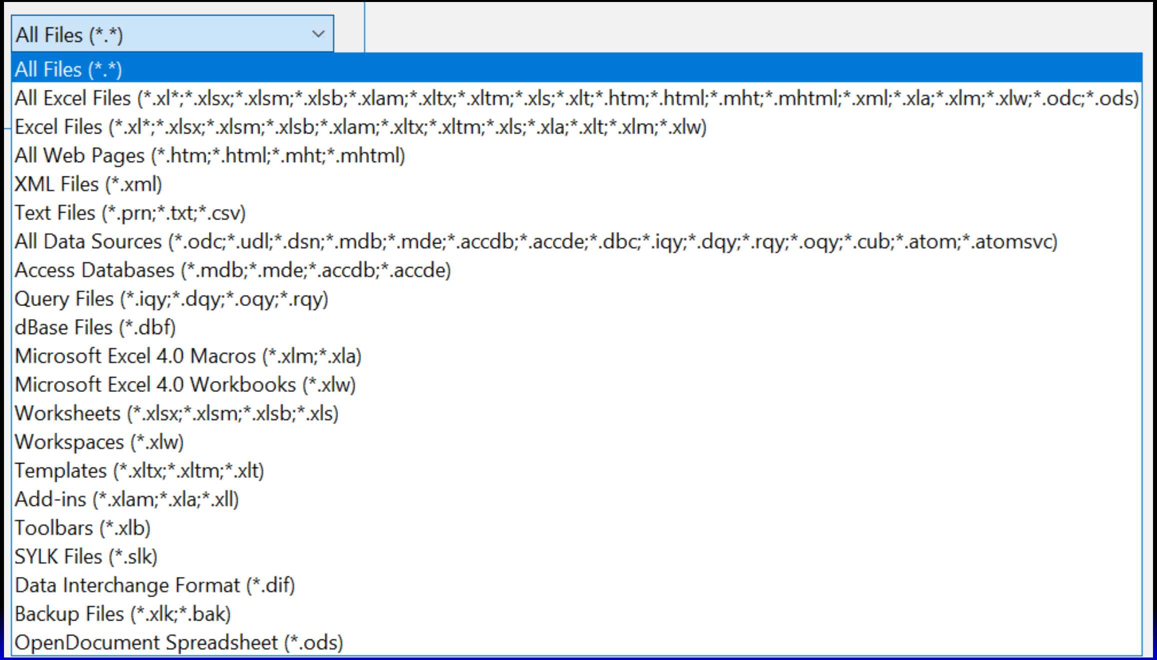
Name	Date modified	Typ
Custom Office Templates	1/3/2021 11:54 PM	File
My Music	12/30/2020 2:01 AM	File
My Pictures	12/30/2020 2:01 AM	File
My Videos	12/30/2020 2:01 AM	File
New folder	1/19/2021 10:02 PM	File
PassMark	1/17/2021 12:03 AM	File

File name:

All Excel Files (*.xl*;*.xlsx;*.xlsm;*

Important Excel Import - Windows

Then, make the selection of the text file you would like to import (be sure to select "All Files")

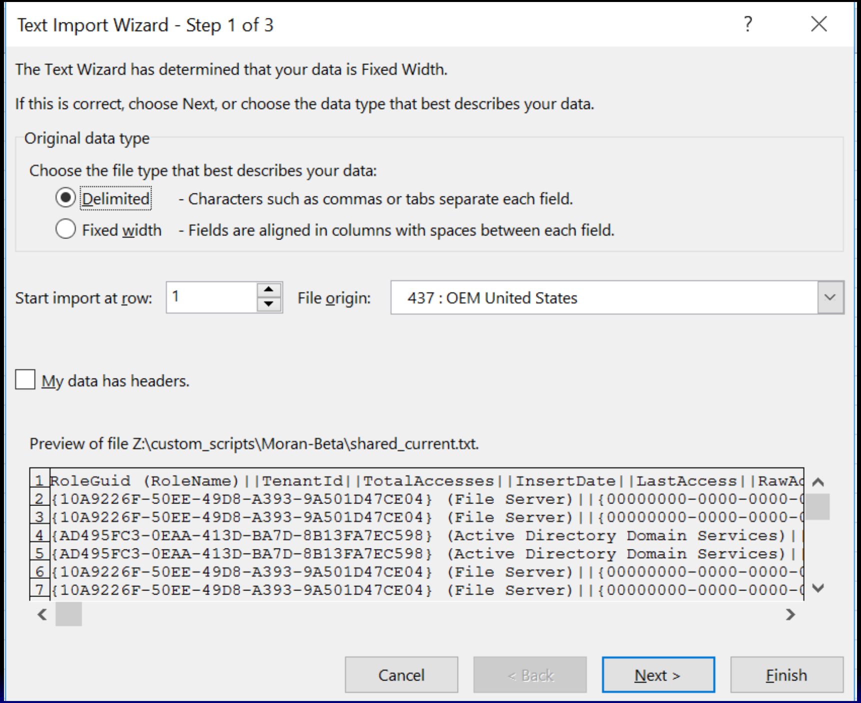


All Files (*.*)

All Files (*.*)
All Excel Files (*.xl*;*.xlsx;*.xlsm;*.xlsb;*.xlam;*.xltx;*.xltm;*.xls;*.xlt;*.htm;*.html;*.mht;*.mhtml;*.xml;*.xla;*.xlm;*.xlw;*.odc;*.ods)
Excel Files (*.xl*;*.xlsx;*.xlsm;*.xlsb;*.xlam;*.xltx;*.xltm;*.xls;*.xla;*.xlt;*.xlm;*.xlw)
All Web Pages (*.htm;*.html;*.mht;*.mhtml)
XML Files (*.xml)
Text Files (*.prn;*.txt;*.csv)
All Data Sources (*.odc;*.udl;*.dsn;*.mdb;*.mde;*.accdb;*.accde;*.dbc;*.iqy;*.dqy;*.rqy;*.oqy;*.cub;*.atom;*.atomsvc)
Access Databases (*.mdb;*.mde;*.accdb;*.accde)
Query Files (*.iqy;*.dqy;*.oqy;*.rqy)
dBase Files (*.dbf)
Microsoft Excel 4.0 Macros (*.xlm;*.xla)
Microsoft Excel 4.0 Workbooks (*.xlw)
Worksheets (*.xlsx;*.xlsm;*.xlsb;*.xls)
Workspaces (*.xlw)
Templates (*.xltx;*.xltm;*.xlt)
Add-ins (*.xlam;*.xla;*.xll)
Toolbars (*.xlb)
SYLK Files (*.slk)
Data Interchange Format (*.dif)
Backup Files (*.xlk;*.bak)
OpenDocument Spreadsheet (*.ods)

Important Excel Import - Windows

Then, the Text Import Wizard will open



Text Import Wizard - Step 1 of 3

The Text Wizard has determined that your data is Fixed Width.

If this is correct, choose Next, or choose the data type that best describes your data.

Original data type

Choose the file type that best describes your data:

● Delimited - Characters such as commas or tabs separate each field.

○ Fixed width - Fields are aligned in columns with spaces between each field.

Start import at row: 1

File origin: 437 : OEM United States

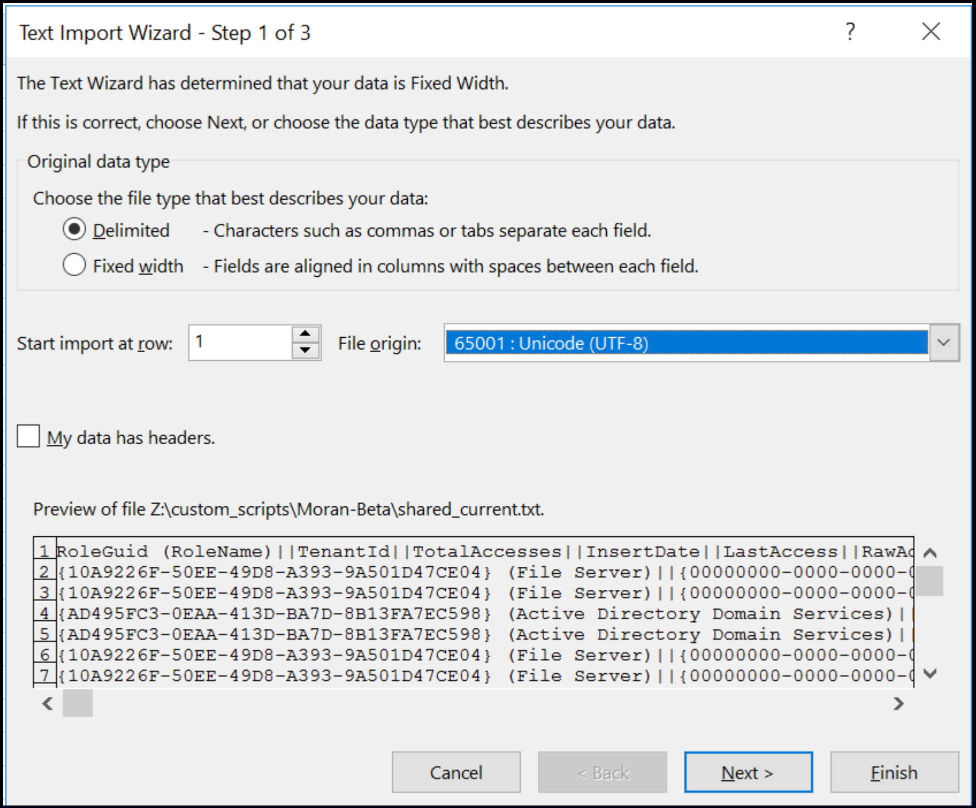
□ My data has headers.

Preview of file Z:\custom_scripts\Moran-Beta\shared_current.txt.

```
RoleGuid (RoleName)||TenantId||TotalAccesses||InsertDate||LastAccess||RawAc
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
```

Important Excel Import - Windows

Select “Delimited”
Select “File origin” as ‘65001 : Unicode (UTF-8)’



The Text Wizard has determined that your data is Fixed Width.

If this is correct, choose Next, or choose the data type that best describes your data.

Original data type

Choose the file type that best describes your data:

● Delimited - Characters such as commas or tabs separate each field.

○ Fixed width - Fields are aligned in columns with spaces between each field.

Start import at row: 1 File origin: 65001 : Unicode (UTF-8)

□ My data has headers.

Preview of file Z:\custom_scripts\Moran-Beta\shared_current.txt.

```
1 RoleGuid (RoleName)||TenantId||TotalAccesses||InsertDate||LastAccess||RawAc
2 {10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
3 {10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
4 {AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||
5 {AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)||
6 {10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
7 {10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)||{00000000-0000-0000-0
```

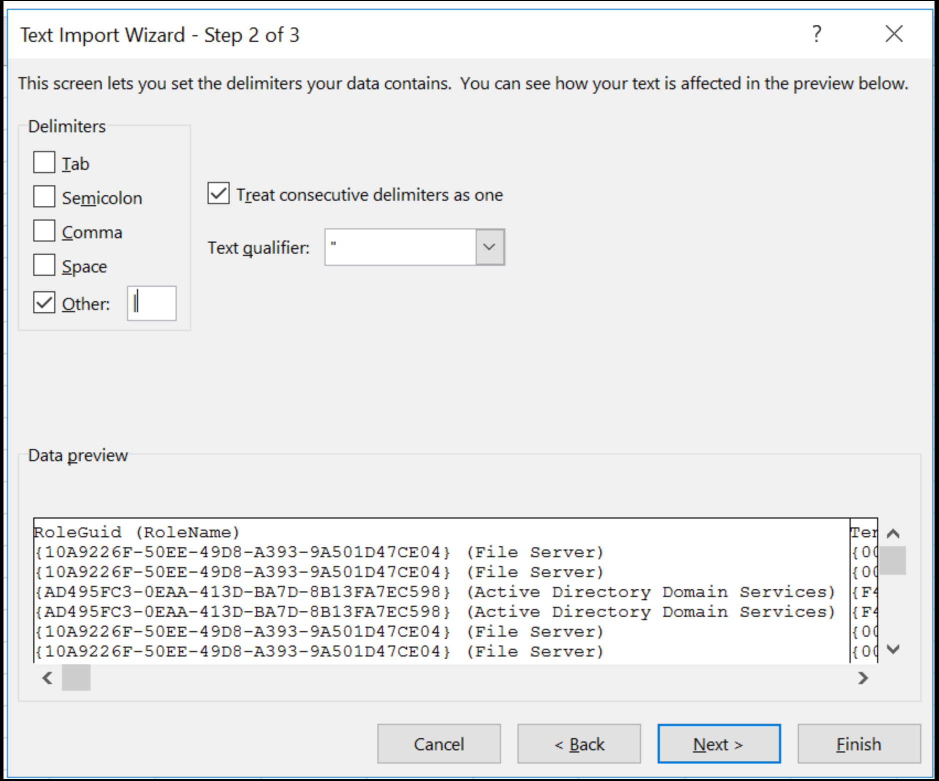
Important Excel Import - Windows

Deselect “Tab”

Select “Other”

- Fill in |

Select “Treat consecutive delimiters as one”



Text Import Wizard - Step 2 of 3

This screen lets you set the delimiters your data contains. You can see how your text is affected in the preview below.

Delimiters

☐ Tab

☐ Semicolon

☐ Comma

☐ Space

☑ Other: |

☑ Treat consecutive delimiters as one

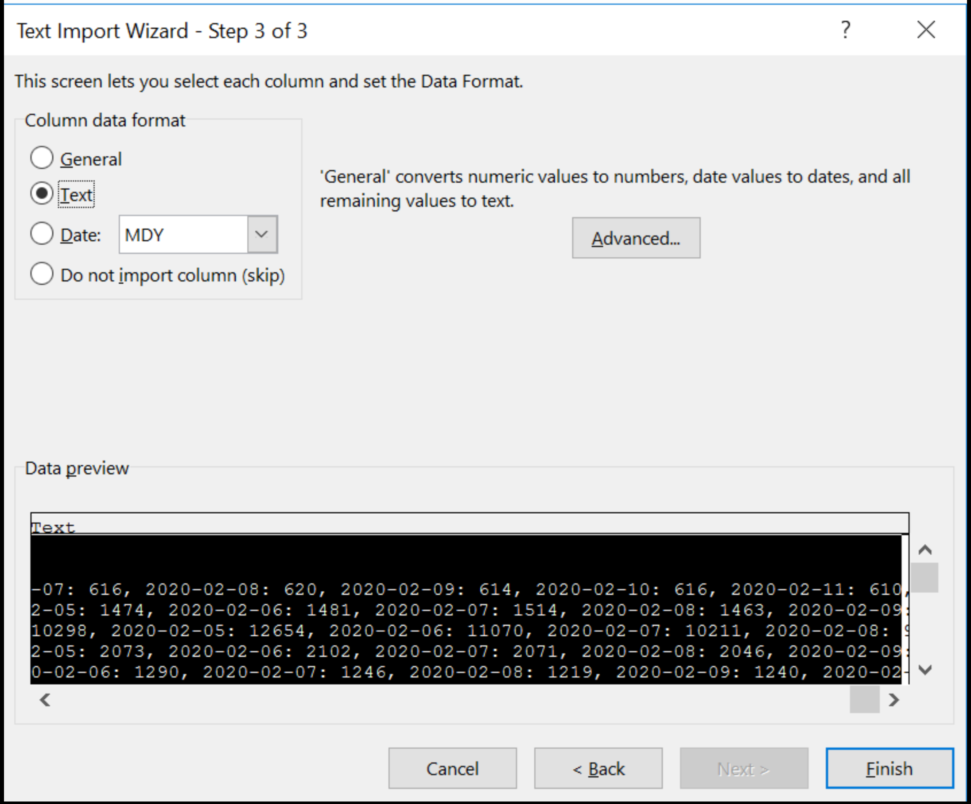
Text qualifier: "

Data preview

```
RoleGuid (RoleName)                                                   Ter
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)                  {0(
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)                  {0(
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services) {F4
{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services) {F4
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)                  {0(
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)                  {0(
```

Important Excel Import - Windows

Select/Highlight all columns
Select “Text” as column data format



This screen lets you select each column and set the Data Format.

Column data format

○ General
● Text
○ Date: MDY
○ Do not import column (skip)

'General' converts numeric values to numbers, date values to dates, and all remaining values to text.

Data preview

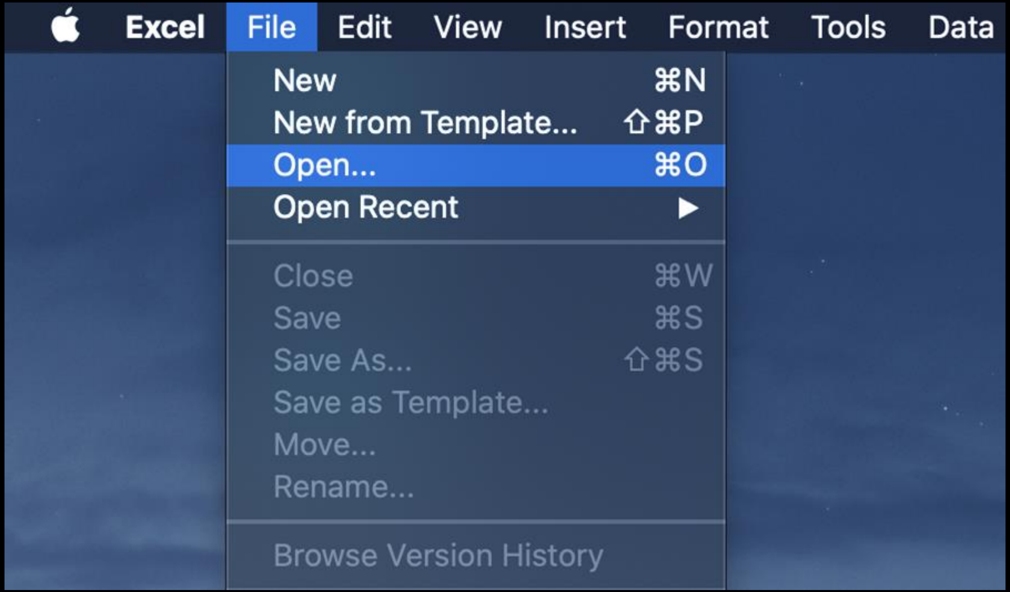
```
Text


-07: 616, 2020-02-08: 620, 2020-02-09: 614, 2020-02-10: 616, 2020-02-11: 610,
2-05: 1474, 2020-02-06: 1481, 2020-02-07: 1514, 2020-02-08: 1463, 2020-02-09
10298, 2020-02-05: 12654, 2020-02-06: 11070, 2020-02-07: 10211, 2020-02-08:
2-05: 2073, 2020-02-06: 2102, 2020-02-07: 2071, 2020-02-08: 2046, 2020-02-09
0-02-06: 1290, 2020-02-07: 1246, 2020-02-08: 1219, 2020-02-09: 1240, 2020-02-
```

Cool. But What if I Have a Mac?

No worries. It’s different, but kinda similar. So ...

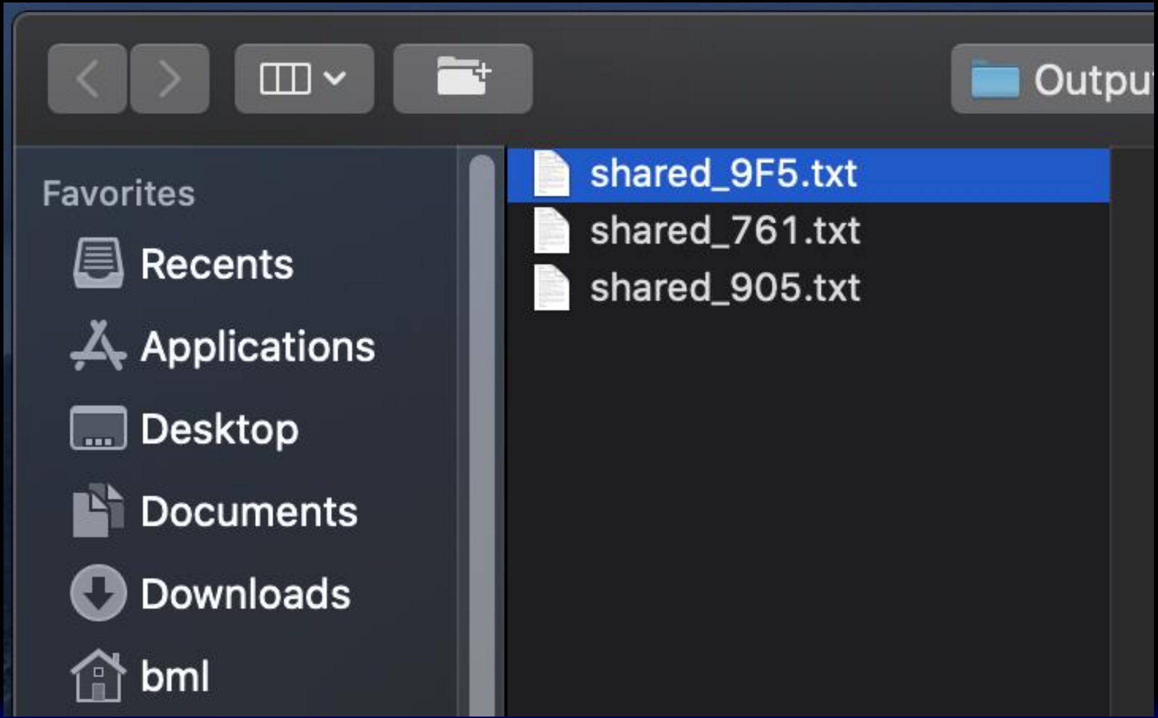
Important Excel Import - MacOS

First, choose to open the text file with the KStrike output:



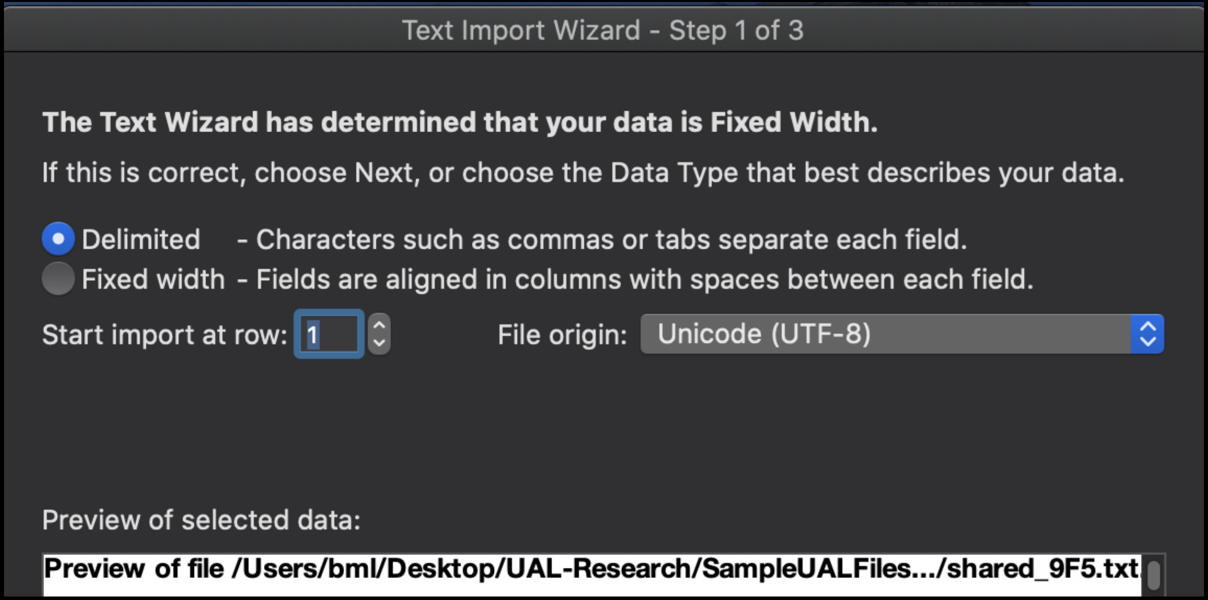
Important Excel Import - MacOS

Then, make the selection of the text file you would like:



Important Excel Import - MacOS

Select “Delimited” and select “File origin” as Unicode (UTF-8)



The Text Wizard has determined that your data is Fixed Width.

If this is correct, choose Next, or choose the Data Type that best describes your data.

● Delimited - Characters such as commas or tabs separate each field.

○ Fixed width - Fields are aligned in columns with spaces between each field.

Start import at row: 1

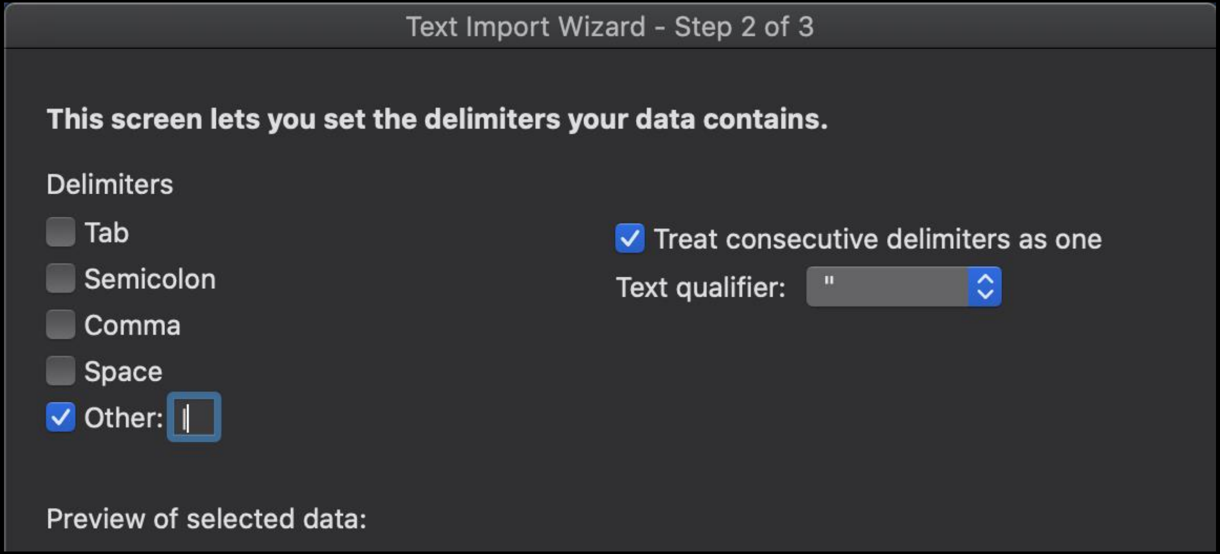
File origin: Unicode (UTF-8)

Preview of selected data:

Preview of file /Users/bml/Desktop/UAL-Research/SampleUALFiles.../shared_9F5.txt

Important Excel Import - MacOS

Enter | in “Other:”, and select “Treat consecutive delimiters as one”



Text Import Wizard - Step 2 of 3

This screen lets you set the delimiters your data contains.

Delimiters

☐ Tab
☐ Semicolon
☐ Comma
☐ Space
☑ Other: |

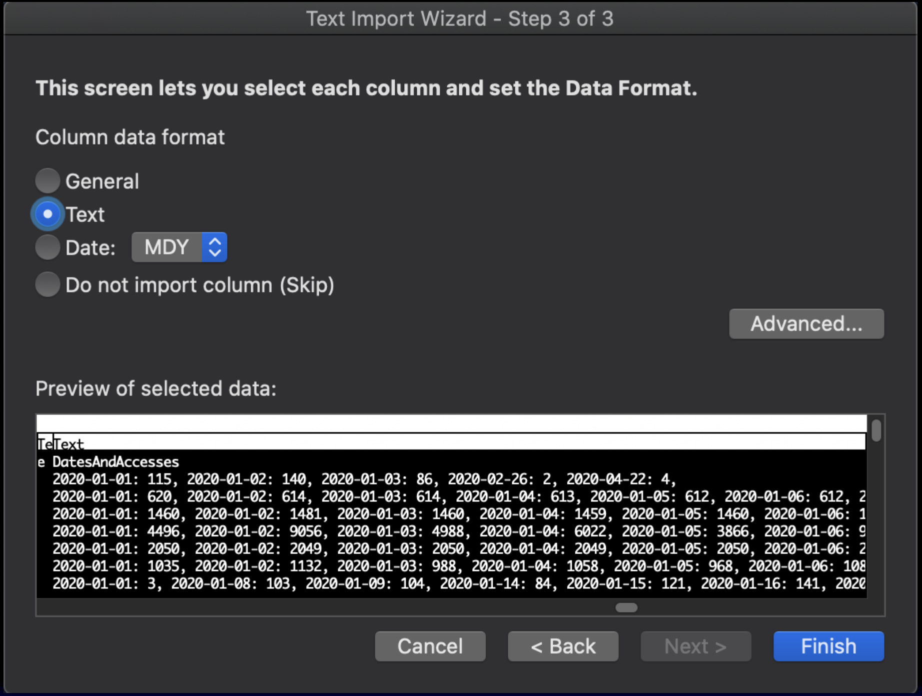
☑ Treat consecutive delimiters as one

Text qualifier: "

Preview of selected data:

Important Excel Import - MacOS

Select all of the columns, and choose “Text” as the Data Format option



Text Import Wizard - Step 3 of 3

This screen lets you select each column and set the Data Format.

Column data format

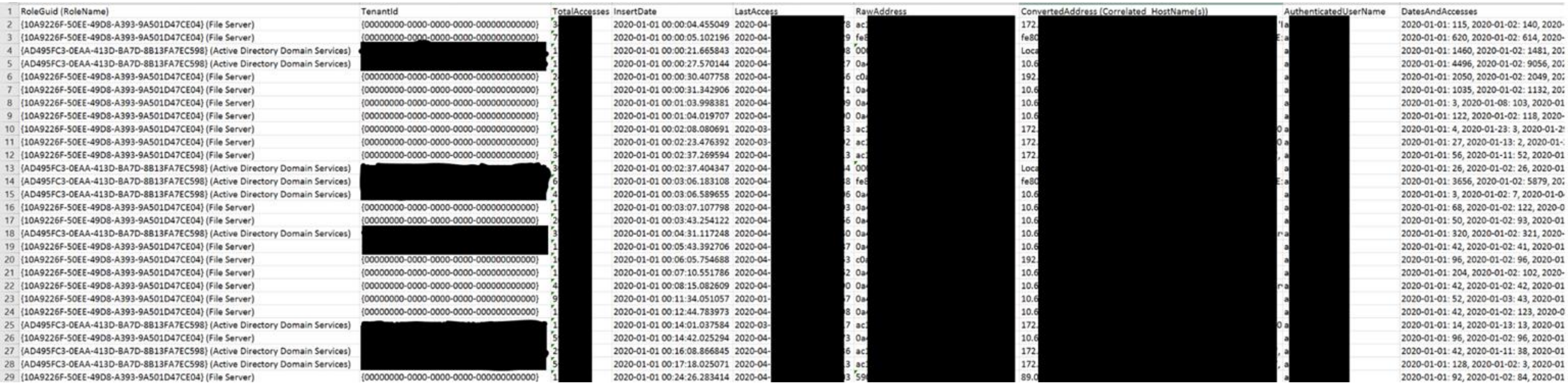
○ General
● Text
○ Date: MDY
○ Do not import column (Skip)

Preview of selected data:

```
TeText
e DatesAndAccesses
  2020-01-01: 115, 2020-01-02: 140, 2020-01-03: 86, 2020-02-26: 2, 2020-04-22: 4,
  2020-01-01: 620, 2020-01-02: 614, 2020-01-03: 614, 2020-01-04: 613, 2020-01-05: 612, 2020-01-06: 612, 2
  2020-01-01: 1460, 2020-01-02: 1481, 2020-01-03: 1460, 2020-01-04: 1459, 2020-01-05: 1460, 2020-01-06: 1
  2020-01-01: 4496, 2020-01-02: 9056, 2020-01-03: 4988, 2020-01-04: 6022, 2020-01-05: 3866, 2020-01-06: 9
  2020-01-01: 2050, 2020-01-02: 2049, 2020-01-03: 2050, 2020-01-04: 2049, 2020-01-05: 2050, 2020-01-06: 2
  2020-01-01: 1035, 2020-01-02: 1132, 2020-01-03: 988, 2020-01-04: 1058, 2020-01-05: 968, 2020-01-06: 108
  2020-01-01: 3, 2020-01-08: 103, 2020-01-09: 104, 2020-01-14: 84, 2020-01-15: 121, 2020-01-16: 141, 2020
```

You Can Fit So Many UAL Entries in Excel

Congratulations! You can now manipulate the Excel file however you would like! (Details redacted, obviously)



	RoleGuid (RoleName)	TenantId	TotalAccesses	InsertDate	LastAccess	RawAddress	ConvertedAddress (Correlated_HostName(s))	AuthenticatedUserName	DatesAndAccesses
2	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:00:04.455049	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 115, 2020-01-02: 140, 2020-
3	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:00:05.102196	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 620, 2020-01-02: 614, 2020-
4	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:00:21.665843	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 1460, 2020-01-02: 1481, 20
5	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:00:27.570144	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 4496, 2020-01-02: 9056, 20
6	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:00:30.407758	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 2050, 2020-01-02: 2049, 20
7	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:00:31.342906	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 1035, 2020-01-02: 1132, 20
8	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:01:03.998381	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 3, 2020-01-08: 103, 2020-01
9	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:01:04.019707	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 122, 2020-01-02: 118, 2020-
10	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:02:08.080691	2020-03- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 4, 2020-01-23: 3, 2020-01-2
11	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:02:23.476392	2020-03- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 27, 2020-01-13: 2, 2020-01-
12	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:02:37.269594	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 56, 2020-01-11: 52, 2020-01
13	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:02:37.404347	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 26, 2020-01-02: 26, 2020-01
14	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:03:06.183108	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 3656, 2020-01-02: 5879, 20
15	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:03:06.589655	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 3, 2020-01-02: 7, 2020-01-0
16	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:03:07.107798	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 68, 2020-01-02: 122, 2020-0
17	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:03:43.254122	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 50, 2020-01-02: 93, 2020-01
18	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:04:31.117248	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 320, 2020-01-02: 321, 2020-
19	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	[redacted]	[redacted]	2020-01-01 00:05:43.392706	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 42, 2020-01-02: 41, 2020-01
20	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:06:05.754688	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 96, 2020-01-02: 96, 2020-01
21	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:07:10.551786	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 204, 2020-01-02: 102, 2020-
22	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:08:15.082609	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 42, 2020-01-02: 42, 2020-01
23	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:11:34.051057	2020-01- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 52, 2020-01-03: 43, 2020-01
24	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:12:44.783973	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 42, 2020-01-02: 123, 2020-0
25	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:14:01.037584	2020-03- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 14, 2020-01-13: 13, 2020-01
26	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	[redacted]	[redacted]	2020-01-01 00:14:42.025294	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 96, 2020-01-02: 96, 2020-01
27	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:16:08.866845	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 42, 2020-01-11: 38, 2020-01
28	{AD495FC3-0EAA-413D-BA7D-8B13FA7EC598} (Active Directory Domain Services)	[redacted]	[redacted]	2020-01-01 00:17:18.025071	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 128, 2020-01-02: 3, 2020-01
29	{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	[redacted]	2020-01-01 00:24:26.283414	2020-04- [redacted]	[redacted]	[redacted]	[redacted]	2020-01-01: 92, 2020-01-02: 84, 2020-01

ESE DB to Excel in One Easy Script!

Other UAL Data Parsing Options

Eric Zimmerman's "SumECmd"

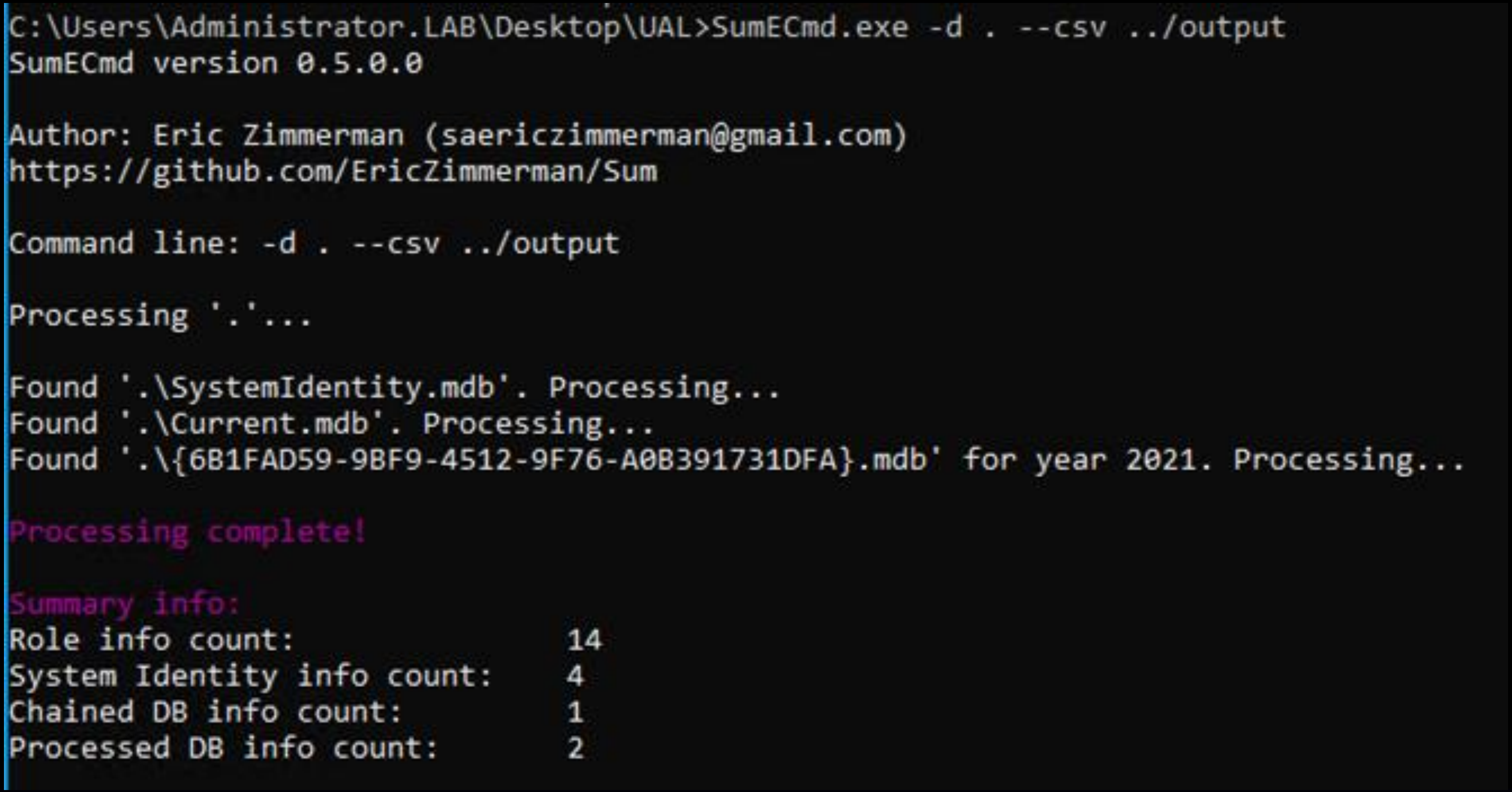
- https://github.com/EricZimmerman/Sum

(NOTE: SumECmd requires the databases to be in a "clean" format. This is not always a viable option from a live system, and you may have to "clean" it)

Mark McKinnon working on an Autopsy plugin

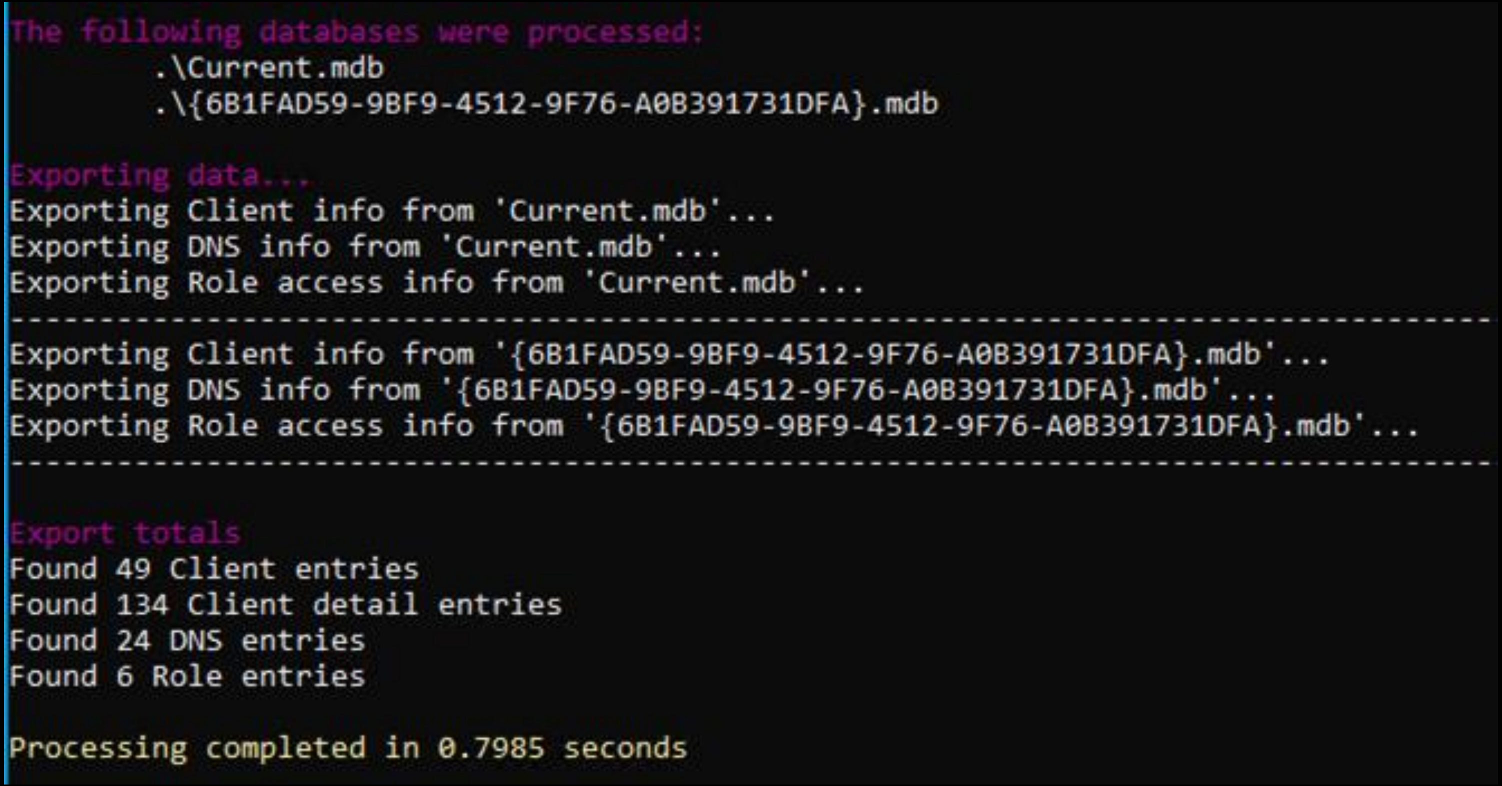
- Because of course he is
- Estimated public release is July 2021

SumECmd Output Example



```
C:\Users\Administrator.LAB\Desktop\UAL>SumECmd.exe -d . --csv ../output
SumECmd version 0.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/Sum

Command line: -d . --csv ../output

Processing '.'...

Found '.\SystemIdentity.mdb'. Processing...
Found '.\Current.mdb'. Processing...
Found '.\{6B1FAD59-9BF9-4512-9F76-A0B391731DFA}.mdb' for year 2021. Processing...

Processing complete!

Summary info:
Role info count:              14
System Identity info count:    4
Chained DB info count:         1
Processed DB info count:       2
```

SumECmd Output Example



```
The following databases were processed:
        .\Current.mdb
        .\{6B1FAD59-9BF9-4512-9F76-A0B391731DFA}.mdb

Exporting data...
Exporting Client info from 'Current.mdb'...
Exporting DNS info from 'Current.mdb'...
Exporting Role access info from 'Current.mdb'...
-----------------------------------------------------------------------------------
Exporting Client info from '{6B1FAD59-9BF9-4512-9F76-A0B391731DFA}.mdb'...
Exporting DNS info from '{6B1FAD59-9BF9-4512-9F76-A0B391731DFA}.mdb'...
Exporting Role access info from '{6B1FAD59-9BF9-4512-9F76-A0B391731DFA}.mdb'...
-----------------------------------------------------------------------------------

Export totals
Found 49 Client entries
Found 134 Client detail entries
Found 24 DNS entries
Found 6 Role entries

Processing completed in 0.7985 seconds
```

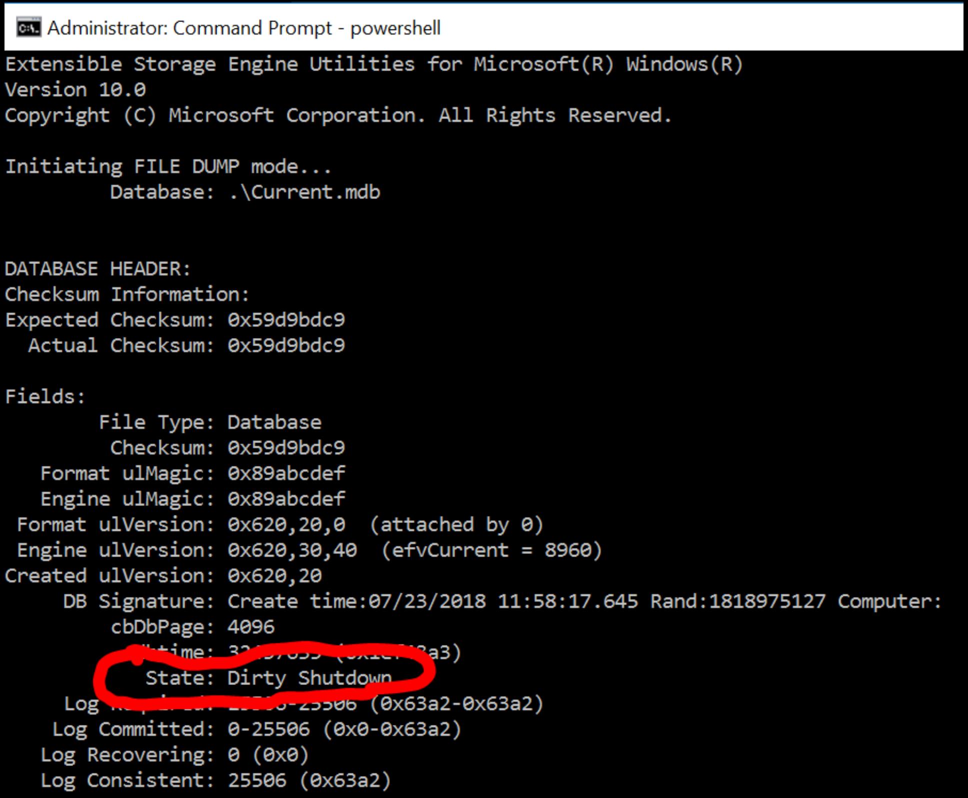
How to Clean ESE DB for Dummies

First, check the status of the database file(s)

- Open PowerShell (as Administrator)
- Set path to folder with UAL files
  - *Set-Location -Path {FOLDER PATH}*
- Run ‘esentutl’ command to check on the database status
  - *esentutl.exe /mh {dbname).mdb*
- If it is “dirty”, restore it
  - *esentutl.exe /r svc /i*
  - *esentutl.exe /p {dbname}.mdb* (for all of them. Be sure to click prompts!)

IMPORTANT NOTE: KStrike will process a “clean” or “dirty” database, but these steps are “best practices” for dealing with ESE databases

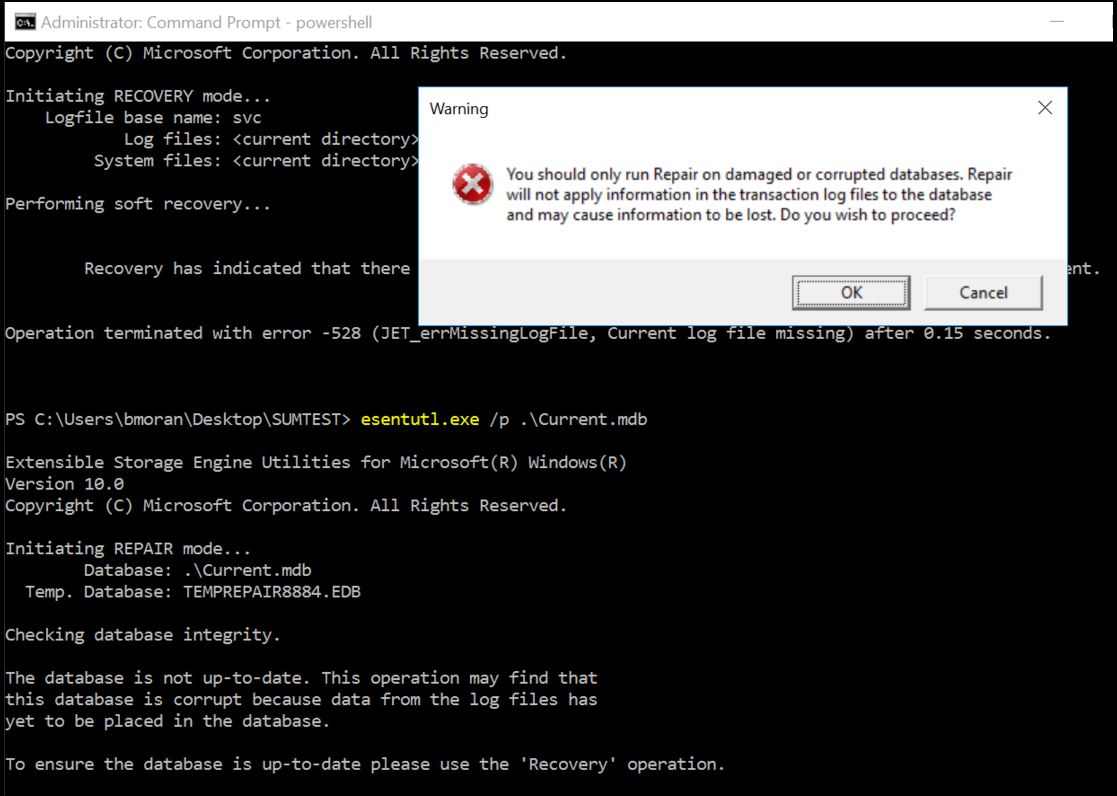
Cleaning ESE DB Examples



Administrator: Command Prompt - powershell

```
Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
         Database: .\Current.mdb


DATABASE HEADER:
Checksum Information:
Expected Checksum: 0x59d9bdc9
  Actual Checksum: 0x59d9bdc9

Fields:
        File Type: Database
         Checksum: 0x59d9bdc9
   Format ulMagic: 0x89abcdef
   Engine ulMagic: 0x89abcdef
 Format ulVersion: 0x620,20,0  (attached by 0)
 Engine ulVersion: 0x620,30,40  (efvCurrent = 8960)
Created ulVersion: 0x620,20
     DB Signature: Create time:07/23/2018 11:58:17.645 Rand:1818975127 Computer:
         cbDbPage: 4096
           dbtime: 32[illegible] (0x[illegible]a3)
            State: Dirty Shutdown
     Log Required: 25506-25506 (0x63a2-0x63a2)
    Log Committed: 0-25506 (0x0-0x63a2)
   Log Recovering: 0 (0x0)
   Log Consistent: 25506 (0x63a2)
```

Cleaning ESE DB Examples

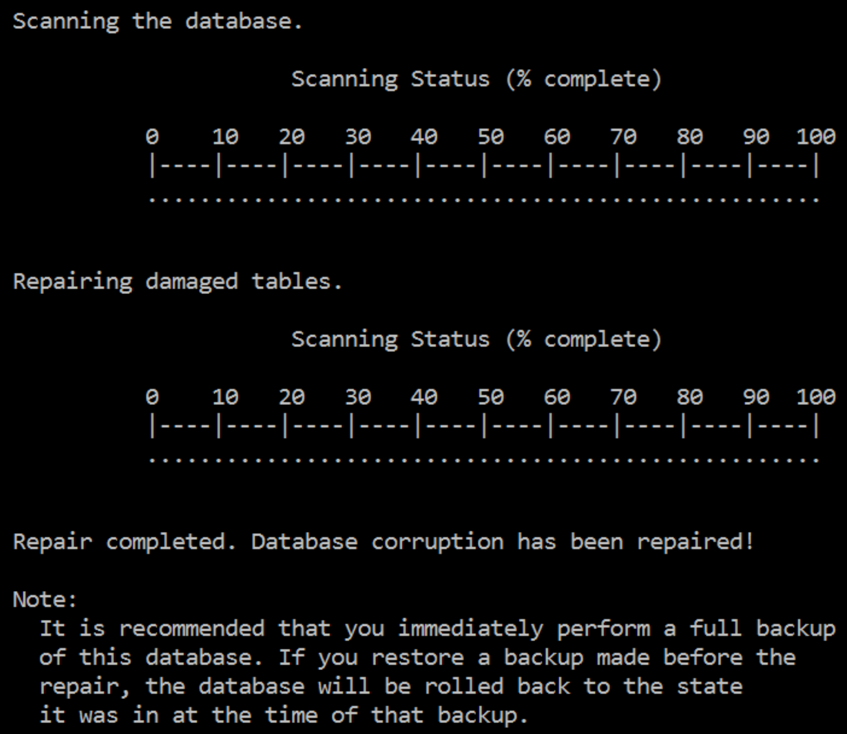


```
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating RECOVERY mode...
    Logfile base name: svc
            Log files: <current directory>
         System files: <current directory>

Performing soft recovery...


        Recovery has indicated that there                                          ent.


Operation terminated with error -528 (JET_errMissingLogFile, Current log file missing) after 0.15 seconds.



PS C:\Users\bmoran\Desktop\SUMTEST> esentutl.exe /p .\Current.mdb

Extensible Storage Engine Utilities for Microsoft(R) Windows(R)
Version 10.0
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating REPAIR mode...
        Database: .\Current.mdb
  Temp. Database: TEMPREPAIR8884.EDB

Checking database integrity.

The database is not up-to-date. This operation may find that
this database is corrupt because data from the log files has
yet to be placed in the database.

To ensure the database is up-to-date please use the 'Recovery' operation.
```

Warning

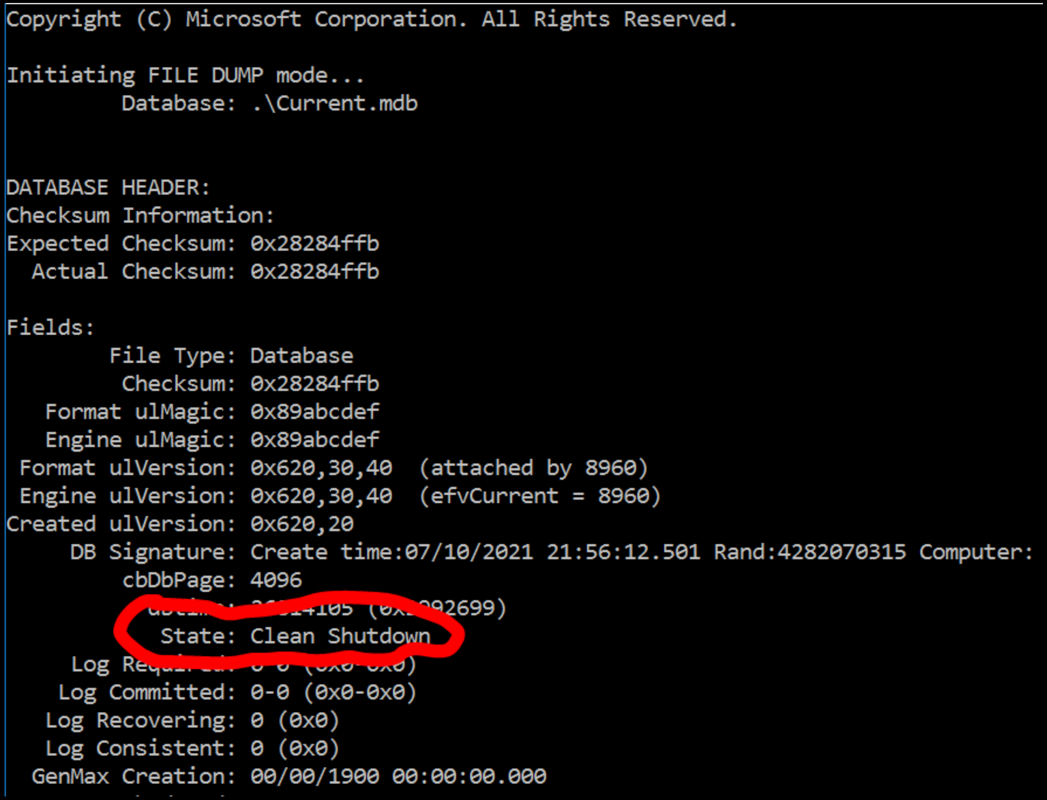
You should only run Repair on damaged or corrupted databases. Repair will not apply information in the transaction log files to the database and may cause information to be lost. Do you wish to proceed?

Cleaning ESE DB Examples



```
Scanning the database.

                     Scanning Status (% complete)

          0    10   20   30   40   50   60   70   80   90   100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................


Repairing damaged tables.

                     Scanning Status (% complete)

          0    10   20   30   40   50   60   70   80   90   100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................


Repair completed. Database corruption has been repaired!

Note:
  It is recommended that you immediately perform a full backup
  of this database. If you restore a backup made before the
  repair, the database will be rolled back to the state
  it was in at the time of that backup.
```

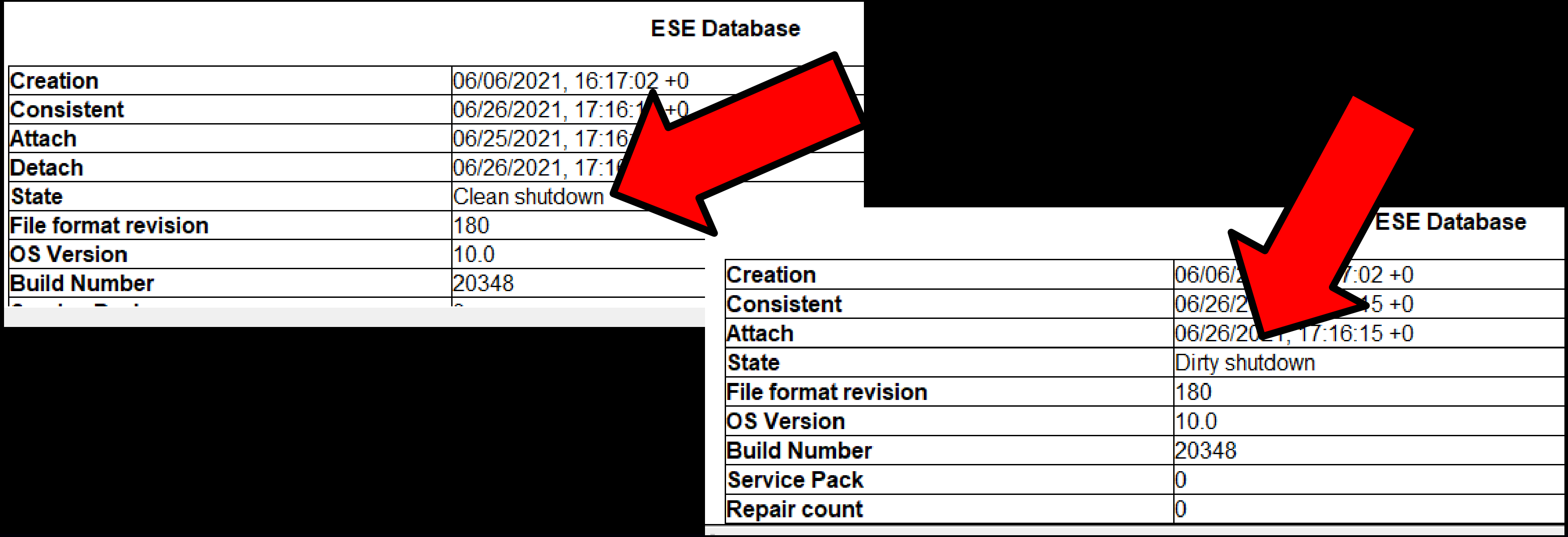
Cleaning ESE DB Examples



```
Copyright (C) Microsoft Corporation. All Rights Reserved.

Initiating FILE DUMP mode...
         Database: .\Current.mdb


DATABASE HEADER:
Checksum Information:
Expected Checksum: 0x28284ffb
  Actual Checksum: 0x28284ffb

Fields:
        File Type: Database
         Checksum: 0x28284ffb
   Format ulMagic: 0x89abcdef
   Engine ulMagic: 0x89abcdef
 Format ulVersion: 0x620,30,40  (attached by 8960)
 Engine ulVersion: 0x620,30,40  (efvCurrent = 8960)
Created ulVersion: 0x620,20
     DB Signature: Create time:07/10/2021 21:56:12.501 Rand:4282070315 Computer:
         cbDbPage: 4096
           dbtime: 26814105 (0x1992699)
            State: Clean Shutdown
     Log Required: 0-0 (0x0-0x0)
    Log Committed: 0-0 (0x0-0x0)
   Log Recovering: 0 (0x0)
   Log Consistent: 0 (0x0)
  GenMax Creation: 00/00/1900 00:00:00.000
```

Command Line Challenged?

Your favorite forensic tool (not named Mark McKinnon) may tell you the ESE database state too!



ESE Database

Creation	06/06/2021, 16:17:02 +0
Consistent	06/26/2021, 17:16:[illegible] +0
Attach	06/25/2021, 17:16[illegible]
Detach	06/26/2021, 17:1[illegible]
State	Clean shutdown
File format revision	180
OS Version	10.0
Build Number	20348

ESE Database

Creation	06/06/[illegible]7:02 +0
Consistent	06/26/2[illegible]5 +0
Attach	06/26/20[illegible], 17:16:15 +0
State	Dirty shutdown
File format revision	180
OS Version	10.0
Build Number	20348
Service Pack	0
Repair count	0

Real World UAL Parsing Benefits

Ransomware (I know, ugh)

IR firm tasked with answering typical questions (who, what, when, where, data exfil, etc)

Followed timeline access patterns until external IP connecting to the environment was found

- Allowing easy identification of “Patient Zero”

Thanks Shanna! (@fancy_flare)

Future Research Goals

Azure, hybrid cloud/on-prem instances

Changes/modifications as more people find out about it

- GUID correlation with additional server roles
- Troubleshooting/bugs with KStrike
  - Please use, contribute, provide feedback!

Follow up with more research tenant ID data

- Thus far, seems to be software dependent
- Need more data with populated tenant ID data

What happens when server roles change/modified?

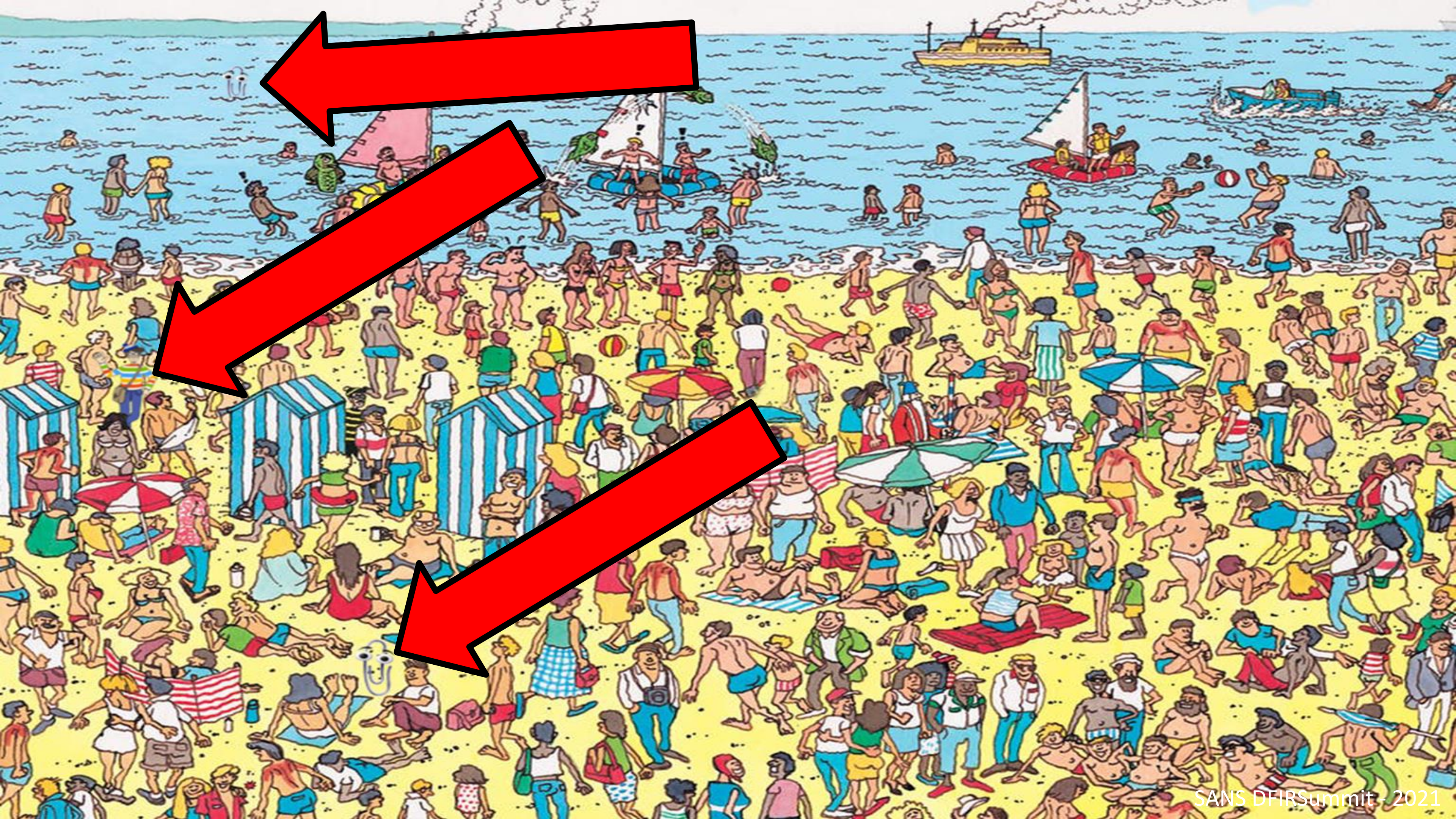
Non-domain system correlation to “anonymous logon” activity

Special Thanks

KPMG Cyber Response Services
Patrick Bennett - CrowdStrike
Microsoft - specifically Nick & Troy
Mark McKinnon
Mark Baggett

… and of course, SVR

… and one more thing …



SANS DFIR SUMMIT & TRAINING 2021

Questions?

Please download/use KStrike: *https://github.com/brimorlabs/KStrike*

Kevin Stokes

Twitter: **@kev365**

Brian Moran

Twitter: **@brianjmoran**