How to Contribute to and Benefit from Open-Source Contributions

EZ Tools/KAPE

Andrew Rathbun, Senior Associate, Kroll Cyber Risk

July 2021

About Andrew Rathbun

Senior Associate, Kroll Cyber Risk

My DFIR Journey

- 2020-Present: Senior Associate at Kroll
  - Digital Forensics & Incident Response
  - KAPE Instructor
- 2019-2020: HHS OIG
  - Forensic Computer Examiner (2210)
- 2012-2019: Michigan State University Police Department
  - 2016-2019: Detective (digital forensics and general investigations)
  - 2012-2015: Police Officer
- 2005-2011: USMC Veteran (0311)
- Bachelor's: Criminal Justice/Sociology
- Master's: HR Administration

Side Projects

- 2018-Present: Administrator of the Digital Forensics Discord Server
  - 2020 DFIR Resource of the Year – Nominee
  - 2019 DFIR Resource of the Year – Winner
- 2019-Present: AboutDFIR.com Contributor
  - 2020 DFIR Resource of the Year – Nominee
  - 2019 DFIR Resource of the Year – Nominee
- 2020-Present: GitHub
- LinkedIn (andrewrathbun), Twitter (@bunsofwrath12), GitHub (rathbuna)

Introduction

What to expect from this presentation

- A lot of information in a small amount of time
  - Use the pause/rewind features when the recording goes live
- Animated GIFs
- Forensic Tools and their ancillary files covered
  - RECmd – Batch files
  - SQLECmd – Maps
  - EvtxECmd – Maps
  - KAPE – Targets/Modules
- Definition of “ancillary” by Oxford
  - Adjective: Providing necessary support to the primary activities or operation of an organization, institution, industry, or system.
  - Example: "the development of ancillary services to support its products"
- Tools of the Trade
  - I’ll list some tools (free and paid) that I use in my daily research travels
- Assumptions this presentation makes
  - You’re at least somewhat familiar with EZ Tools and KAPE and are curious what influences the CSV output

Why Should I Care?

A life without cause is a life without effect

- Why should I care about this topic?
  - You should know what makes your tools tick so you can better speak to the magic that’s going on behind the scenes
  - You should know what’s going on behind the scenes so you can help make it BETTER for yourself and others
  - You should strongly consider helping to make the tools better because it very well could save someone’s life or help solve a case/engagement that doesn’t involve life or limb
- But don’t I have to know how to code?
  - I currently don’t, so you don’t either. All you need is inspiration, motivation, and follow-through. At the beginning, you also might need a mentor that can provide some direction.
- This presentation aims to help inspire your DFIR creativity so we can all benefit as well as educate the end users of these tools to better understand how they work
- This presentation also aims to empower those who feel like they don’t have the “necessary” skills needed to contribute to the DFIR community in any meaningful fashion. Showing up is half the battle!

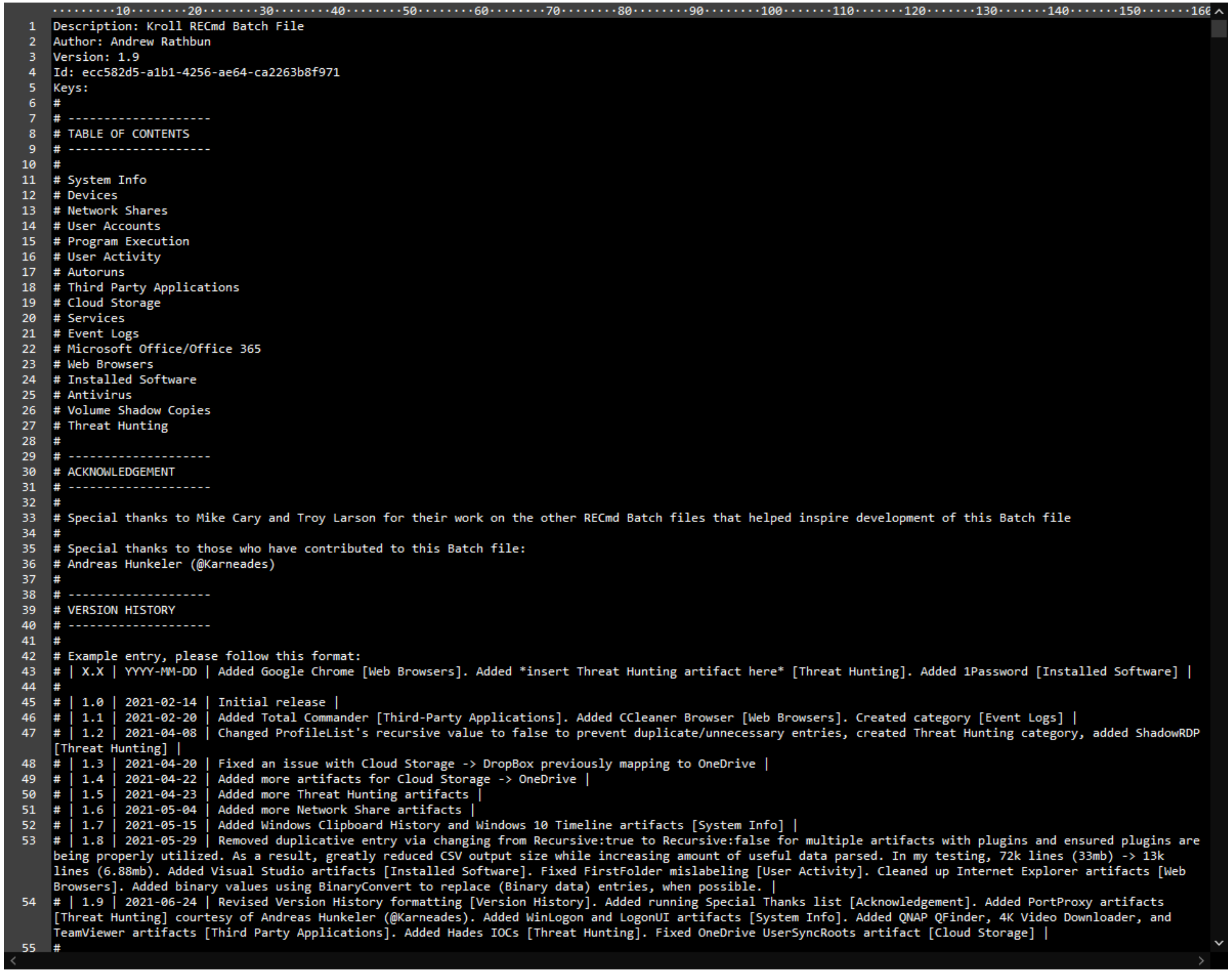
RECmd

Batch Files

RECmd Batch Files

What are they and why do I care?

- Batch files give RECmd instructions on which Keys, SubKeys, and Values to parse and include into the tool’s CSV output
- Multiple Batch files exists within the .\RegistryExplorer\BatchExamples directory
- RECmd_Kroll.reb is the most actively maintained Batch file
  - Serves as a useful way to learn about important Registry artifacts
  - Documentation included for each artifact, if it exists
  - Comments help provide context to understand the data
  - Optimized for triggering Plugins to generate output
- RECmd boasts extra columns within CSV output for Plugins to display parsed data in:
  - ValueData (native to Windows Registry)
  - ValueData2 and ValueData3 (native to RECmd)

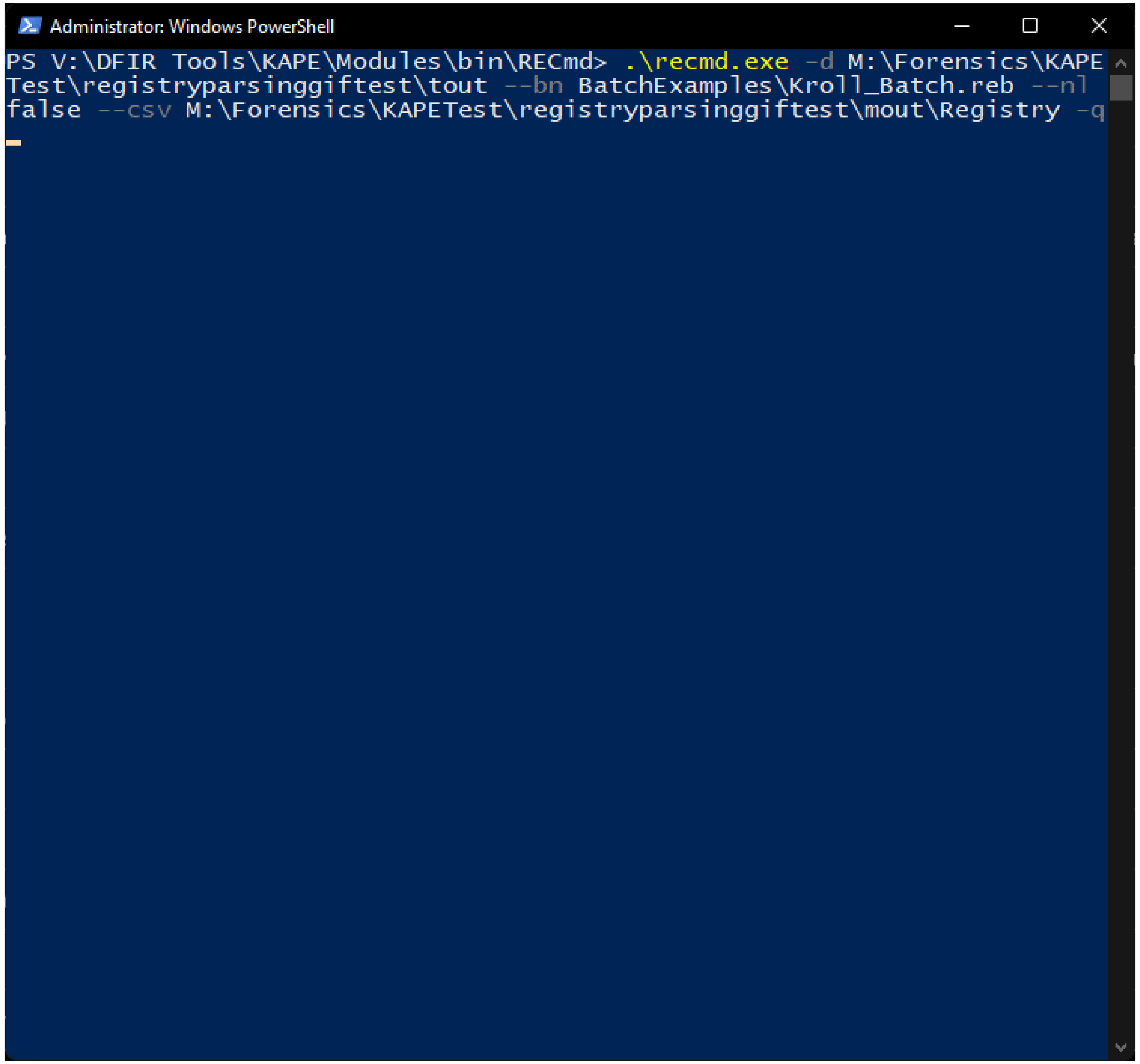


```
Description: Kroll RECmd Batch File
Author: Andrew Rathbun
Version: 1.9
Id: ecc582d5-a1b1-4256-ae64-ca2263b8f971
Keys:
#
# --------------------
# TABLE OF CONTENTS
# --------------------
#
# System Info
# Devices
# Network Shares
# User Accounts
# Program Execution
# User Activity
# Autoruns
# Third Party Applications
# Cloud Storage
# Services
# Event Logs
# Microsoft Office/Office 365
# Web Browsers
# Installed Software
# Antivirus
# Volume Shadow Copies
# Threat Hunting
#
# --------------------
# ACKNOWLEDGEMENT
# --------------------
#
# Special thanks to Mike Cary and Troy Larson for their work on the other RECmd Batch files that helped inspire development of this Batch file
#
# Special thanks to those who have contributed to this Batch file:
# Andreas Hunkeler (@Karneades)
#
# --------------------
# VERSION HISTORY
# --------------------
#
# Example entry, please follow this format:
# | X.X | YYYY-MM-DD | Added Google Chrome [Web Browsers]. Added *insert Threat Hunting artifact here* [Threat Hunting]. Added 1Password [Installed Software] |
#
# | 1.0 | 2021-02-14 | Initial release |
# | 1.1 | 2021-02-20 | Added Total Commander [Third-Party Applications]. Added CCleaner Browser [Web Browsers]. Created category [Event Logs] |
# | 1.2 | 2021-04-08 | Changed ProfileList's recursive value to false to prevent duplicate/unnecessary entries, created Threat Hunting category, added ShadowRDP [Threat Hunting] |
# | 1.3 | 2021-04-20 | Fixed an issue with Cloud Storage -> DropBox previously mapping to OneDrive |
# | 1.4 | 2021-04-22 | Added more artifacts for Cloud Storage -> OneDrive |
# | 1.5 | 2021-04-23 | Added more Threat Hunting artifacts |
# | 1.6 | 2021-05-04 | Added more Network Share artifacts |
# | 1.7 | 2021-05-15 | Added Windows Clipboard History and Windows 10 Timeline artifacts [System Info] |
# | 1.8 | 2021-05-29 | Removed duplicative entry via changing from Recursive:true to Recursive:false for multiple artifacts with plugins and ensured plugins are being properly utilized. As a result, greatly reduced CSV output size while increasing amount of useful data parsed. In my testing, 72k lines (33mb) -> 13k lines (6.88mb). Added Visual Studio artifacts [Installed Software]. Fixed FirstFolder mislabeling [User Activity]. Cleaned up Internet Explorer artifacts [Web Browsers]. Added binary values using BinaryConvert to replace (Binary data) entries, when possible. |
# | 1.9 | 2021-06-24 | Revised Version History formatting [Version History]. Added running Special Thanks list [Acknowledgement]. Added PortProxy artifacts [Threat Hunting] courtesy of Andreas Hunkeler (@Karneades). Added WinLogon and LogonUI artifacts [System Info]. Added QNAP QFinder, 4K Video Downloader, and TeamViewer artifacts [Third Party Applications]. Added Hades IOCs [Threat Hunting]. Fixed OneDrive UserSyncRoots artifact [Cloud Storage] |
#
```

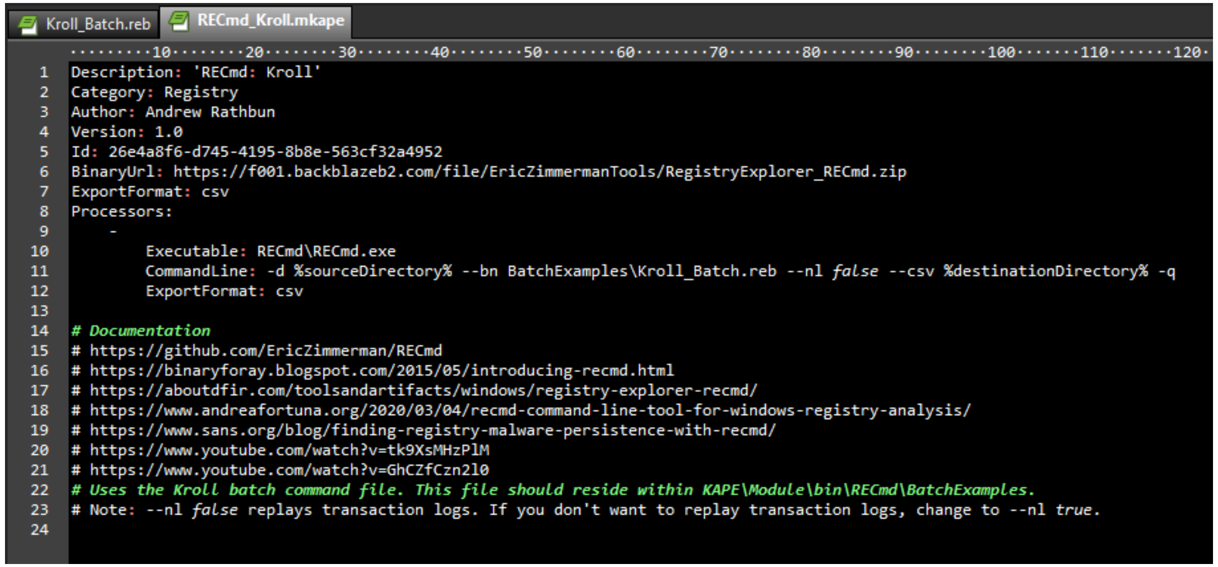
Kroll Batch File

Constantly updated with new artifacts. Overview on next slide

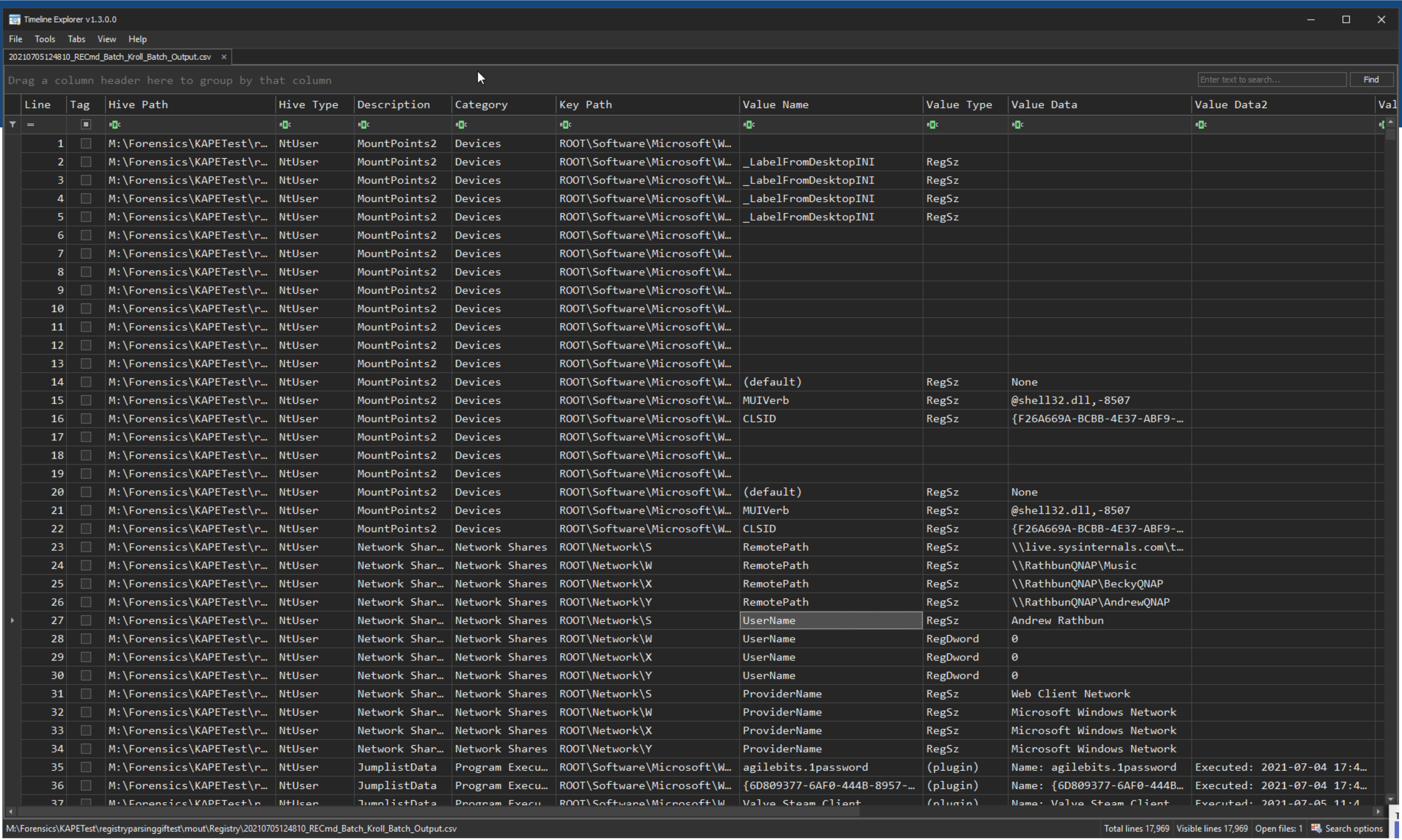
- Kroll Batch File has been optimized with great care to utilize Plugins (more on that next) to minimize rows in CSV while maximizing useful output
- Running RECmd Module in KAPE will default to Kroll Batch file (below)
- Example of RECmd parsing hives, replaying transaction logs, and pulling contents from hives per direction of Kroll Batch file (right)



```
PS V:\DFIR Tools\KAPE\Modules\bin\RECmd> .\recmd.exe -d M:\Forensics\KAPE
Test\registryparsinggiftest\tout --bn BatchExamples\Kroll_Batch.reb --nl
false --csv M:\Forensics\KAPETest\registryparsinggiftest\mout\Registry -q
```



```
Description: 'RECmd: Kroll'
Category: Registry
Author: Andrew Rathbun
Version: 1.0
Id: 26e4a8f6-d745-4195-8b8e-563cf32a4952
BinaryUrl: https://f001.backblazeb2.com/file/EricZimmermanTools/RegistryExplorer_RECmd.zip
ExportFormat: csv
Processors:
    -
        Executable: RECmd\RECmd.exe
        CommandLine: -d %sourceDirectory% --bn BatchExamples\Kroll_Batch.reb --nl false --csv %destinationDirectory% -q
        ExportFormat: csv

# Documentation
# https://github.com/EricZimmerman/RECmd
# https://binaryforay.blogspot.com/2015/05/introducing-recmd.html
# https://aboutdfir.com/toolsandartifacts/windows/registry-explorer-recmd/
# https://www.andreafortuna.org/2020/03/04/recmd-command-line-tool-for-windows-registry-analysis/
# https://www.sans.org/blog/finding-registry-malware-persistence-with-recmd/
# https://www.youtube.com/watch?v=tk9XsMHzPlM
# https://www.youtube.com/watch?v=GhCZfCzn2l0
# Uses the Kroll batch command file. This file should reside within KAPE\Module\bin\RECmd\BatchExamples.
# Note: --nl false replays transaction logs. If you don't want to replay transaction logs, change to --nl true.
```


Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
20210705124810_RECmd_Batch_Kroll_Batch_Output.csv
Drag a column header here to group by that column
Enter text to search...
Find

Line	Tag	Hive Path	Hive Type	Description	Category	Key Path	Value Name	Value Type	Value Data	Value Data2	Val
1	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
2	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	_LabelFromDesktopINI	RegSz			
3	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	_LabelFromDesktopINI	RegSz			
4	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	_LabelFromDesktopINI	RegSz			
5	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	_LabelFromDesktopINI	RegSz			
6	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
7	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
8	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
9	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
10	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
11	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
12	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
13	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
14	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	(default)	RegSz	None		
15	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	MUIVerb	RegSz	@shell32.dll,-8507		
16	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	CLSID	RegSz	{F26A669A-BCBB-4E37-ABF9-…		
17	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
18	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
19	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…					
20	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	(default)	RegSz	None		
21	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	MUIVerb	RegSz	@shell32.dll,-8507		
22	□	M:\Forensics\KAPETest\r…	NtUser	MountPoints2	Devices	ROOT\Software\Microsoft\W…	CLSID	RegSz	{F26A669A-BCBB-4E37-ABF9-…		
23	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\S	RemotePath	RegSz	\\live.sysinternals.com\t…		
24	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\W	RemotePath	RegSz	\\RathbunQNAP\Music		
25	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\X	RemotePath	RegSz	\\RathbunQNAP\BeckyQNAP		
26	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\Y	RemotePath	RegSz	\\RathbunQNAP\AndrewQNAP		
27	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\S	UserName	RegSz	Andrew Rathbun		
28	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\W	UserName	RegDword	0		
29	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\X	UserName	RegDword	0		
30	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\Y	UserName	RegDword	0		
31	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\S	ProviderName	RegSz	Web Client Network		
32	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\W	ProviderName	RegSz	Microsoft Windows Network		
33	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\X	ProviderName	RegSz	Microsoft Windows Network		
34	□	M:\Forensics\KAPETest\r…	NtUser	Network Shar…	Network Shares	ROOT\Network\Y	ProviderName	RegSz	Microsoft Windows Network		
35	□	M:\Forensics\KAPETest\r…	NtUser	JumplistData	Program Execu…	ROOT\Software\Microsoft\W…	agilebits.1password	(plugin)	Name: agilebits.1password	Executed: 2021-07-04 17:4…	
36	□	M:\Forensics\KAPETest\r…	NtUser	JumplistData	Program Execu…	ROOT\Software\Microsoft\W…	{6D809377-6AF0-444B-8957-…	(plugin)	Name: {6D809377-6AF0-444B…	Executed: 2021-07-04 17:4…	
37	□	M:\Forensics\KAPETest\r…	NtUser	JumplistData	Program Execu…	ROOT\Software\Microsoft\W…	Valve Steam Client	(plugin)	Name: Valve Steam Client	Executed: 2021-07-05 11:4…	

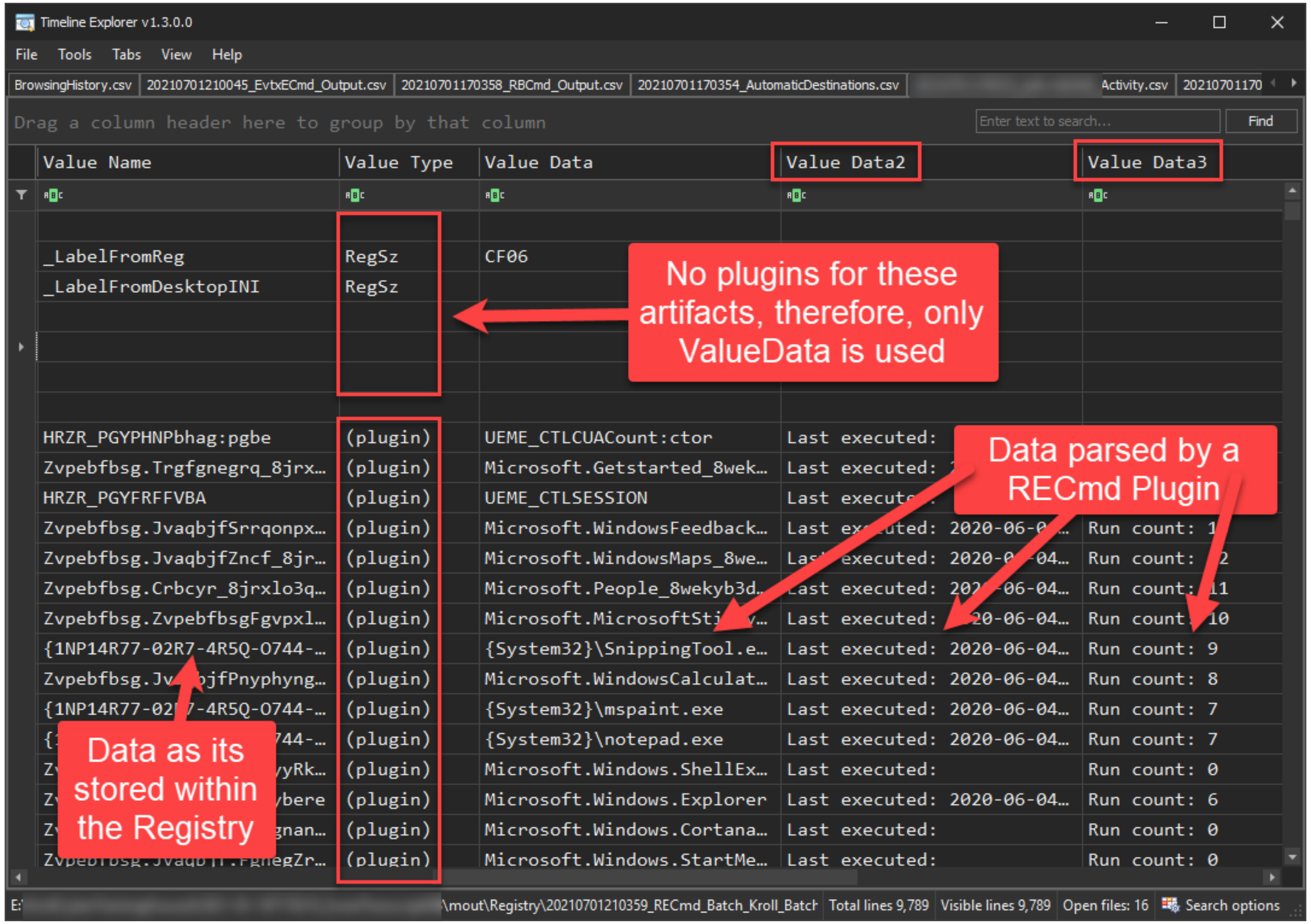
M:\Forensics\KAPETest\registryparsinggiftest\mout\Registry\20210705124810_RECmd_Batch_Kroll_Batch_Output.csv

Total lines 17,969 Visible lines 17,969 Open files: 1 Search options

RECmd Plugins

These require coding knowledge, but they help make CSV output more efficient

- Location:
  - .\RegistryExplorer\Plugins
  - .\KAPE\Modules\bin\RECmd\Plugins
- Requires any .NET language skills to create
- Also used by Registry Explorer (GUI)
- Reduces the number of rows in a CSV by utilizing ValueData2 and ValueData3 columns to store parsed data
- Plugins are helpful because they can solve problems like decoding values stored in ROT13, Windows Filetime, Epoch, etc
  - 132694395618842227 vs 2021-06-29 11:26:01
- Without plugins, we just see (Binary data) or the actual binary data itself (IncludeBinary)
  - IncludeBinary: true = B4-9F-1E-40-FD-4B-D7-01


Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
BrowsingHistory.csv
20210701210045_EvtxECmd_Output.csv
20210701170358_RBCmd_Output.csv
20210701170354_AutomaticDestinations.csv
[redacted]
Activity.csv
20210701170
Drag a column header here to group by that column
Enter text to search...
Find

Value Name	Value Type	Value Data	Value Data2	Value Data3
_LabelFromReg	RegSz	CF06		
_LabelFromDesktopINI	RegSz			
HRZR_PGYPHNPbhag:pgbe	(plugin)	UEME_CTLCUACount:ctor	Last executed:	[illegible]
Zvpebfbsg.Trgfgnegrq_8jrx…	(plugin)	Microsoft.Getstarted_8wek…	Last executed: [illegible]	[illegible]
HRZR_PGYFRFFVBA	(plugin)	UEME_CTLSESSION	Last executed:	[illegible]
Zvpebfbsg.JvaqbjfSrrqonpx…	(plugin)	Microsoft.WindowsFeedback…	Last executed: 2020-06-0…	Run count: 1
Zvpebfbsg.JvaqbjfZncf_8jr…	(plugin)	Microsoft.WindowsMaps_8we…	Last executed: 2020-06-04…	Run count: 2
Zvpebfbsg.Crbcyr_8jrxlo3q…	(plugin)	Microsoft.People_8wekyb3d…	Last executed: 2020-06-04…	Run count: 11
Zvpebfbsg.ZvpebfbsgFgvpxl…	(plugin)	Microsoft.MicrosoftSti[illegible]y…	Last executed: 2020-06-04…	Run count: 10
{1NP14R77-02R7-4R5Q-0744-…	(plugin)	{System32}\SnippingTool.e…	Last executed: 2020-06-04…	Run count: 9
Zvpebfbsg.Jv[illegible]bjfPnyphyng…	(plugin)	Microsoft.WindowsCalculat…	Last executed: 2020-06-04…	Run count: 8
{1NP14R77-02[illegible]7-4R5Q-0744-…	(plugin)	{System32}\mspaint.exe	Last executed: 2020-06-04…	Run count: 7
{1[illegible]744-…	(plugin)	{System32}\notepad.exe	Last executed: 2020-06-04…	Run count: 7
Z[illegible]yRk…	(plugin)	Microsoft.Windows.ShellEx…	Last executed:	Run count: 0
Z[illegible]bere	(plugin)	Microsoft.Windows.Explorer	Last executed: 2020-06-04…	Run count: 6
Z[illegible]gnan…	(plugin)	Microsoft.Windows.Cortana…	Last executed:	Run count: 0
Zvpebfbsg.Jvaqbjf.FgnegZr…	(plugin)	Microsoft.Windows.StartMe…	Last executed:	Run count: 0

E:[redacted]\mout\Registry\20210701210359_RECmd_Batch_Kroll_Batch Total lines 9,789 Visible lines 9,789 Open files: 16 Search options

No plugins for these artifacts, therefore, only ValueData is used

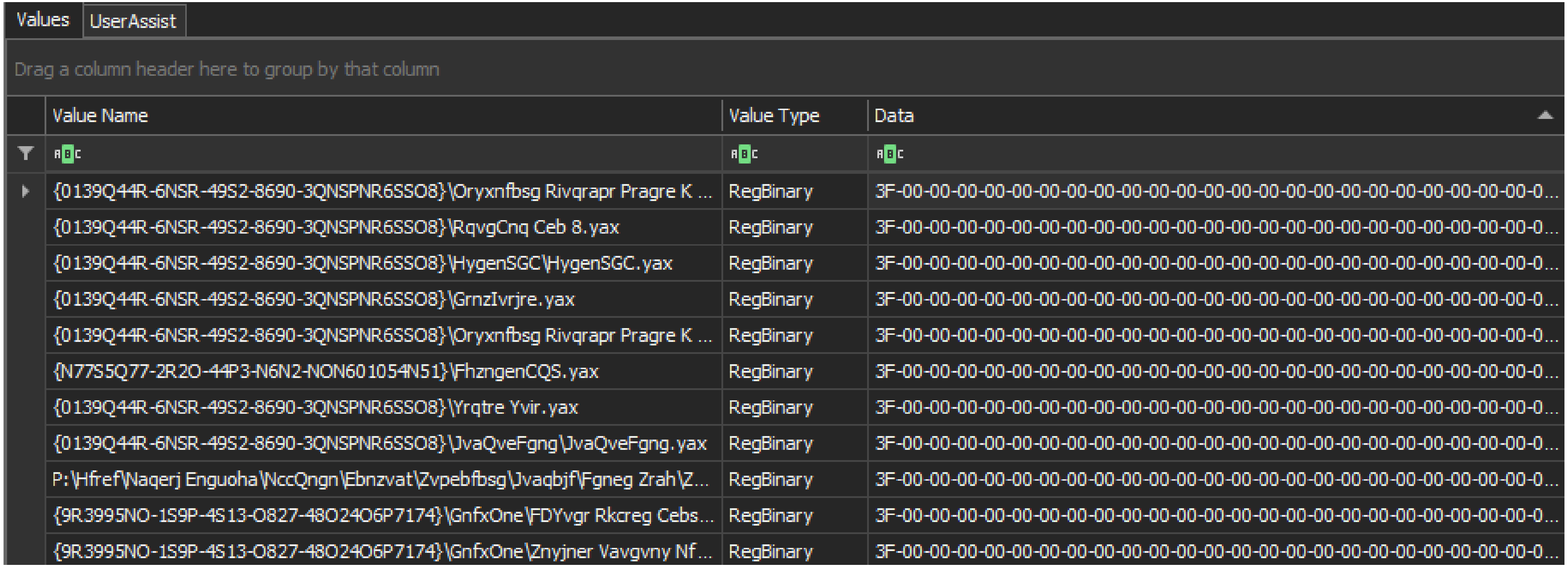
Data parsed by a RECmd Plugin

Data as its stored within the Registry

Registry Explorer Plugins

UserAssist Plugin adds a tab that shows decoded data from NTUser.dat

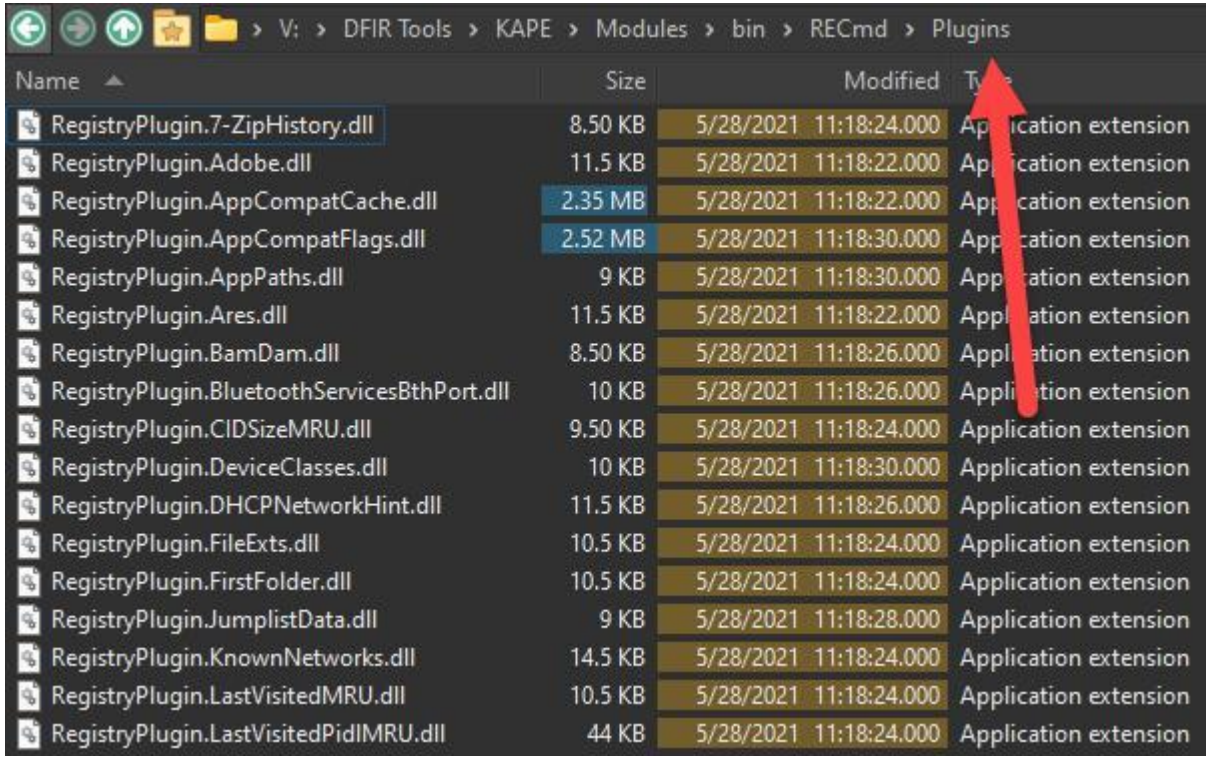
- Values – values stored natively within the Windows Registry
- UserAssist – values decoded by Registry Explorer/RECmd's UserAssist Plugin



Value Name	Value Type	Data
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Oryxnfbsg Rivqrapr Pragre K ...	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\RqvgCnq Ceb 8.yax	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\HygenSGC\HygenSGC.yax	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\GrnzIvrjre.yax	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Oryxnfbsg Rivqrapr Pragre K ...	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{N77S5Q77-2R2O-44P3-N6N2-NON601054N51}\FhzngenCQS.yax	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\Yrqtre Yvir.yax	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{0139Q44R-6NSR-49S2-8690-3QNSPNR6SSO8}\JvaQveFgng\JvaQveFgng.yax	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
P:\Hfref\Naqerj Enguoha\NccQngn\Ebnzvat\Zvpebfbsg\Jvaqbjf\Fgneg Zrah\Z...	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{9R3995NO-1S9P-4S13-O827-48O24O6P7174}\GnfxOne\FDYvgr Rkcreg Cebs...	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...
{9R3995NO-1S9P-4S13-O827-48O24O6P7174}\GnfxOne\Znyjner Vavgvny Nf...	RegBinary	3F-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-0...

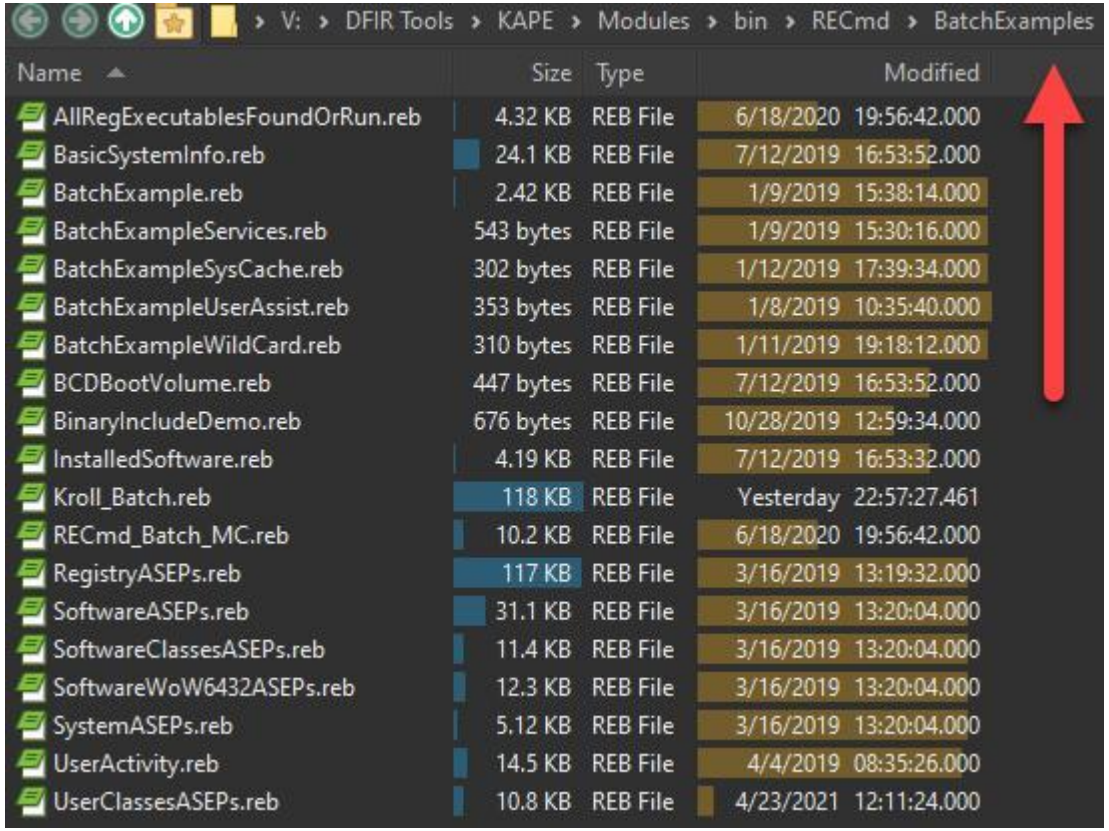
Locations of RECmd Batch Files and Plugins

Check Github for the source code of RECmd Plugins (.dll files)



V: › DFIR Tools › KAPE › Modules › bin › RECmd › Plugins

Name	Size	Modified	Type
RegistryPlugin.7-ZipHistory.dll	8.50 KB	5/28/2021 11:18:24.000	Application extension
RegistryPlugin.Adobe.dll	11.5 KB	5/28/2021 11:18:22.000	Application extension
RegistryPlugin.AppCompatCache.dll	2.35 MB	5/28/2021 11:18:22.000	Application extension
RegistryPlugin.AppCompatFlags.dll	2.52 MB	5/28/2021 11:18:30.000	Application extension
RegistryPlugin.AppPaths.dll	9 KB	5/28/2021 11:18:30.000	Application extension
RegistryPlugin.Ares.dll	11.5 KB	5/28/2021 11:18:22.000	Application extension
RegistryPlugin.BamDam.dll	8.50 KB	5/28/2021 11:18:26.000	Application extension
RegistryPlugin.BluetoothServicesBthPort.dll	10 KB	5/28/2021 11:18:26.000	Application extension
RegistryPlugin.CIDSizeMRU.dll	9.50 KB	5/28/2021 11:18:24.000	Application extension
RegistryPlugin.DeviceClasses.dll	10 KB	5/28/2021 11:18:30.000	Application extension
RegistryPlugin.DHCPNetworkHint.dll	11.5 KB	5/28/2021 11:18:26.000	Application extension
RegistryPlugin.FileExts.dll	10.5 KB	5/28/2021 11:18:24.000	Application extension
RegistryPlugin.FirstFolder.dll	10.5 KB	5/28/2021 11:18:24.000	Application extension
RegistryPlugin.JumplistData.dll	9 KB	5/28/2021 11:18:28.000	Application extension
RegistryPlugin.KnownNetworks.dll	14.5 KB	5/28/2021 11:18:24.000	Application extension
RegistryPlugin.LastVisitedMRU.dll	10.5 KB	5/28/2021 11:18:24.000	Application extension
RegistryPlugin.LastVisitedPidlMRU.dll	44 KB	5/28/2021 11:18:24.000	Application extension



V: › DFIR Tools › KAPE › Modules › bin › RECmd › BatchExamples

Name	Size	Type	Modified
AllRegExecutablesFoundOrRun.reb	4.32 KB	REB File	6/18/2020 19:56:42.000
BasicSystemInfo.reb	24.1 KB	REB File	7/12/2019 16:53:52.000
BatchExample.reb	2.42 KB	REB File	1/9/2019 15:38:14.000
BatchExampleServices.reb	543 bytes	REB File	1/9/2019 15:30:16.000
BatchExampleSysCache.reb	302 bytes	REB File	1/12/2019 17:39:34.000
BatchExampleUserAssist.reb	353 bytes	REB File	1/8/2019 10:35:40.000
BatchExampleWildCard.reb	310 bytes	REB File	1/11/2019 19:18:12.000
BCDBootVolume.reb	447 bytes	REB File	7/12/2019 16:53:52.000
BinaryIncludeDemo.reb	676 bytes	REB File	10/28/2019 12:59:34.000
InstalledSoftware.reb	4.19 KB	REB File	7/12/2019 16:53:32.000
Kroll_Batch.reb	118 KB	REB File	Yesterday 22:57:27.461
RECmd_Batch_MC.reb	10.2 KB	REB File	6/18/2020 19:56:42.000
RegistryASEPs.reb	117 KB	REB File	3/16/2019 13:19:32.000
SoftwareASEPs.reb	31.1 KB	REB File	3/16/2019 13:20:04.000
SoftwareClassesASEPs.reb	11.4 KB	REB File	3/16/2019 13:20:04.000
SoftwareWoW6432ASEPs.reb	12.3 KB	REB File	3/16/2019 13:20:04.000
SystemASEPs.reb	5.12 KB	REB File	3/16/2019 13:20:04.000
UserActivity.reb	14.5 KB	REB File	4/4/2019 08:35:26.000
UserClassesASEPs.reb	10.8 KB	REB File	4/23/2021 12:11:24.000

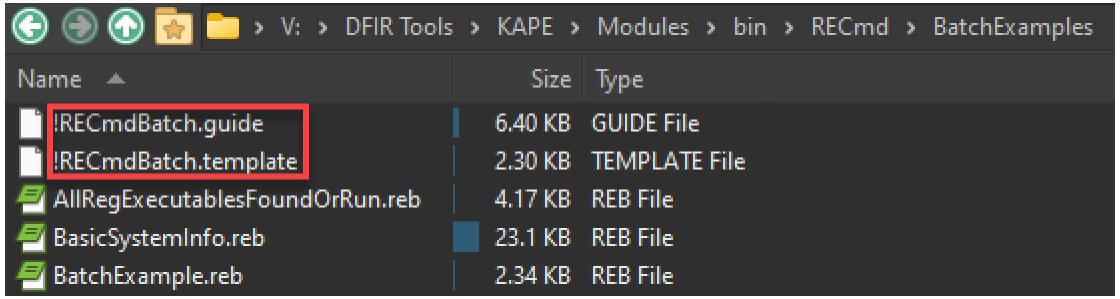
Helpful Tips for Researching the Windows Registry

Quick wins for Registry research

- Tools of the Trade
  - Free: **Registry Explorer**, **RECmd**, **NirSoft's RegistryChangesView**, **ProcMon**, RegEdit, BleachBit (open-source CCleaner alternative - Winapp2.ini and Winapp3.ini)
  - Paid: No reason to pay for a Registry viewer tool, not many exist anyways ☺
- Tips for locating new Keys and Values of interest
  - Investigate yourself on your own computer
    - Open Registry Explorer as Admin and load all live hives. Ctrl+F (Find) for your name, email, apps you use every day, mapped network drives, and anything else you'd want to know about yourself if you were investigating you!
    - Alternatively, dump your hives to JSON using KapeResearch_Registry.mkape
  - Compare Registry snapshots when using or installing software
    - Take Registry snapshots with RegistryChangesView, then install new software or use currently installed software to see what changes are made to the Registry
    - Alternatively, use ProcMon to monitor all Registry actions taken by a program
  - Create VMs and install or execute software/malware used by threat actors
    - Using the tools above, find what is changed where within the Registry without compromising your own personal computer
  - Registry Explorer bookmarks provide useful pointers to forensically interesting locations within the Registry

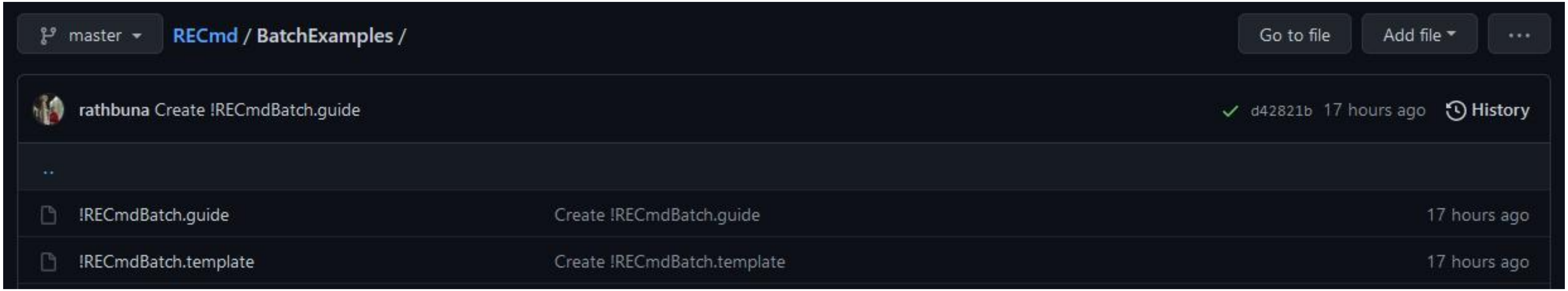
Other RECmd Resources

.\KAPE\Modules\bin\RECmd\BatchExamples or RECmd Batch Guide/Template on GitHub



V: › DFIR Tools › KAPE › Modules › bin › RECmd › BatchExamples

Name	Size	Type
!RECmdBatch.guide	6.40 KB	GUIDE File
!RECmdBatch.template	2.30 KB	TEMPLATE File
AllRegExecutablesFoundOrRun.reb	4.17 KB	REB File
BasicSystemInfo.reb	23.1 KB	REB File
BatchExample.reb	2.34 KB	REB File



RECmd / BatchExamples /

rathbuna Create !RECmdBatch.guide ✓ d42821b 17 hours ago

..

!RECmdBatch.guide	Create !RECmdBatch.guide	17 hours ago
!RECmdBatch.template	Create !RECmdBatch.template	17 hours ago

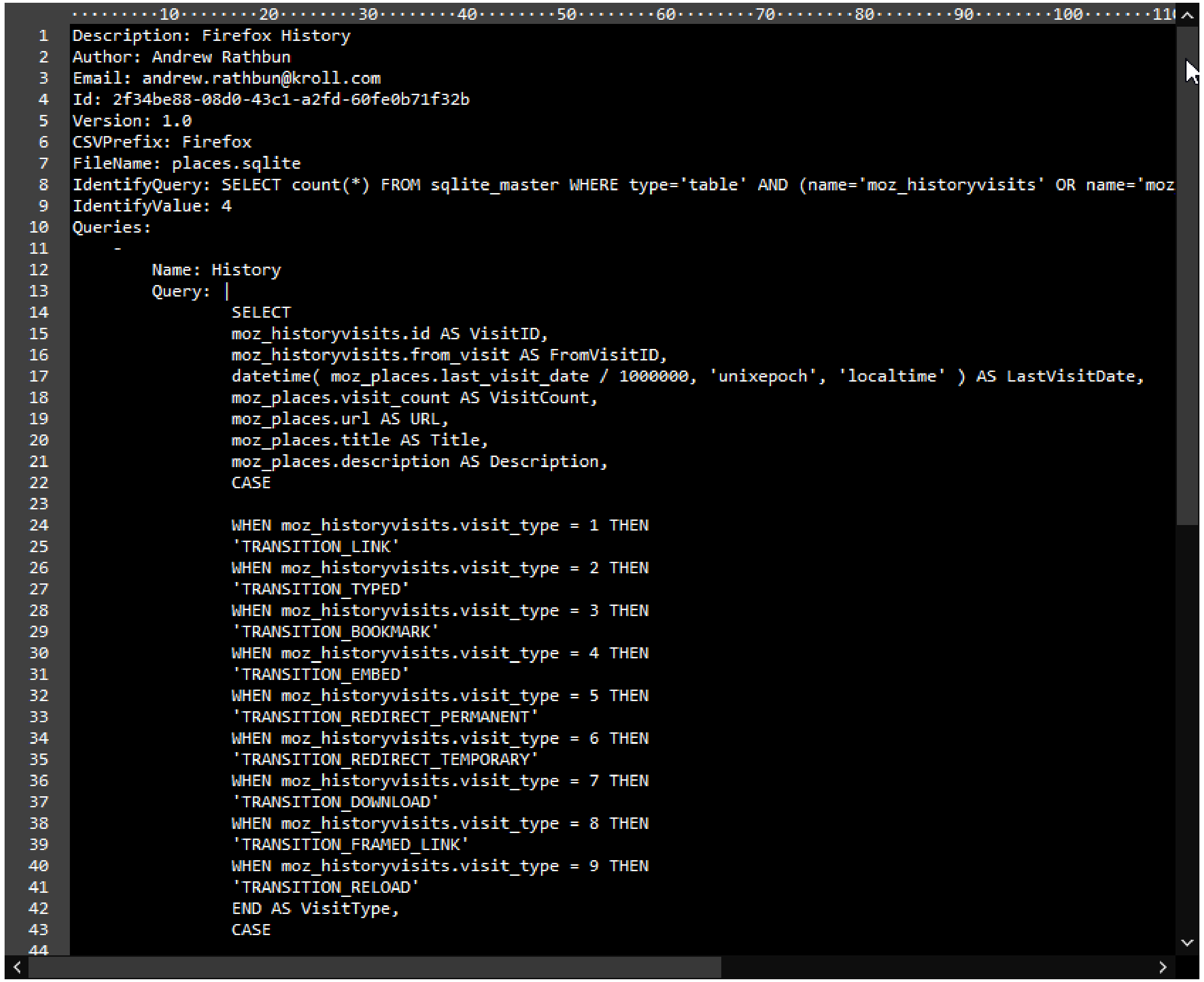
SQLECmd

Maps

SQLECmd Maps

What are they and why do I care?

- Maps are used by SQLECmd to extract data from SQLite databases using SQL queries and output the data to CSV
- Text files (.smap) in YAML using SQLite queries
- 67 Maps as of 6/25/2021
- TONS of currently untapped potential as it can be used to parse data from nearly any OS
  - Any .db*, .sqlite*, or even files that don’t have file extensions can be SQLite databases
    - Run SQLECmd.exe --hunt over C:\ to see how many there are! Or, run it over a folder with databases from a mobile extraction
- Ideally, one SQLECmd Map per database filename (i.e., Places.sqlite), but multiple SQL queries can exist within a single SQLECmd Map for when multiple datasets can be parsed from a given SQLite database

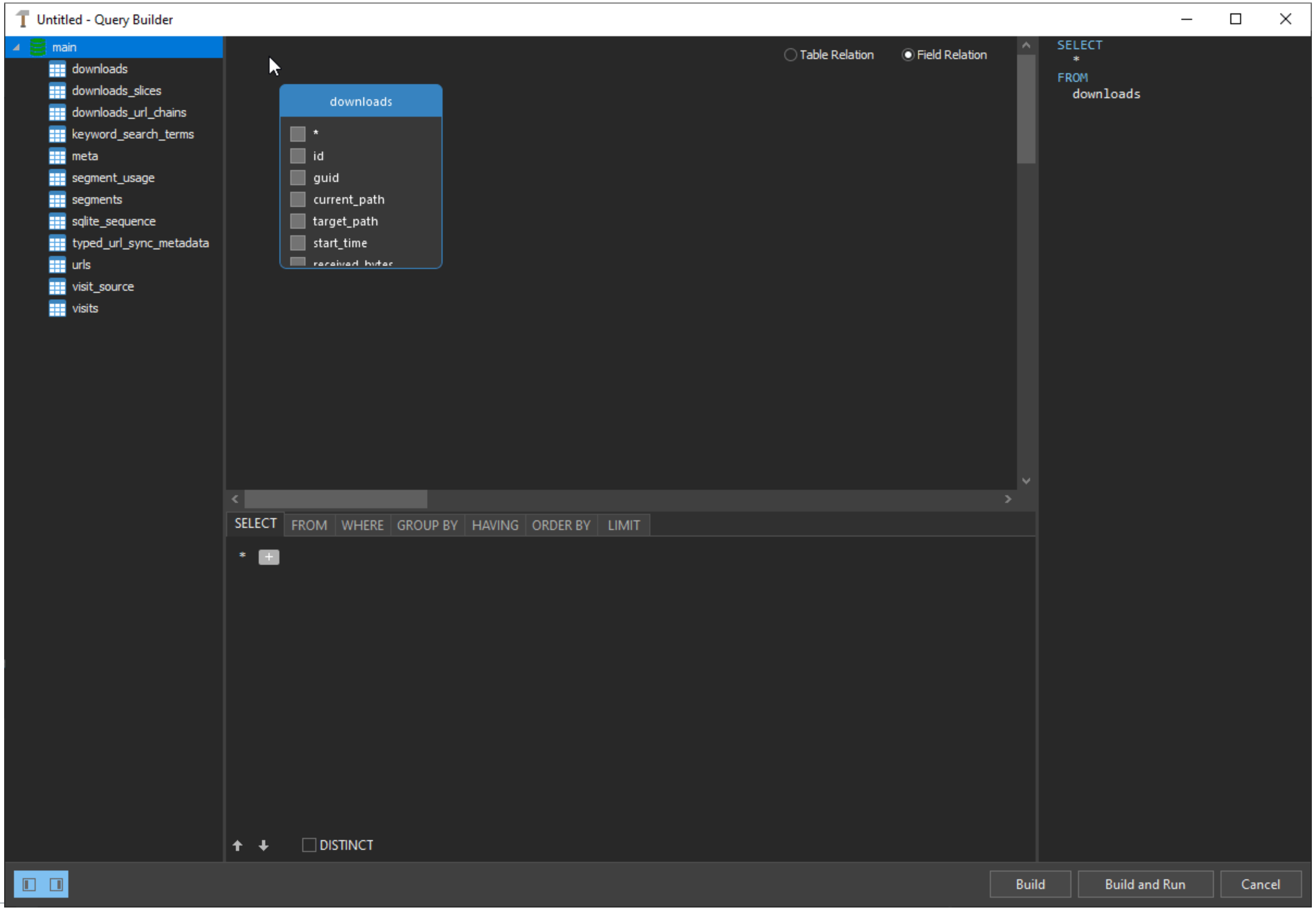


```
Description: Firefox History
Author: Andrew Rathbun
Email: andrew.rathbun@kroll.com
Id: 2f34be88-08d0-43c1-a2fd-60fe0b71f32b
Version: 1.0
CSVPrefix: Firefox
FileName: places.sqlite
IdentifyQuery: SELECT count(*) FROM sqlite_master WHERE type='table' AND (name='moz_historyvisits' OR name='moz
IdentifyValue: 4
Queries:
    -
        Name: History
        Query: |
                SELECT
                moz_historyvisits.id AS VisitID,
                moz_historyvisits.from_visit AS FromVisitID,
                datetime( moz_places.last_visit_date / 1000000, 'unixepoch', 'localtime' ) AS LastVisitDate,
                moz_places.visit_count AS VisitCount,
                moz_places.url AS URL,
                moz_places.title AS Title,
                moz_places.description AS Description,
                CASE

                WHEN moz_historyvisits.visit_type = 1 THEN
                'TRANSITION_LINK'
                WHEN moz_historyvisits.visit_type = 2 THEN
                'TRANSITION_TYPED'
                WHEN moz_historyvisits.visit_type = 3 THEN
                'TRANSITION_BOOKMARK'
                WHEN moz_historyvisits.visit_type = 4 THEN
                'TRANSITION_EMBED'
                WHEN moz_historyvisits.visit_type = 5 THEN
                'TRANSITION_REDIRECT_PERMANENT'
                WHEN moz_historyvisits.visit_type = 6 THEN
                'TRANSITION_REDIRECT_TEMPORARY'
                WHEN moz_historyvisits.visit_type = 7 THEN
                'TRANSITION_DOWNLOAD'
                WHEN moz_historyvisits.visit_type = 8 THEN
                'TRANSITION_FRAMED_LINK'
                WHEN moz_historyvisits.visit_type = 9 THEN
                'TRANSITION_RELOAD'
                END AS VisitType,
                CASE
```

Building SQL Queries

No experience necessary, just patience!

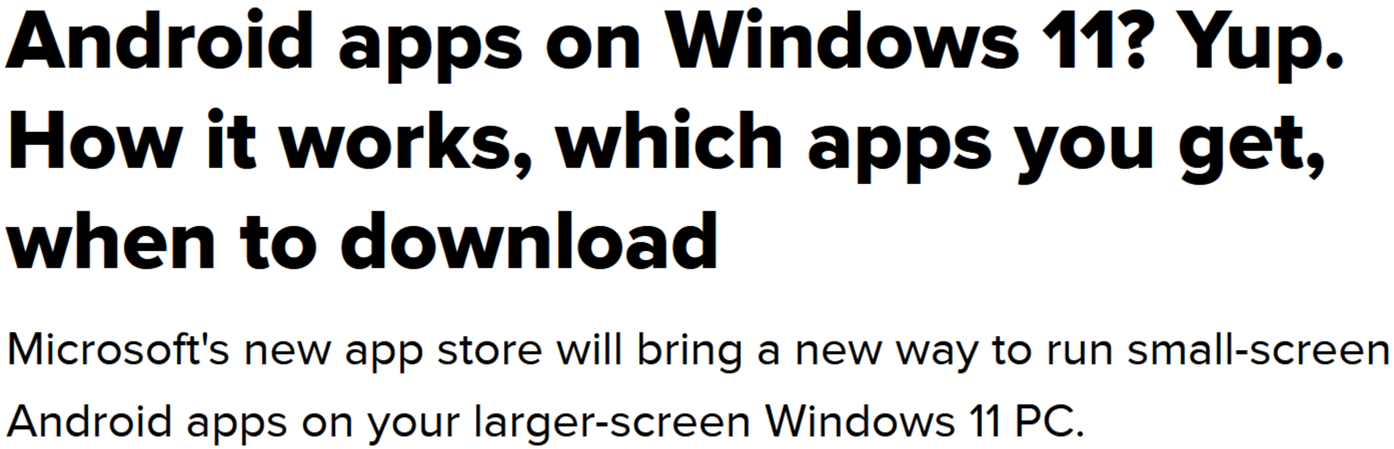
- Trust but verify your forensic tools and parse SQLite databases yourself
- When using a tool with a robust SQLite Query builder, it won’t take long to pick up on what drives the output from your query
- Build your query, run it, observe, adjust as necessary, rerun, and once perfected, share!
- Tools of the Trade (SQLite):
  - Free: DB Browser for SQLite
  - Paid: **Navicat for SQLite**, SQLite Expert Professional, Sanderson Forensic Toolkit
- Note: DB Browser for SQLite requires manual SQLite Query building
- Tools of the Trade (Monitoring)
  - Free: **Everything**, **ProcMon**
  - Paid: **Directory Monitor Pro**



```
SELECT
  *
FROM
  downloads
```

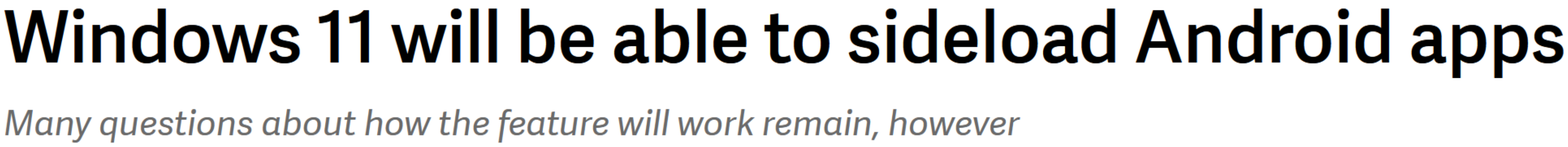
Have You Heard the News?

Android Apps on Windows 11 – Announced June 24, 2021 during Windows 11 reveal



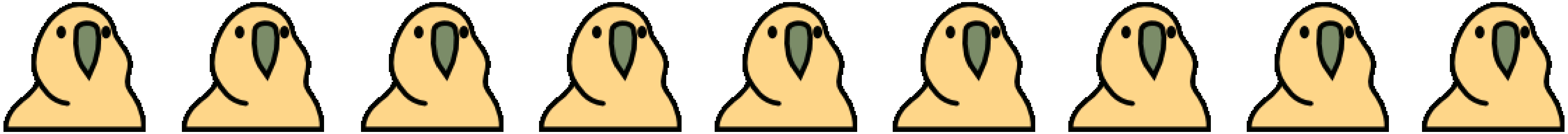
Android apps on Windows 11? Yup. How it works, which apps you get, when to download

Microsoft's new app store will bring a new way to run small-screen Android apps on your larger-screen Windows 11 PC.



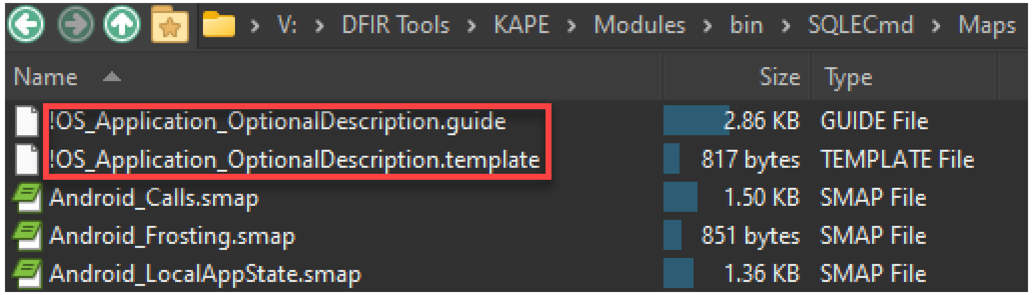
Windows 11 will be able to sideload Android apps

Many questions about how the feature will work remain, however

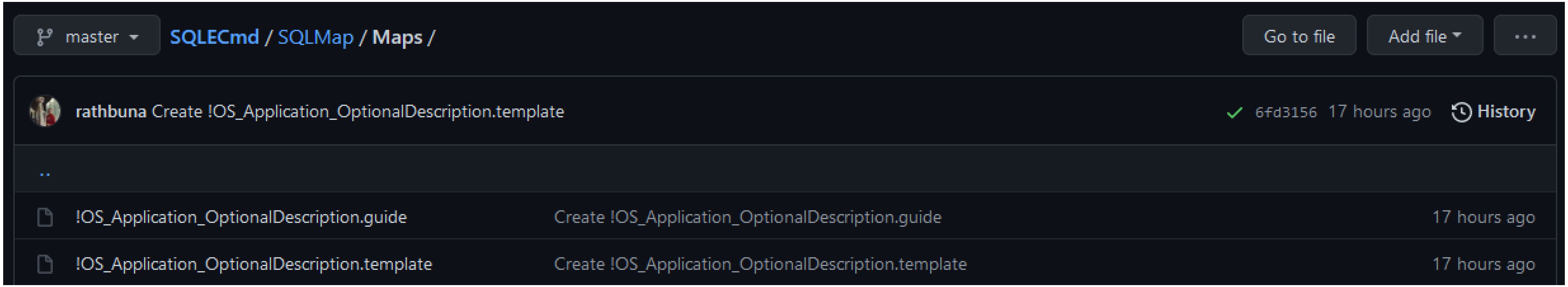


Other SQLECmd Resources

.\KAPE\Modules\bin\SQLECmd\Maps or SQLECmd Maps Guide/Template on GitHub



Name	Size	Type
!OS_Application_OptionalDescription.guide	2.86 KB	GUIDE File
!OS_Application_OptionalDescription.template	817 bytes	TEMPLATE File
Android_Calls.smap	1.50 KB	SMAP File
Android_Frosting.smap	851 bytes	SMAP File
Android_LocalAppState.smap	1.36 KB	SMAP File



rathbuna Create !OS_Application_OptionalDescription.template ✓ 6fd3156 17 hours ago

..

!OS_Application_OptionalDescription.guide	Create !OS_Application_OptionalDescription.guide	17 hours ago
!OS_Application_OptionalDescription.template	Create !OS_Application_OptionalDescription.template	17 hours ago

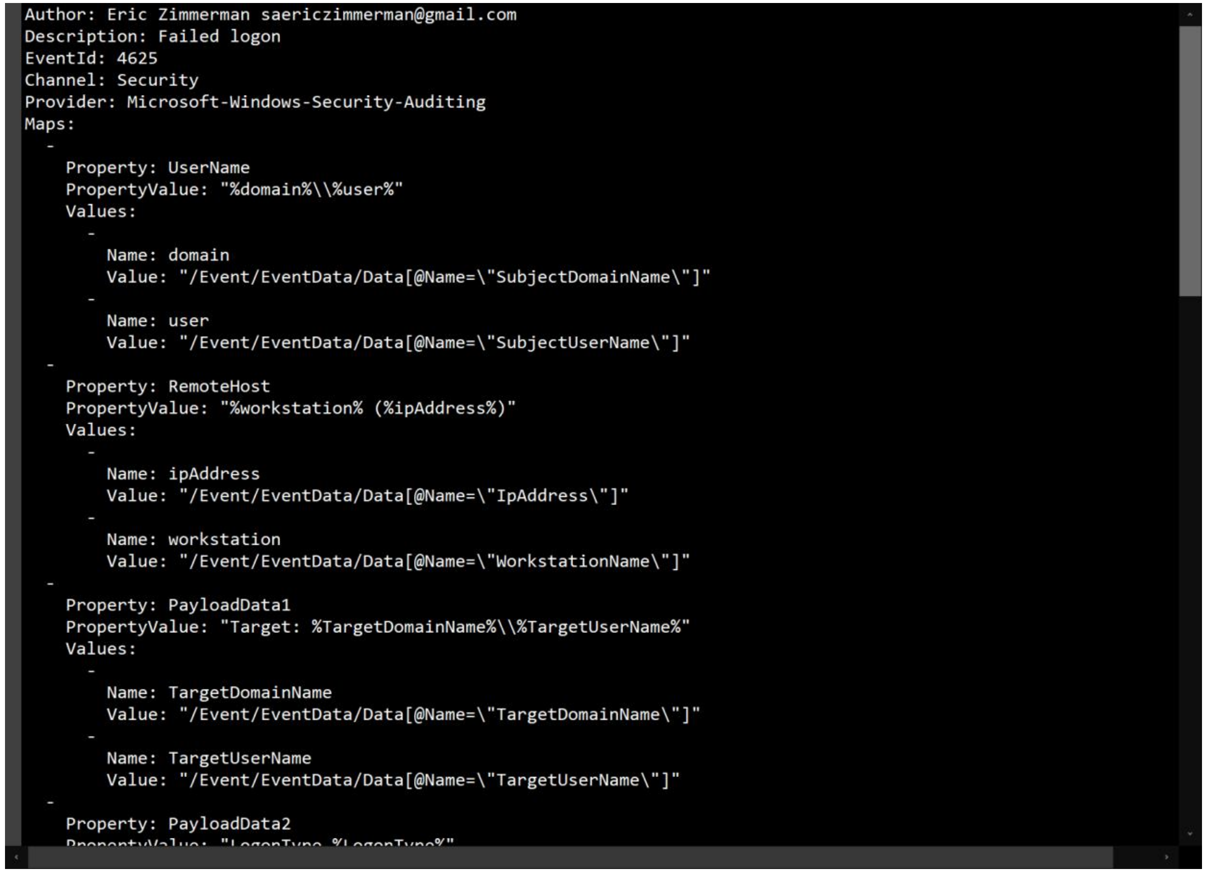
EvtxECmd

Maps

EvtxECmd Maps

What are they and why do I care?

- Maps are used by EvtxECmd to extract data from parsed event logs and display the data into an easily digestible format within various columns unique to EvtxECmd, similar to RECmd
    - Map Description, UserName, RemoteHost PayloadData1-6, and ExecutableInfo
- Text files (.map) in YAML using XPath queries
- 352 Maps as of 6/25/2021
- Ideally, the most useful events would be mapped, not EVERY event in existence
- Really cool features like Lookups and Regex
- All data stored within an event log will reside within the Payload column of the CSV output. Maps simply separate out the most important data points from each Event Log's XML Payload

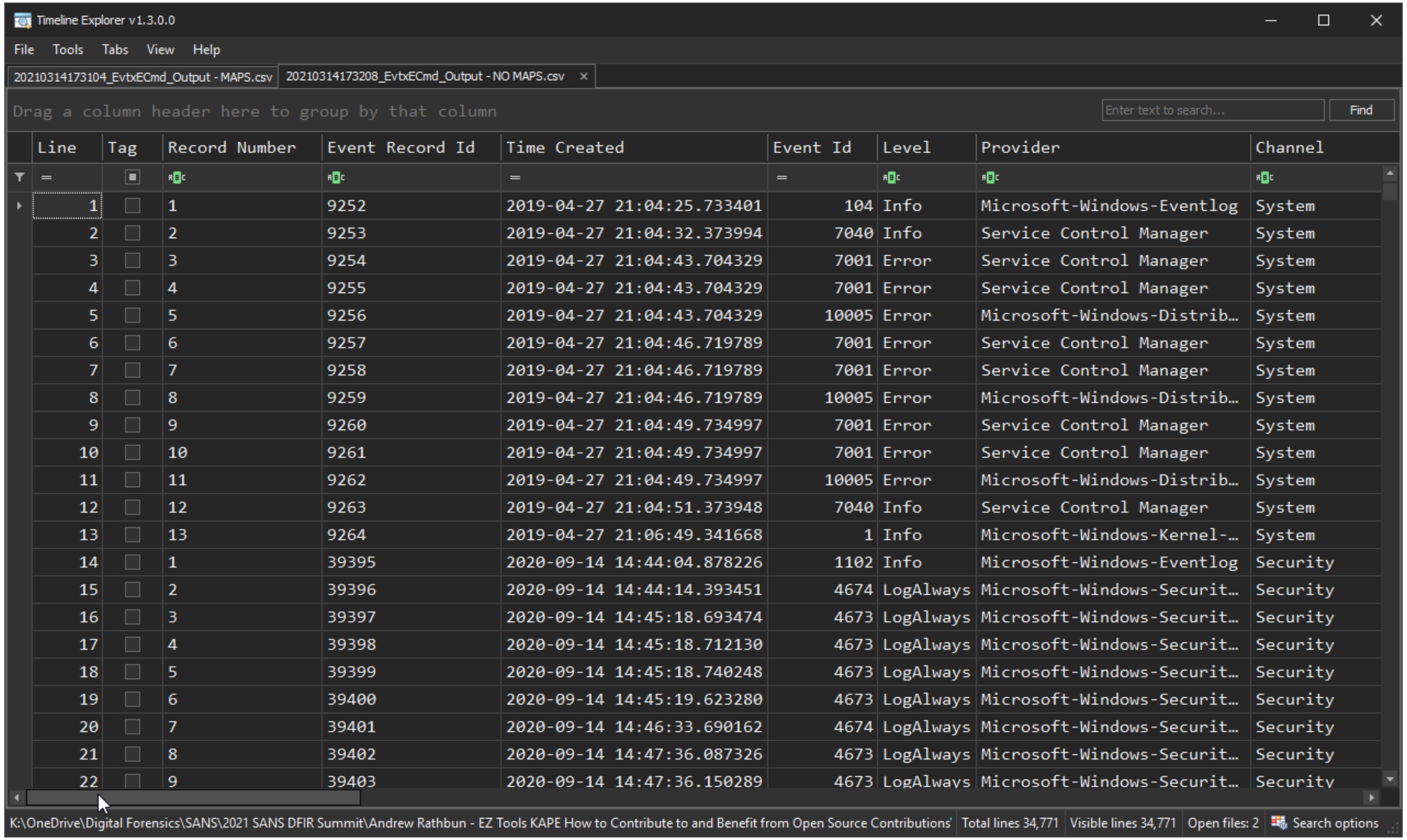


```
Author: Eric Zimmerman saericzimmerman@gmail.com
Description: Failed logon
EventId: 4625
Channel: Security
Provider: Microsoft-Windows-Security-Auditing
Maps:
  -
    Property: UserName
    PropertyValue: "%domain%\\%user%"
    Values:
      -
        Name: domain
        Value: "/Event/EventData/Data[@Name=\"SubjectDomainName\"]"
      -
        Name: user
        Value: "/Event/EventData/Data[@Name=\"SubjectUserName\"]"
  -
    Property: RemoteHost
    PropertyValue: "%workstation% (%ipAddress%)"
    Values:
      -
        Name: ipAddress
        Value: "/Event/EventData/Data[@Name=\"IpAddress\"]"
      -
        Name: workstation
        Value: "/Event/EventData/Data[@Name=\"WorkstationName\"]"
  -
    Property: PayloadData1
    PropertyValue: "Target: %TargetDomainName%\\%TargetUserName%"
    Values:
      -
        Name: TargetDomainName
        Value: "/Event/EventData/Data[@Name=\"TargetDomainName\"]"
      -
        Name: TargetUserName
        Value: "/Event/EventData/Data[@Name=\"TargetUserName\"]"
  -
    Property: PayloadData2
    PropertyValue: "LogonType %LogonType%"
```

EvtxECmd CSV Output in Timeline Explorer

Windows Event Logs parsed without any Maps (deleted .\EvtxECmd\Maps folder prior to parsing)

- Notice how there's no data populated within any of the following columns:
  - Map Description, UserName, RemoteHost PayloadData1-6, and ExecutableInfo
- Again, all data still exists within Payload column to the far right, but it's all a massive blob, and frankly, not all of it is relevant to the everyday DFIR examiner
- 29.9mb CSV ->



Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
20210314173104_EvtxECmd_Output - MAPS.csv
20210314173208_EvtxECmd_Output - NO MAPS.csv
Drag a column header here to group by that column
Enter text to search...
Find
Search options

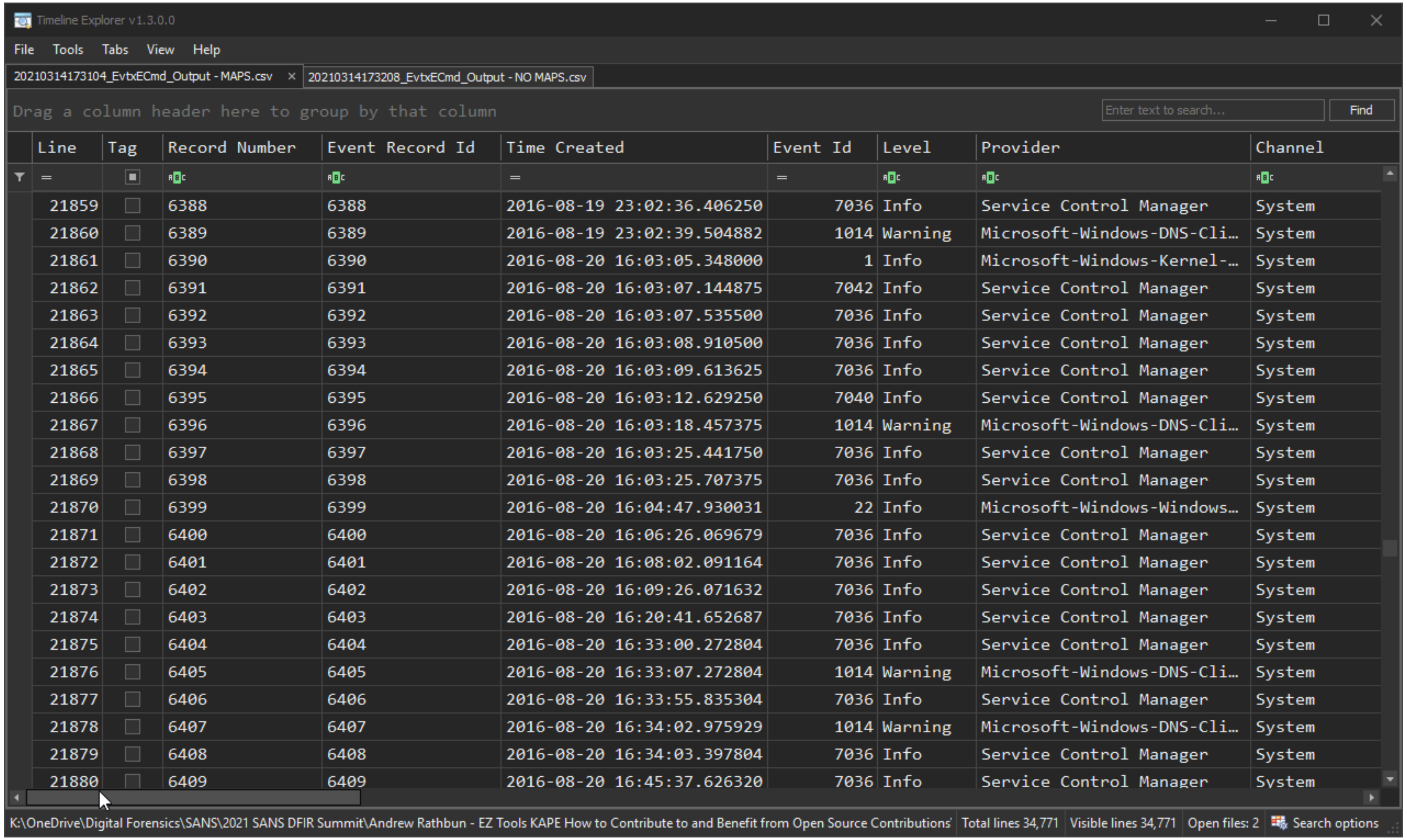
Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel
1	☐	1	9252	2019-04-27 21:04:25.733401	104	Info	Microsoft-Windows-Eventlog	System
2	☐	2	9253	2019-04-27 21:04:32.373994	7040	Info	Service Control Manager	System
3	☐	3	9254	2019-04-27 21:04:43.704329	7001	Error	Service Control Manager	System
4	☐	4	9255	2019-04-27 21:04:43.704329	7001	Error	Service Control Manager	System
5	☐	5	9256	2019-04-27 21:04:43.704329	10005	Error	Microsoft-Windows-Distrib...	System
6	☐	6	9257	2019-04-27 21:04:46.719789	7001	Error	Service Control Manager	System
7	☐	7	9258	2019-04-27 21:04:46.719789	7001	Error	Service Control Manager	System
8	☐	8	9259	2019-04-27 21:04:46.719789	10005	Error	Microsoft-Windows-Distrib...	System
9	☐	9	9260	2019-04-27 21:04:49.734997	7001	Error	Service Control Manager	System
10	☐	10	9261	2019-04-27 21:04:49.734997	7001	Error	Service Control Manager	System
11	☐	11	9262	2019-04-27 21:04:49.734997	10005	Error	Microsoft-Windows-Distrib...	System
12	☐	12	9263	2019-04-27 21:04:51.373948	7040	Info	Service Control Manager	System
13	☐	13	9264	2019-04-27 21:06:49.341668	1	Info	Microsoft-Windows-Kernel-...	System
14	☐	1	39395	2020-09-14 14:44:04.878226	1102	Info	Microsoft-Windows-Eventlog	Security
15	☐	2	39396	2020-09-14 14:44:14.393451	4674	LogAlways	Microsoft-Windows-Securit...	Security
16	☐	3	39397	2020-09-14 14:45:18.693474	4673	LogAlways	Microsoft-Windows-Securit...	Security
17	☐	4	39398	2020-09-14 14:45:18.712130	4673	LogAlways	Microsoft-Windows-Securit...	Security
18	☐	5	39399	2020-09-14 14:45:18.740248	4673	LogAlways	Microsoft-Windows-Securit...	Security
19	☐	6	39400	2020-09-14 14:45:19.623280	4673	LogAlways	Microsoft-Windows-Securit...	Security
20	☐	7	39401	2020-09-14 14:46:33.690162	4674	LogAlways	Microsoft-Windows-Securit...	Security
21	☐	8	39402	2020-09-14 14:47:36.087326	4673	LogAlways	Microsoft-Windows-Securit...	Security
22	☐	9	39403	2020-09-14 14:47:36.150289	4673	LogAlways	Microsoft-Windows-Securit...	Security

K:\OneDrive\Digital Forensics\SANS\2021 SANS DFIR Summit\Andrew Rathbun - EZ Tools KAPE How to Contribute to and Benefit from Open Source Contributions | Total lines 34,771 | Visible lines 34,771 | Open files: 2

EvtxECmd CSV Output in Timeline Explorer

Windows Event Logs parsed with all EvtxECmd Maps as of 6/25/2021

- Notice how there's data populated within the columns not populated in the previous slide
  - Maps make this happen!
- The author of each Map decides which data point(s) reside where within the CSV output
- Ideally, the most interesting data points from each Event Log's XML Payload is displayed within these columns
- Map Description removes the need to memorize which Event IDs mean what, as well as correlating different events with the same description (i.e., account logon, task started, etc)
- 36.5mb CSV ->
  - Only 6mb bigger!



Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
20210314173104_EvtxECmd_Output - MAPS.csv
20210314173208_EvtxECmd_Output - NO MAPS.csv
Drag a column header here to group by that column
Enter text to search...
Find

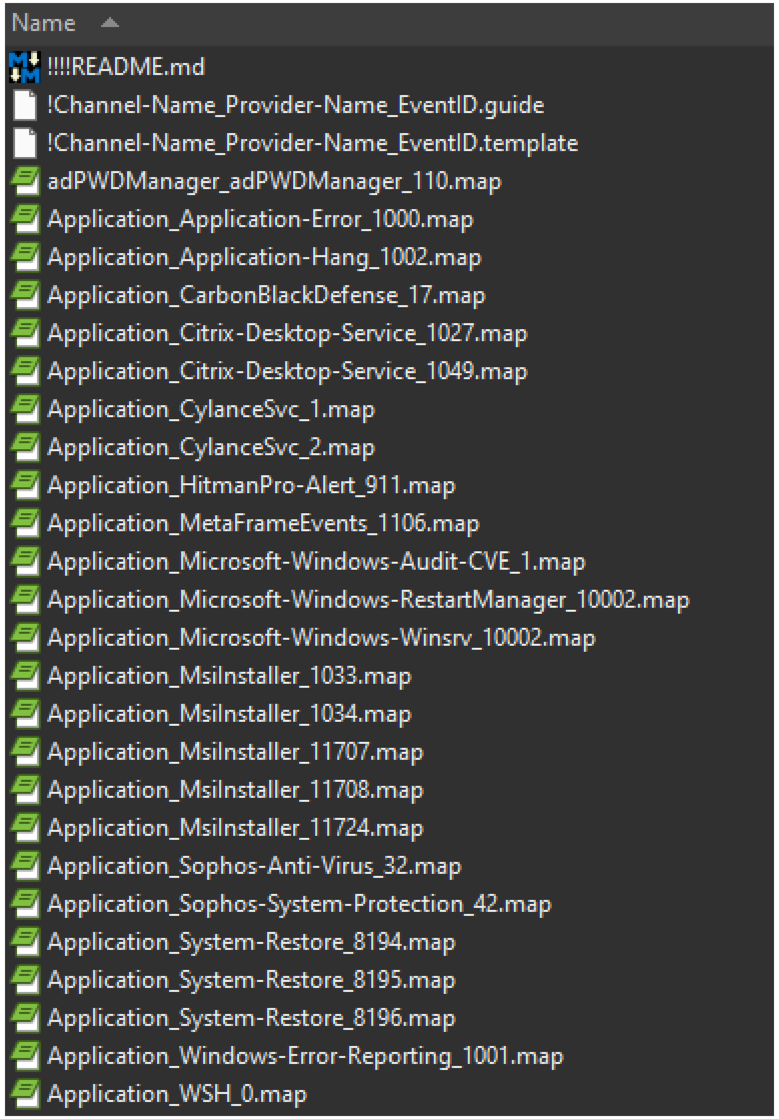
Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel
21859	□	6388	6388	2016-08-19 23:02:36.406250	7036	Info	Service Control Manager	System
21860	□	6389	6389	2016-08-19 23:02:39.504882	1014	Warning	Microsoft-Windows-DNS-Cli...	System
21861	□	6390	6390	2016-08-20 16:03:05.348000	1	Info	Microsoft-Windows-Kernel-...	System
21862	□	6391	6391	2016-08-20 16:03:07.144875	7042	Info	Service Control Manager	System
21863	□	6392	6392	2016-08-20 16:03:07.535500	7036	Info	Service Control Manager	System
21864	□	6393	6393	2016-08-20 16:03:08.910500	7036	Info	Service Control Manager	System
21865	□	6394	6394	2016-08-20 16:03:09.613625	7036	Info	Service Control Manager	System
21866	□	6395	6395	2016-08-20 16:03:12.629250	7040	Info	Service Control Manager	System
21867	□	6396	6396	2016-08-20 16:03:18.457375	1014	Warning	Microsoft-Windows-DNS-Cli...	System
21868	□	6397	6397	2016-08-20 16:03:25.441750	7036	Info	Service Control Manager	System
21869	□	6398	6398	2016-08-20 16:03:25.707375	7036	Info	Service Control Manager	System
21870	□	6399	6399	2016-08-20 16:04:47.930031	22	Info	Microsoft-Windows-Windows...	System
21871	□	6400	6400	2016-08-20 16:06:26.069679	7036	Info	Service Control Manager	System
21872	□	6401	6401	2016-08-20 16:08:02.091164	7036	Info	Service Control Manager	System
21873	□	6402	6402	2016-08-20 16:09:26.071632	7036	Info	Service Control Manager	System
21874	□	6403	6403	2016-08-20 16:20:41.652687	7036	Info	Service Control Manager	System
21875	□	6404	6404	2016-08-20 16:33:00.272804	7036	Info	Service Control Manager	System
21876	□	6405	6405	2016-08-20 16:33:07.272804	1014	Warning	Microsoft-Windows-DNS-Cli...	System
21877	□	6406	6406	2016-08-20 16:33:55.835304	7036	Info	Service Control Manager	System
21878	□	6407	6407	2016-08-20 16:34:02.975929	1014	Warning	Microsoft-Windows-DNS-Cli...	System
21879	□	6408	6408	2016-08-20 16:34:03.397804	7036	Info	Service Control Manager	System
21880	□	6409	6409	2016-08-20 16:45:37.626320	7036	Info	Service Control Manager	System

K:\OneDrive\Digital Forensics\SANS\2021 SANS DFIR Summit\Andrew Rathbun - EZ Tools KAPE How to Contribute to and Benefit from Open Source Contributions' | Total lines 34,771 | Visible lines 34,771 | Open files: 2 | Search options

Getting Started Making EvtxECmd Maps

The first one is always the hardest. After that, it’s all downhill from there

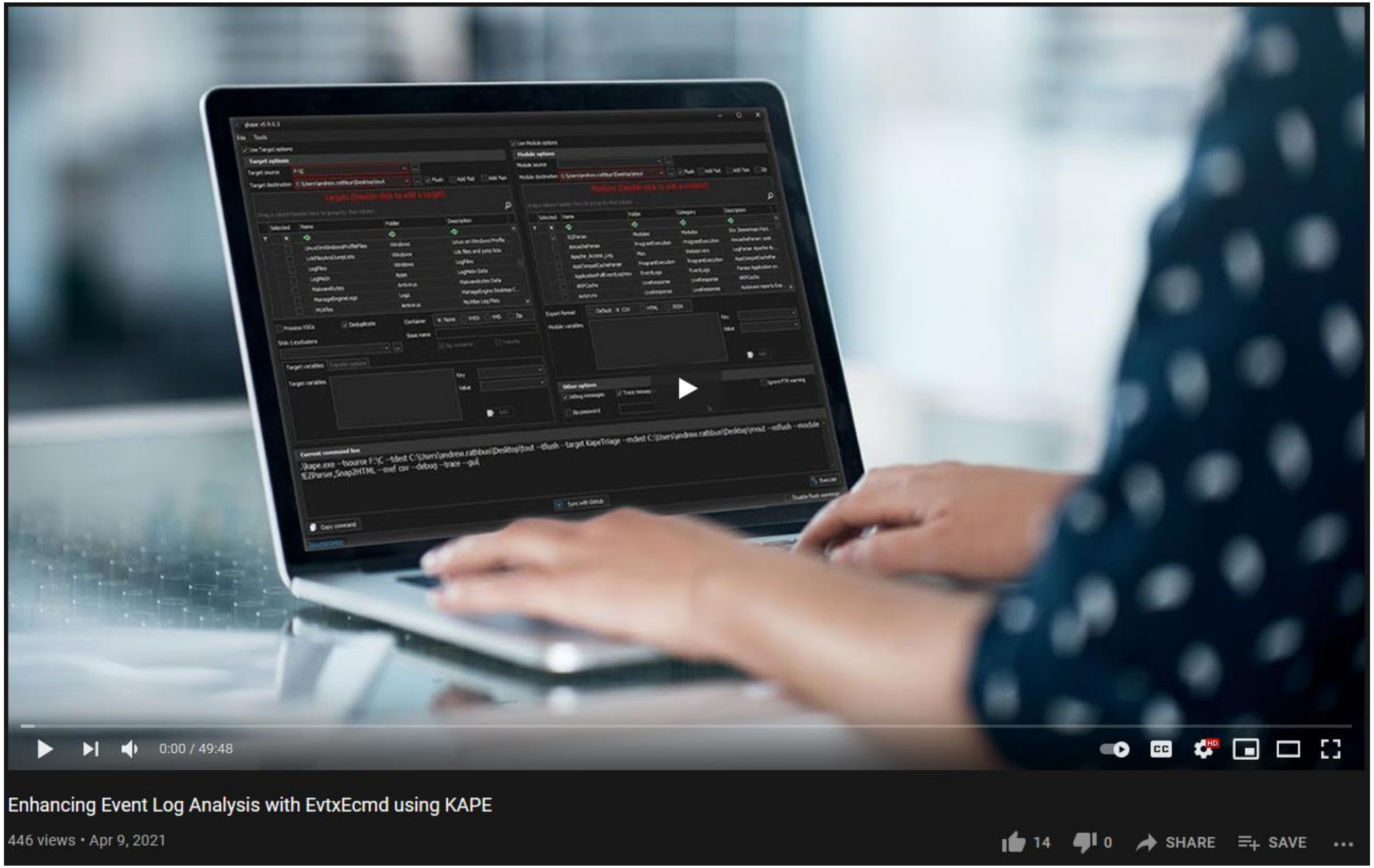
1. Identify a relevant event that needs a Map (happens often during everyday analysis)
   a) Make sure a Map doesn’t already exist for the event!
2. Convert .evtx file to XML using EvtxECmd
   a) evtxecmd.exe --f “path\to\evtx\file.evtx” --xml “C:\output\path” --debug
   b) KapeResearch_EventLogs.mkape
3. Read/follow the EvtxECmd Guide/Template on GitHub
4. Make a copy of an existing Map and rename it to give you a running start
5. Once the Map is created, put the Map within your .\EvtxECmd\Maps directory and parse your event log!
   a) evtxecmd.exe --f “path\to\evtx\file.evtx” --csv “C:\output\path” --debug
6. Review the output
   a) If something isn’t right, go back to your Map and adjust, as necessary. Trial and error!
   b) If you get stuck, don’t quit. Message me on Discord! Let’s walk it through to completion
7. Once desired output is achieved, contribute to the public repo
8. Tools of the Trade:
   a) Free: **EvtxECmd**, Windows Event Viewer (Useful for event messages, with OS-specific caveats)
   b) Paid: Event Log Observer, LogViewPlus, LogFusion Pro, Log Parser Lizard, Event Log Explorer



```
Name
!!!!README.md
!Channel-Name_Provider-Name_EventID.guide
!Channel-Name_Provider-Name_EventID.template
adPWDManager_adPWDManager_110.map
Application_Application-Error_1000.map
Application_Application-Hang_1002.map
Application_CarbonBlackDefense_17.map
Application_Citrix-Desktop-Service_1027.map
Application_Citrix-Desktop-Service_1049.map
Application_CylanceSvc_1.map
Application_CylanceSvc_2.map
Application_HitmanPro-Alert_911.map
Application_MetaFrameEvents_1106.map
Application_Microsoft-Windows-Audit-CVE_1.map
Application_Microsoft-Windows-RestartManager_10002.map
Application_Microsoft-Windows-Winsrv_10002.map
Application_MsiInstaller_1033.map
Application_MsiInstaller_1034.map
Application_MsiInstaller_11707.map
Application_MsiInstaller_11708.map
Application_MsiInstaller_11724.map
Application_Sophos-Anti-Virus_32.map
Application_Sophos-System-Protection_42.map
Application_System-Restore_8194.map
Application_System-Restore_8195.map
Application_System-Restore_8196.map
Application_Windows-Error-Reporting_1001.map
Application_WSH_0.map
```

Other EvtxECmd Resources

March 2021 Webinar



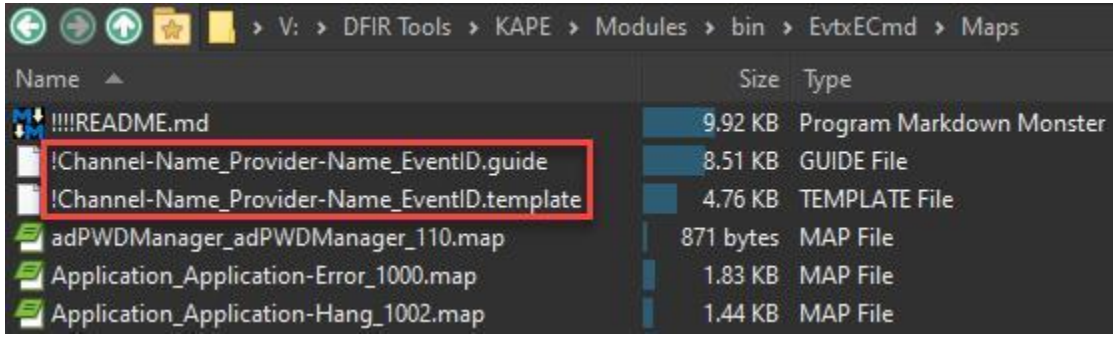
```
.\kape.exe --tsource F:\C --tdest C:\Users\andrew.rathbun\Desktop\tout --tflush --target KapeTriage --mdest C:\Users\andrew.rathbun\Desktop\mout --mflush --module
!EZParser,Snap2HTML --mef csv --debug --trace --gui
```

Enhancing Event Log Analysis with EvtxEcmd using KAPE

446 views • Apr 9, 2021

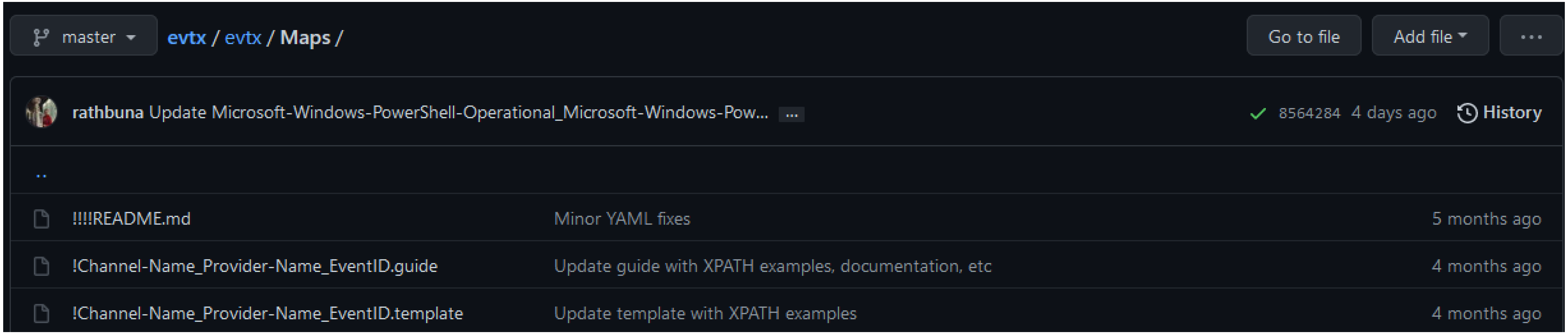
Other EvtxECmd Resources

.\KAPE\Modules\bin\EvtxECmd\Maps or EvtxECmd Maps Guide/Template on GitHub



V: › DFIR Tools › KAPE › Modules › bin › EvtxECmd › Maps

Name	Size	Type
!!!!README.md	9.92 KB	Program Markdown Monster
!Channel-Name_Provider-Name_EventID.guide	8.51 KB	GUIDE File
!Channel-Name_Provider-Name_EventID.template	4.76 KB	TEMPLATE File
adPWDManager_adPWDManager_110.map	871 bytes	MAP File
Application_Application-Error_1000.map	1.83 KB	MAP File
Application_Application-Hang_1002.map	1.44 KB	MAP File



evtx / evtx / Maps /

rathbuna Update Microsoft-Windows-PowerShell-Operational_Microsoft-Windows-Pow... … ✓ 8564284 4 days ago

..

!!!!README.md	Minor YAML fixes	5 months ago
!Channel-Name_Provider-Name_EventID.guide	Update guide with XPATH examples, documentation, etc	4 months ago
!Channel-Name_Provider-Name_EventID.template	Update template with XPATH examples	4 months ago

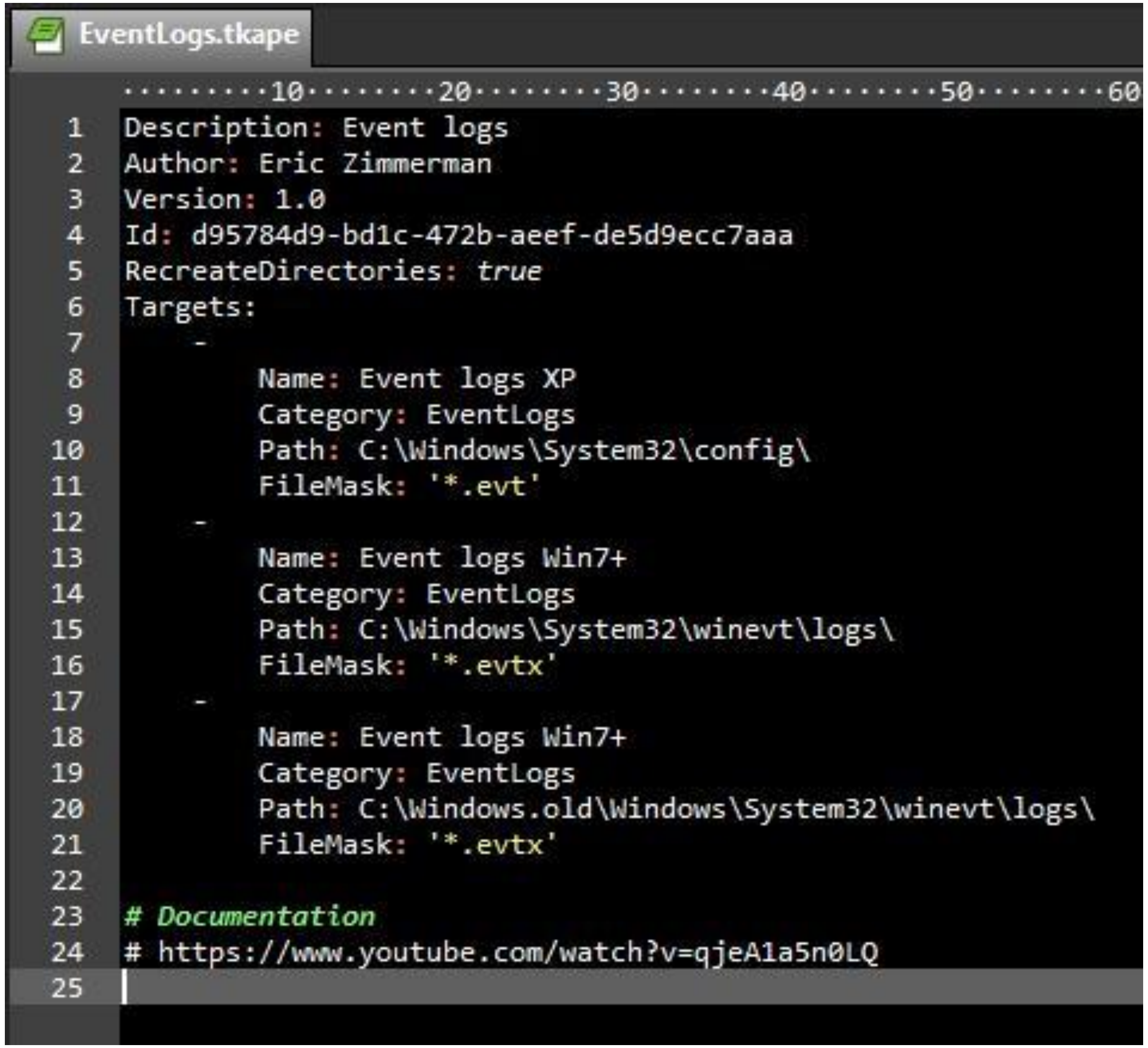
KAPE

Targets and Modules

KAPE Targets

What are they and why do I care?

- Targets contain the location(s) of artifact(s) and KAPE uses those locations to grab those files in a forensically sound manner
- Text files (.tkape) in YAML
- 233 Targets as of 7/2/2021
- Windows applications usually write artifacts to disk in the following locations:
  - C:\Users\%User%\AppData\(Local|Roaming)
  - C:\ProgramData
  - Or…somewhere else, go hunt!
- Tools of the trade:
  - Free: **Everything**, **ProcMon**
  - Paid: **Directory Monitor Pro**
- Documentation at bottom of each Target provides a great way to learn about artifacts

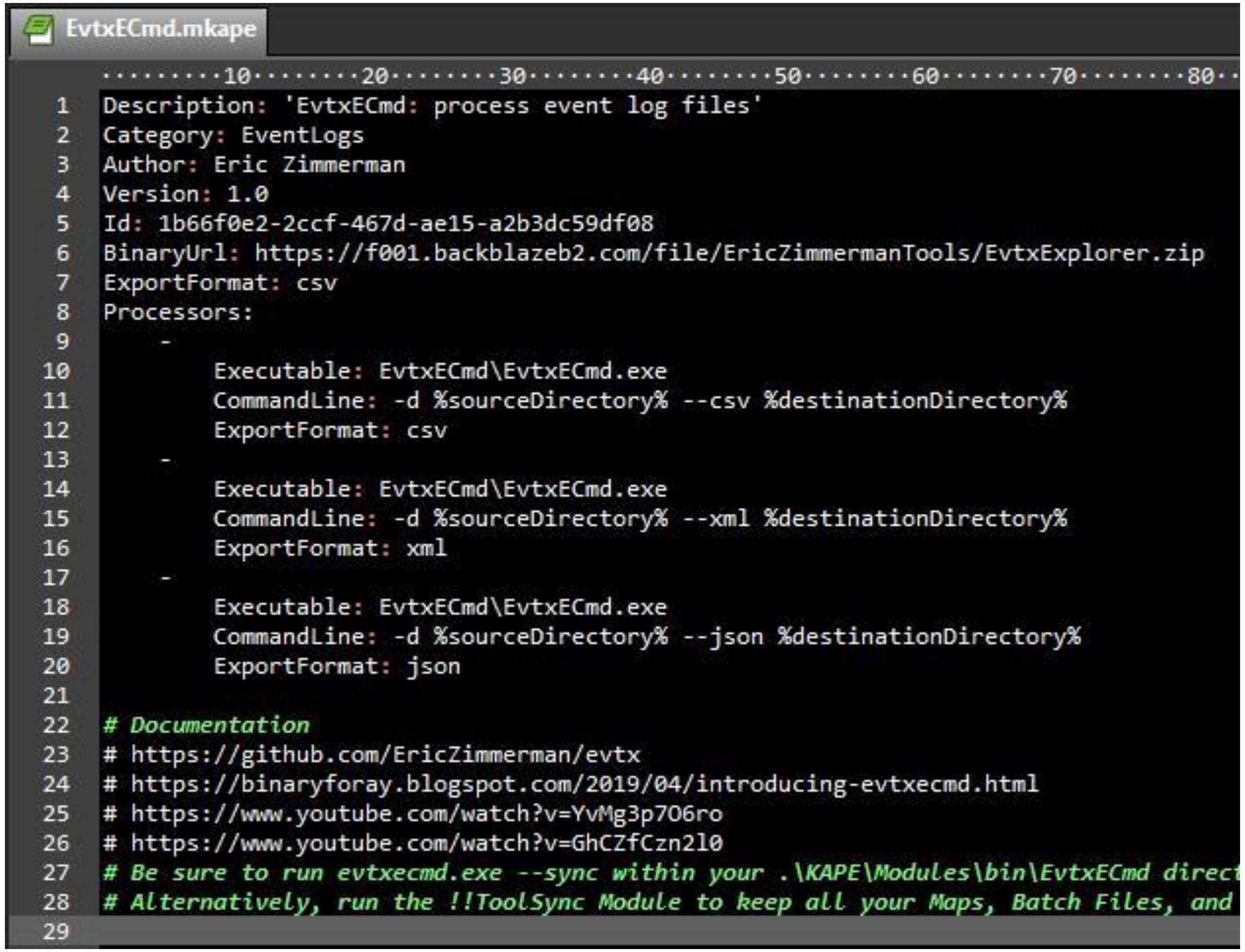


```
Description: Event logs
Author: Eric Zimmerman
Version: 1.0
Id: d95784d9-bd1c-472b-aeef-de5d9ecc7aaa
RecreateDirectories: true
Targets:
    -
        Name: Event logs XP
        Category: EventLogs
        Path: C:\Windows\System32\config\
        FileMask: '*.evt'
    -
        Name: Event logs Win7+
        Category: EventLogs
        Path: C:\Windows\System32\winevt\logs\
        FileMask: '*.evtx'
    -
        Name: Event logs Win7+
        Category: EventLogs
        Path: C:\Windows.old\Windows\System32\winevt\logs\
        FileMask: '*.evtx'

# Documentation
# https://www.youtube.com/watch?v=qjeA1a5n0LQ

```

KAPE Modules

What are they and why do I care?

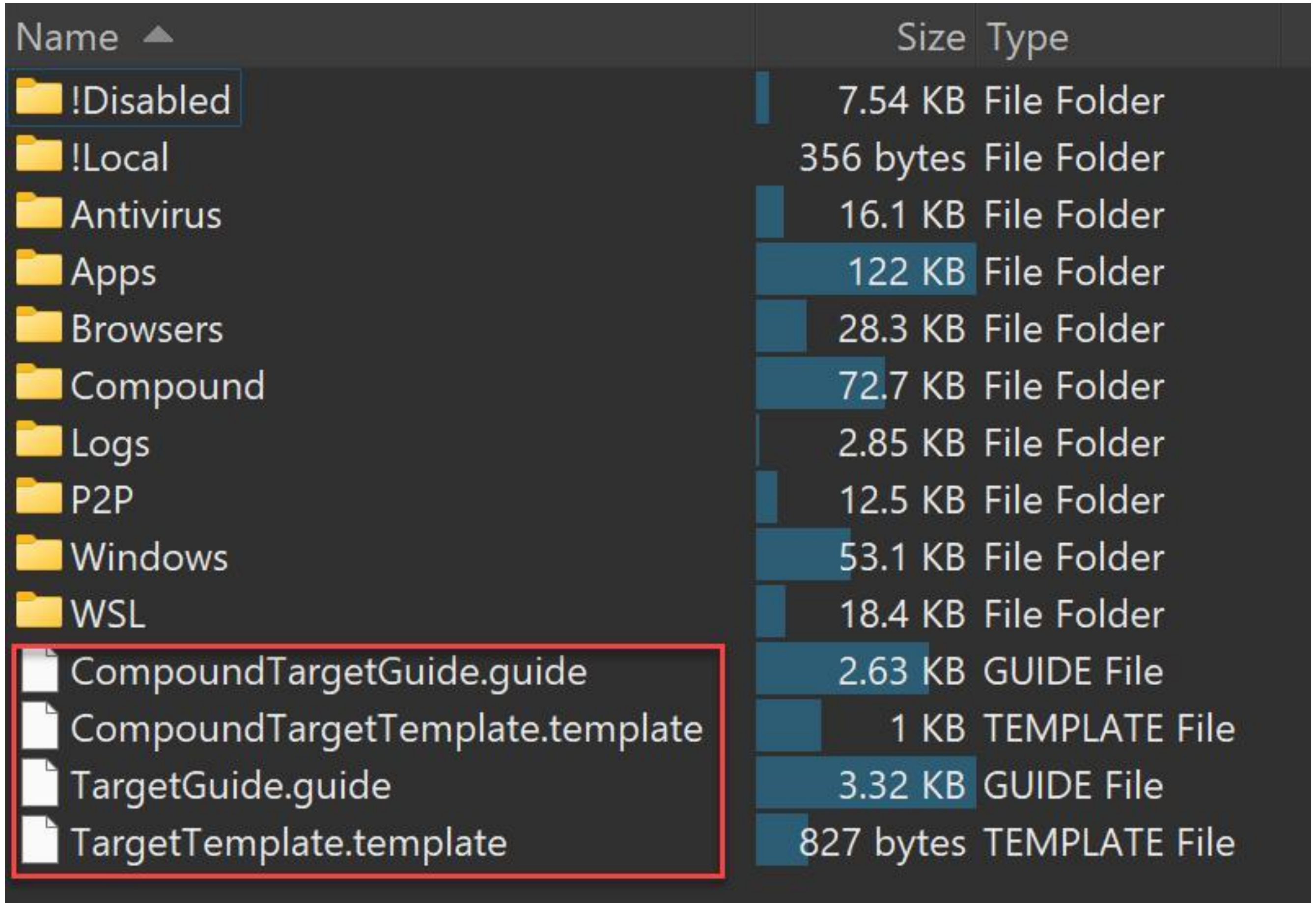
- Modules contain the commands for any given command line tool for KAPE to execute against collected data
- Text files (.mkape) in YAML
- 213 Modules as of 7/2/2021
- The use of any program with a command line interface can be automated using KAPE Modules
- Most of EZ Tools ship with KAPE and have Modules that contain commands that cover the most common use cases
- Modules for edge cases can always be created and shared to the public GitHub repo
- Any non-EZ Tool binary must reside in KAPE\Modules\bin for the associated Module to work
  - Use the link provided in BinaryUrl within each Module to download the tool
- Tools of the Trade:
  - Free: PowerShell/CMD, and the tool itself
  - Paid: the tool itself, if not free



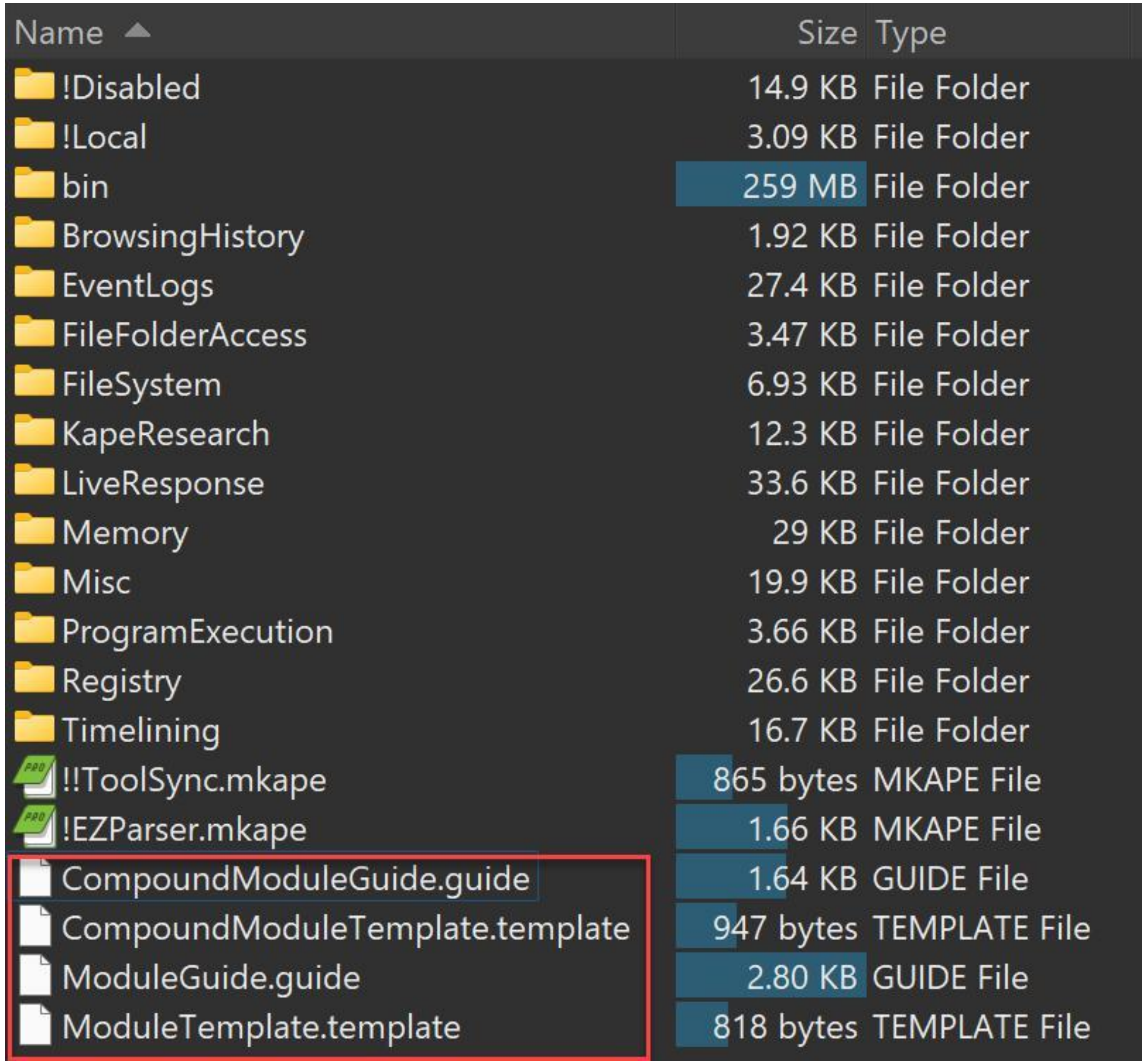
```
Description: 'EvtxECmd: process event log files'
Category: EventLogs
Author: Eric Zimmerman
Version: 1.0
Id: 1b66f0e2-2ccf-467d-ae15-a2b3dc59df08
BinaryUrl: https://f001.backblazeb2.com/file/EricZimmermanTools/EvtxExplorer.zip
ExportFormat: csv
Processors:
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --csv %destinationDirectory%
        ExportFormat: csv
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --xml %destinationDirectory%
        ExportFormat: xml
    -
        Executable: EvtxECmd\EvtxECmd.exe
        CommandLine: -d %sourceDirectory% --json %destinationDirectory%
        ExportFormat: json

# Documentation
# https://github.com/EricZimmerman/evtx
# https://binaryforay.blogspot.com/2019/04/introducing-evtxecmd.html
# https://www.youtube.com/watch?v=YvMg3p7O6ro
# https://www.youtube.com/watch?v=GhCZfCzn2l0
# Be sure to run evtxecmd.exe --sync within your .\KAPE\Modules\bin\EvtxECmd direct
# Alternatively, run the !!ToolSync Module to keep all your Maps, Batch Files, and

```

Other KAPE Targets and Modules Resources

.\KAPE\Targets or .\KAPE\Modules or KAPE Targets/Modules Guides/Template on GitHub



Name	Size	Type
!Disabled	7.54 KB	File Folder
!Local	356 bytes	File Folder
Antivirus	16.1 KB	File Folder
Apps	122 KB	File Folder
Browsers	28.3 KB	File Folder
Compound	72.7 KB	File Folder
Logs	2.85 KB	File Folder
P2P	12.5 KB	File Folder
Windows	53.1 KB	File Folder
WSL	18.4 KB	File Folder
CompoundTargetGuide.guide	2.63 KB	GUIDE File
CompoundTargetTemplate.template	1 KB	TEMPLATE File
TargetGuide.guide	3.32 KB	GUIDE File
TargetTemplate.template	827 bytes	TEMPLATE File



Name	Size	Type
!Disabled	14.9 KB	File Folder
!Local	3.09 KB	File Folder
bin	259 MB	File Folder
BrowsingHistory	1.92 KB	File Folder
EventLogs	27.4 KB	File Folder
FileFolderAccess	3.47 KB	File Folder
FileSystem	6.93 KB	File Folder
KapeResearch	12.3 KB	File Folder
LiveResponse	33.6 KB	File Folder
Memory	29 KB	File Folder
Misc	19.9 KB	File Folder
ProgramExecution	3.66 KB	File Folder
Registry	26.6 KB	File Folder
Timelining	16.7 KB	File Folder
!!ToolSync.mkape	865 bytes	MKAPE File
!EZParser.mkape	1.66 KB	MKAPE File
CompoundModuleGuide.guide	1.64 KB	GUIDE File
CompoundModuleTemplate.template	947 bytes	TEMPLATE File
ModuleGuide.guide	2.80 KB	GUIDE File
ModuleTemplate.template	818 bytes	TEMPLATE File

Keeping EZ Tools/KAPE Updated/Synced

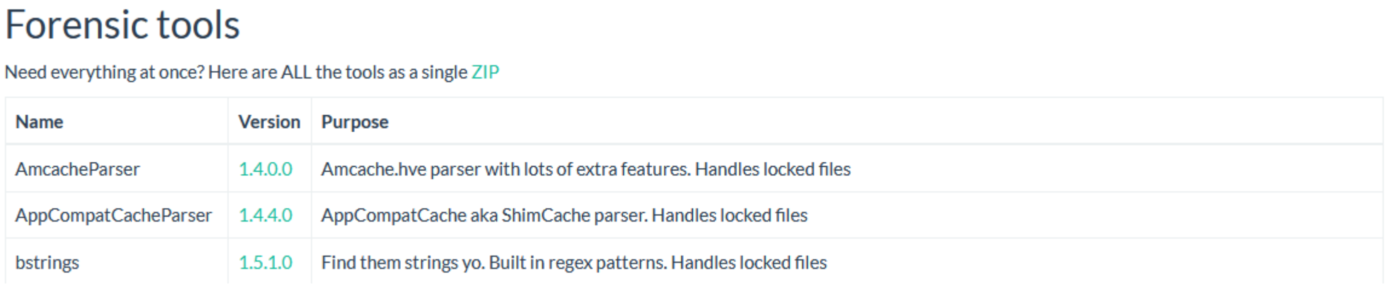
Update vs Sync and 3 Methods of Updating/Syncing

Important Considerations

Proper tool maintenance is just as important as knowing what the tool is doing and interpreting its results

***** Important *****

- It’s important to remember that EvtxECmd, SQLECmd, RECmd, and other EZ Tools can be used standalone (**Get-ZimmermanTools.ps1**) as well as called on by KAPE using Modules
- In that instance, any given EZ Tool binary is in two separate locations and therefore requires proper maintenance (i.e., checking for binary updates and syncing with GitHub) if they’re being actively used in either location
- It should go without saying that if you downloaded EZ Tools a year ago, use them daily, but haven’t yet synced or updated the binaries that you’re potentially missing out on a lot of Maps, Batch file updates, and new features/bug fixes



Forensic tools

Need everything at once? Here are ALL the tools as a single ZIP

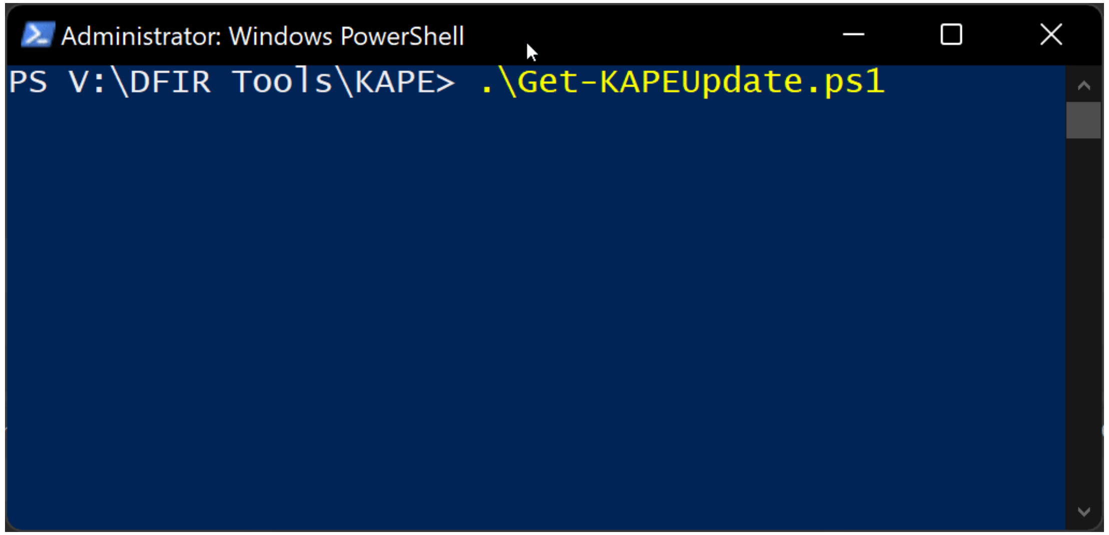
Name	Version	Purpose
AmcacheParser	1.4.0.0	Amcache.hve parser with lots of extra features. Handles locked files
AppCompatCacheParser	1.4.4.0	AppCompatCache aka ShimCache parser. Handles locked files
bstrings	1.5.1.0	Find them strings yo. Built in regex patterns. Handles locked files

THIS IS REALLY IMPORTANT

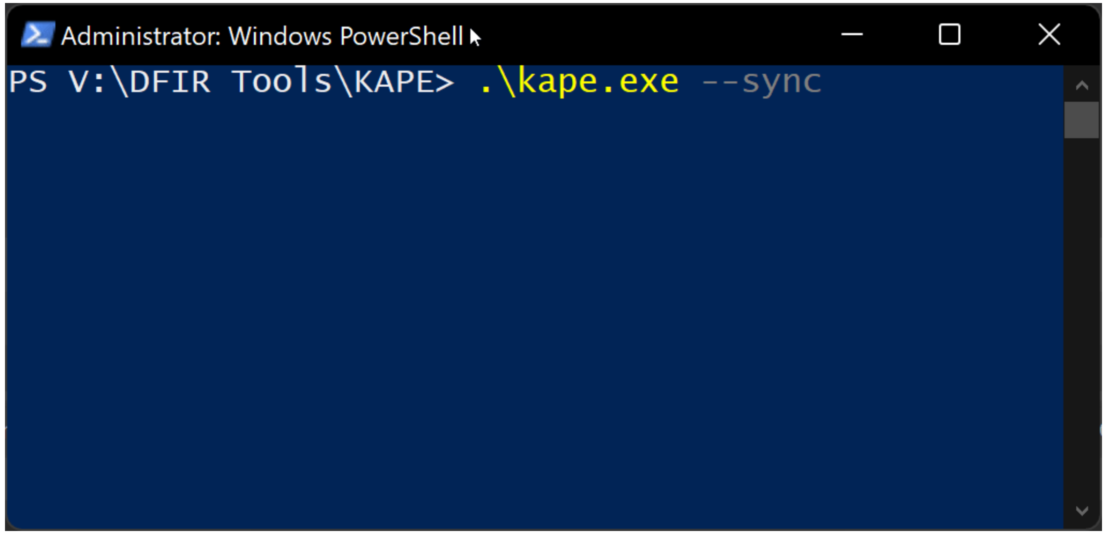
Differentiating Between Sync and Update

While similar in nature, they are talking about two different things

- Top GIF
  - **Update**: Checking to see if there is a new version of the KAPE binary
    - **Get-KAPEUpdate.ps1**
- Bottom GIF
  - **Sync**: Checking to see if Targets and Modules exist on GitHub that don't exist in local .\KAPE\Targets or .\KAPE\Modules directories
    - For this example, I removed the TotalCommander.tkape Target for demonstration, and then ran the sync command
      - **kape.exe --sync**
  - This process is identical for EvtxECmd, SQLECmd, and RECmd and their ancillary files
  - Let's call all the above Option 1



```
PS V:\DFIR Tools\KAPE> .\Get-KAPEUpdate.ps1
```

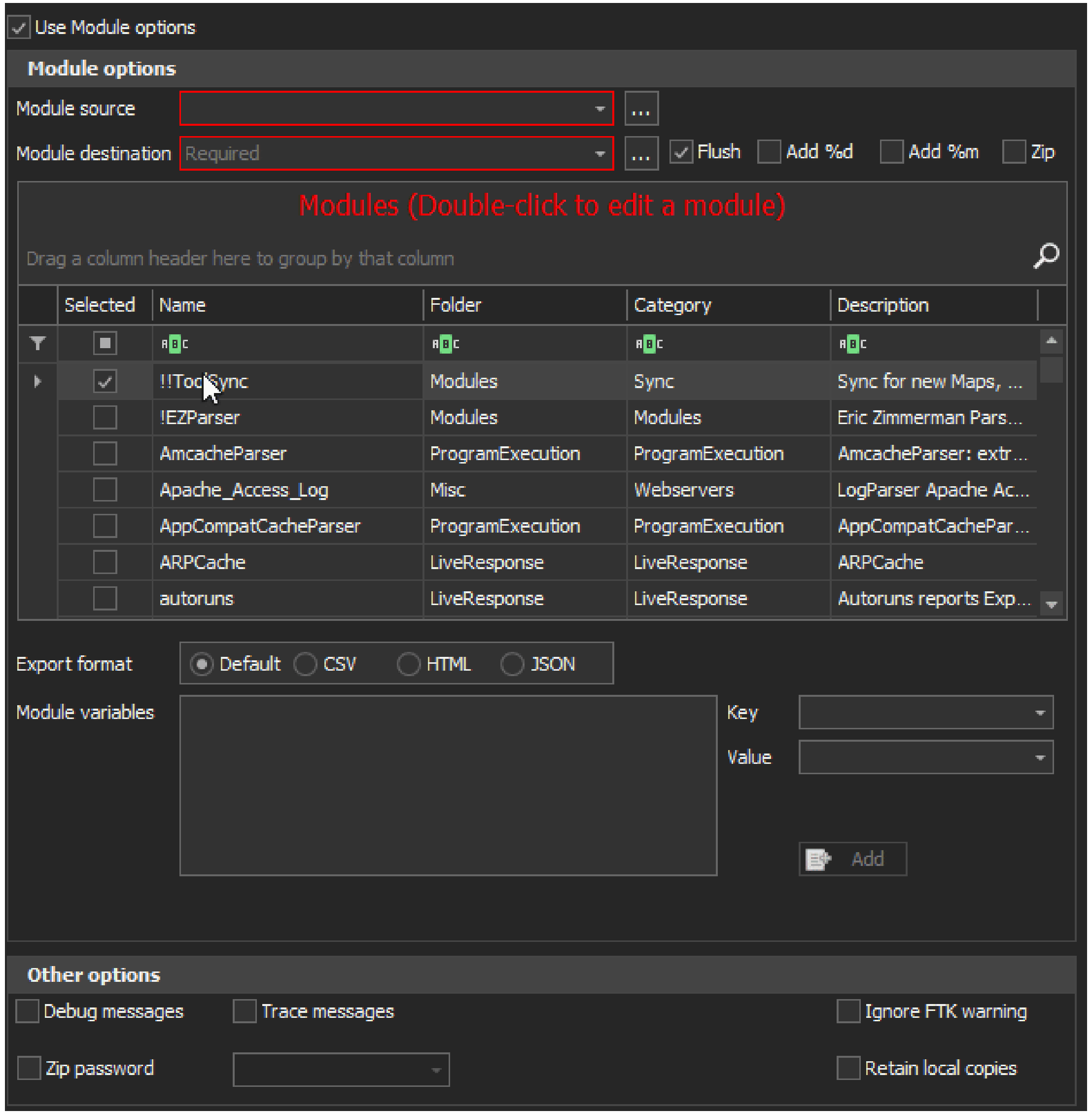


```
PS V:\DFIR Tools\KAPE> .\kape.exe --sync
```

Automating the Syncing of EZ Tools Used by KAPE

Option 2: !!ToolSync Module

- !!ToolSync Module **(!!ToolSync.mkape**) is a Compound Module that will keep all KAPE Targets/Module, EvtxECmd Maps, RECmd Batch Files, and SQLECmd Maps updated with a single click!
- !!ToolSync consists of the following commands:
  - .\evtxecmd.exe --sync
  - .\kape.exe --sync
  - .\recmd.exe –sync
  - .\sqlecmd.exe –sync
- Let’s call this Option 2
- Add this Module to your daily workflow to benefit!
- However, this doesn’t keep your KAPE binaries updated
  - .\KAPE\Modules\bin
- If only we had a solution to perform the task of !!ToolSync **AND** updating EZ Tools binaries for KAPE
- On to Option 3!



☑ Use Module options

Module options

Module source

Module destination Required ☑ Flush □ Add %d □ Add %m □ Zip

Modules (Double-click to edit a module)

Drag a column header here to group by that column

Selected	Name	Folder	Category	Description
☑	!!ToolSync	Modules	Sync	Sync for new Maps, ...
□	!EZParser	Modules	Modules	Eric Zimmerman Pars...
□	AmcacheParser	ProgramExecution	ProgramExecution	AmcacheParser: extr...
□	Apache_Access_Log	Misc	Webservers	LogParser Apache Ac...
□	AppCompatCacheParser	ProgramExecution	ProgramExecution	AppCompatCachePar...
□	ARPCache	LiveResponse	LiveResponse	ARPCache
□	autoruns	LiveResponse	LiveResponse	Autoruns reports Exp...

Export format ● Default ○ CSV ○ HTML ○ JSON

Module variables

Key

Value

Add

Other options

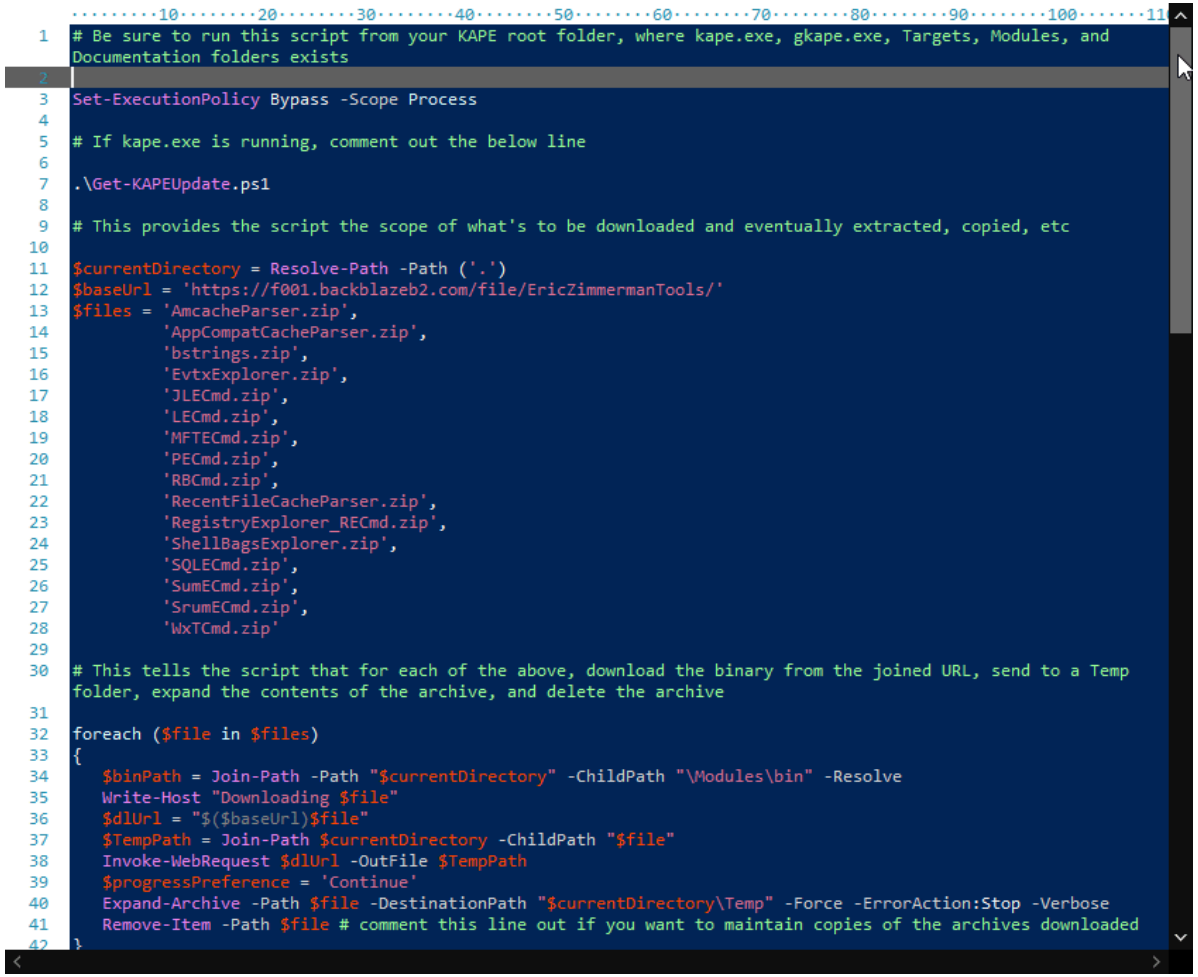
□ Debug messages □ Trace messages □ Ignore FTK warning

□ Zip password □ Retain local copies

Option 3: Get-KAPEUpdate2021.ps1

Sibling script to the preexisting Get-KAPEUpdate.ps1 script originally written by Eric Zimmerman

- My first experience with scripting in any language!
- Made specifically for this event, slide, and overall presentation
- PowerShell script that makes life easier when maintaining your instance of KAPE! This script does the following:
  1. Updates KAPE by calling **Get-KAPEUpdate.ps1**
  2. Downloads a curated group of EZ Tools to satisfy the requirements for the KAPE !EZParser Module
  3. Downloads each tool, unzips them, and deletes unnecessary files (i.e., GUI applications)
  4. Performs a sync to update all Maps, Batch Files, Targets, and Modules
  5. Copies everything you need to run a fully updated version of KAPE with updated EZ Tools binaries and the latest ancillary files
- Yes, earlier I said I can’t code, but I can Google! Again, you don’t have to know everything. Being resourceful is way more valuable (and realistic) than knowing everything



```
# Be sure to run this script from your KAPE root folder, where kape.exe, gkape.exe, Targets, Modules, and Documentation folders exists

Set-ExecutionPolicy Bypass -Scope Process

# If kape.exe is running, comment out the below line

.\Get-KAPEUpdate.ps1

# This provides the script the scope of what's to be downloaded and eventually extracted, copied, etc

$currentDirectory = Resolve-Path -Path ('.')
$baseUrl = 'https://f001.backblazeb2.com/file/EricZimmermanTools/'
$files = 'AmcacheParser.zip',
         'AppCompatCacheParser.zip',
         'bstrings.zip',
         'EvtxExplorer.zip',
         'JLECmd.zip',
         'LECmd.zip',
         'MFTECmd.zip',
         'PECmd.zip',
         'RBCmd.zip',
         'RecentFileCacheParser.zip',
         'RegistryExplorer_RECmd.zip',
         'ShellBagsExplorer.zip',
         'SQLECmd.zip',
         'SumECmd.zip',
         'SrumECmd.zip',
         'WxTCmd.zip'

# This tells the script that for each of the above, download the binary from the joined URL, send to a Temp folder, expand the contents of the archive, and delete the archive

foreach ($file in $files)
{
   $binPath = Join-Path -Path "$currentDirectory" -ChildPath "\Modules\bin" -Resolve
   Write-Host "Downloading $file"
   $dlUrl = "$($baseUrl)$file"
   $TempPath = Join-Path $currentDirectory -ChildPath "$file"
   Invoke-WebRequest $dlUrl -OutFile $TempPath
   $progressPreference = 'Continue'
   Expand-Archive -Path $file -DestinationPath "$currentDirectory\Temp" -Force -ErrorAction:Stop -Verbose
   Remove-Item -Path $file # comment this line out if you want to maintain copies of the archives downloaded
}
```

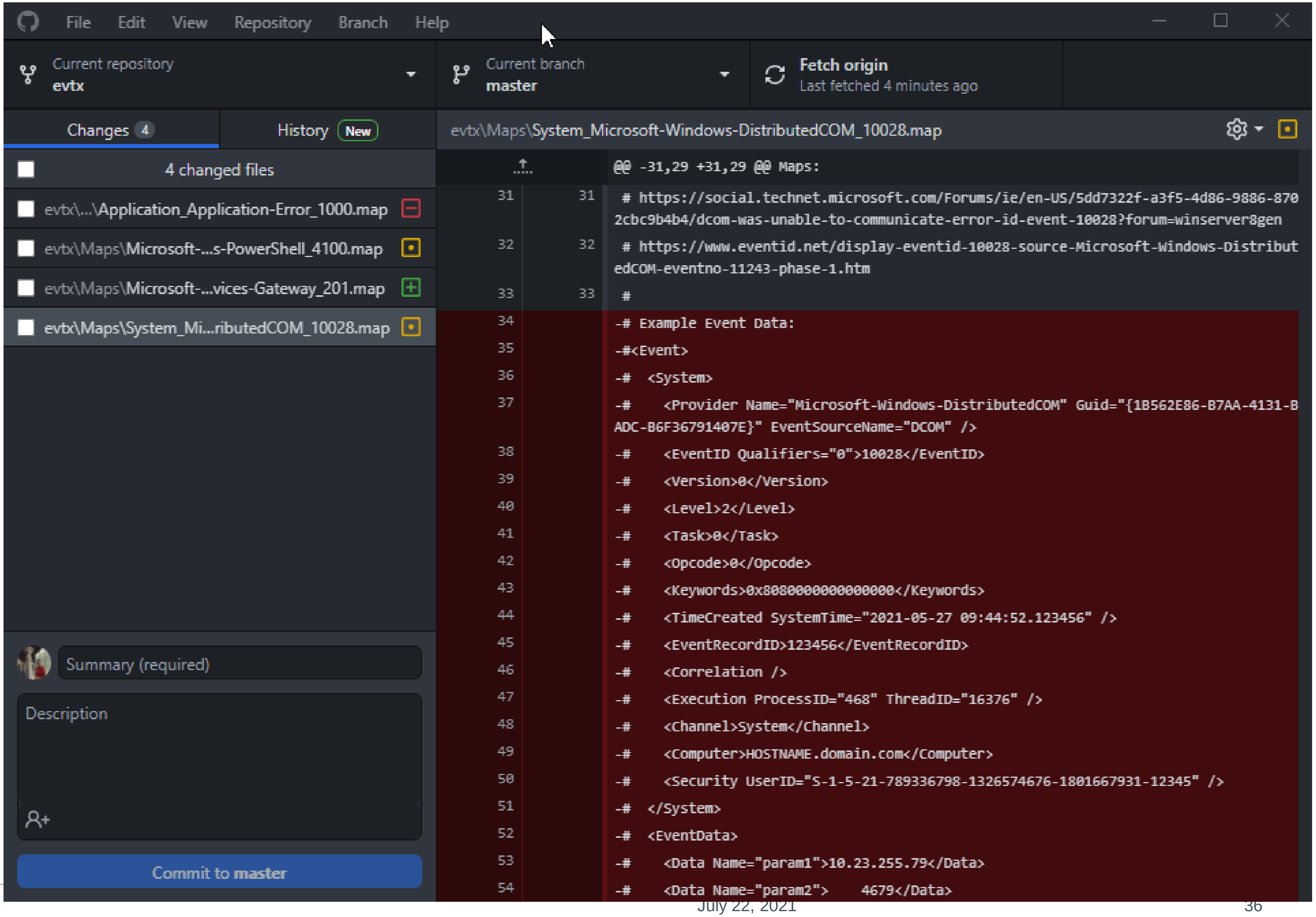
Contributing to GitHub

GitHub Desktop, Tips, and GitHub Repos to Watch

Contributing to GitHub – The Basics

Use a Git client to monitor repositories on your file system and easily share your work on GitHub!

- Clients with Git integration effectively monitor any changes to a specific folder where files cloned from GitHub repos reside
- You can edit these files in any way you want with any applications you want
- Once you’re ready to commit to a GitHub repo, just pick and choose which changes you want to commit!
- Tools of the Trade:
    - Free: **GitHub Desktop**, Git (CLI)
    - Paid: Sublime Merge, Araxis Merge, Fork, Atom, UEStudio, Tower, GitKraken, and more



□ 4 changed files

- □ evtx\...\Application_Application-Error_1000.map
- □ evtx\Maps\Microsoft-...s-PowerShell_4100.map
- □ evtx\Maps\Microsoft-...vices-Gateway_201.map
- □ evtx\Maps\System_Mi...ributedCOM_10028.map

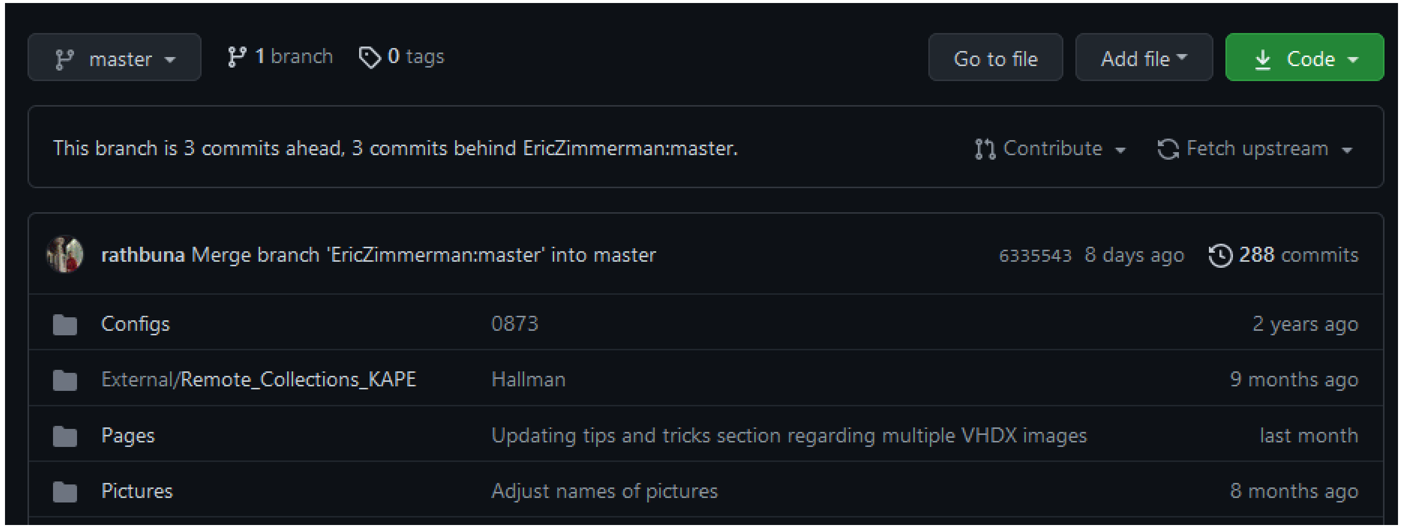
evtx\Maps\System_Microsoft-Windows-DistributedCOM_10028.map

```
@@ -31,29 +31,29 @@ Maps:
 # https://social.technet.microsoft.com/Forums/ie/en-US/5dd7322f-a3f5-4d86-9886-8702cbc9b4b4/dcom-was-unable-to-communicate-error-id-event-10028?forum=winserver8gen
 # https://www.eventid.net/display-eventid-10028-source-Microsoft-Windows-DistributedCOM-eventno-11243-phase-1.htm
 #
-# Example Event Data:
-#<Event>
-#  <System>
-#    <Provider Name="Microsoft-Windows-DistributedCOM" Guid="{1B562E86-B7AA-4131-BADC-B6F36791407E}" EventSourceName="DCOM" />
-#    <EventID Qualifiers="0">10028</EventID>
-#    <Version>0</Version>
-#    <Level>2</Level>
-#    <Task>0</Task>
-#    <Opcode>0</Opcode>
-#    <Keywords>0x8080000000000000</Keywords>
-#    <TimeCreated SystemTime="2021-05-27 09:44:52.123456" />
-#    <EventRecordID>123456</EventRecordID>
-#    <Correlation />
-#    <Execution ProcessID="468" ThreadID="16376" />
-#    <Channel>System</Channel>
-#    <Computer>HOSTNAME.domain.com</Computer>
-#    <Security UserID="S-1-5-21-789336798-1326574676-1801667931-12345" />
-#  </System>
-#  <EventData>
-#    <Data Name="param1">10.23.255.79</Data>
-#    <Data Name="param2">    4679</Data>
```

Contributing to GitHub – Things Learned the Hard Way

Learn from my mistakes!

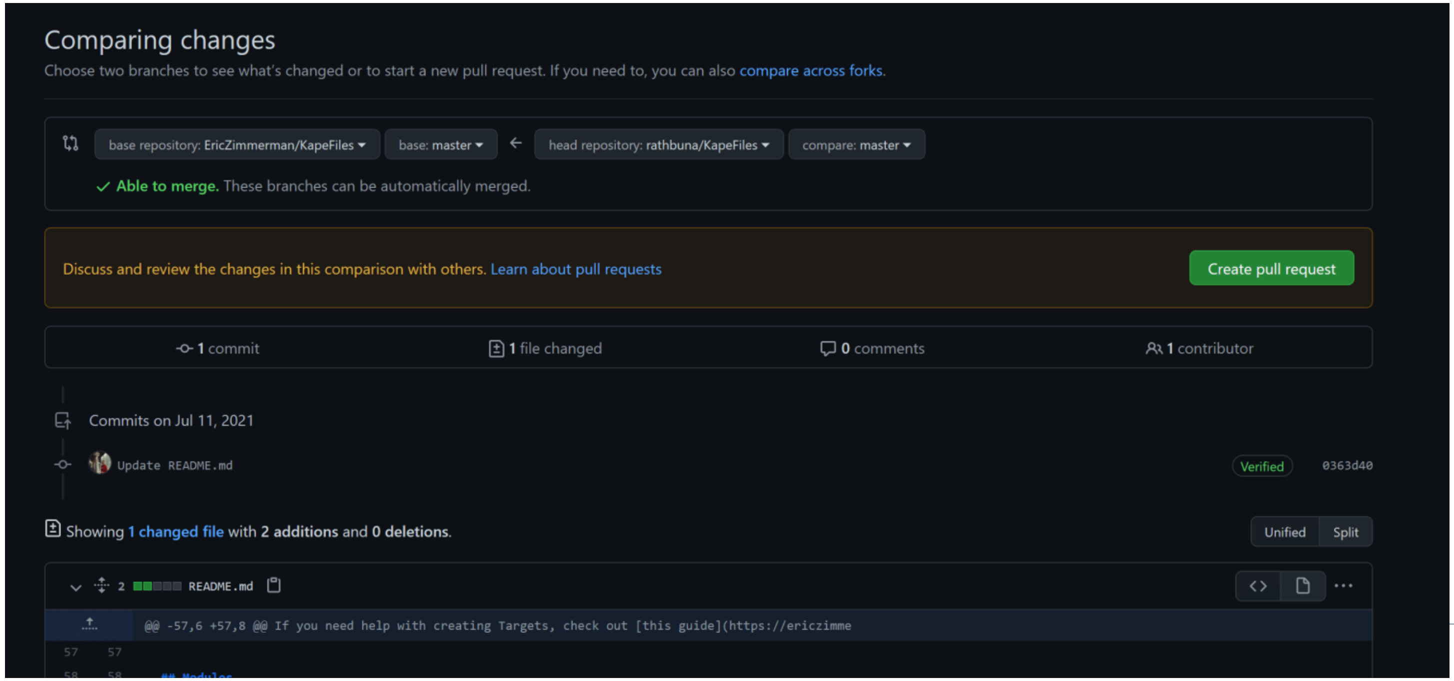
- Update your fork before contributing to your upstream!
  - GitHub recently made this much easier with more plain-English (see image to the right)
- https://github.com/firstcontributions/first-contributions/blob/master/gui-tool-tutorials/github-desktop-tutorial.md



This branch is 3 commits ahead, 3 commits behind EricZimmerman:master.

rathbuna Merge branch 'EricZimmerman:master' into master 6335543 8 days ago 288 commits

Configs	0873	2 years ago
External/Remote_Collections_KAPE	Hallman	9 months ago
Pages	Updating tips and tricks section regarding multiple VHDX images	last month
Pictures	Adjust names of pictures	8 months ago



Comparing changes

Choose two branches to see what's changed or to start a new pull request. If you need to, you can also compare across forks.

base repository: EricZimmerman/KapeFiles ← base: master ← head repository: rathbuna/KapeFiles compare: master

✓ Able to merge. These branches can be automatically merged.

Discuss and review the changes in this comparison with others. Learn about pull requests

1 commit 1 file changed 0 comments 1 contributor

Commits on Jul 11, 2021

Update README.md Verified 0363d40

Showing 1 changed file with 2 additions and 0 deletions.

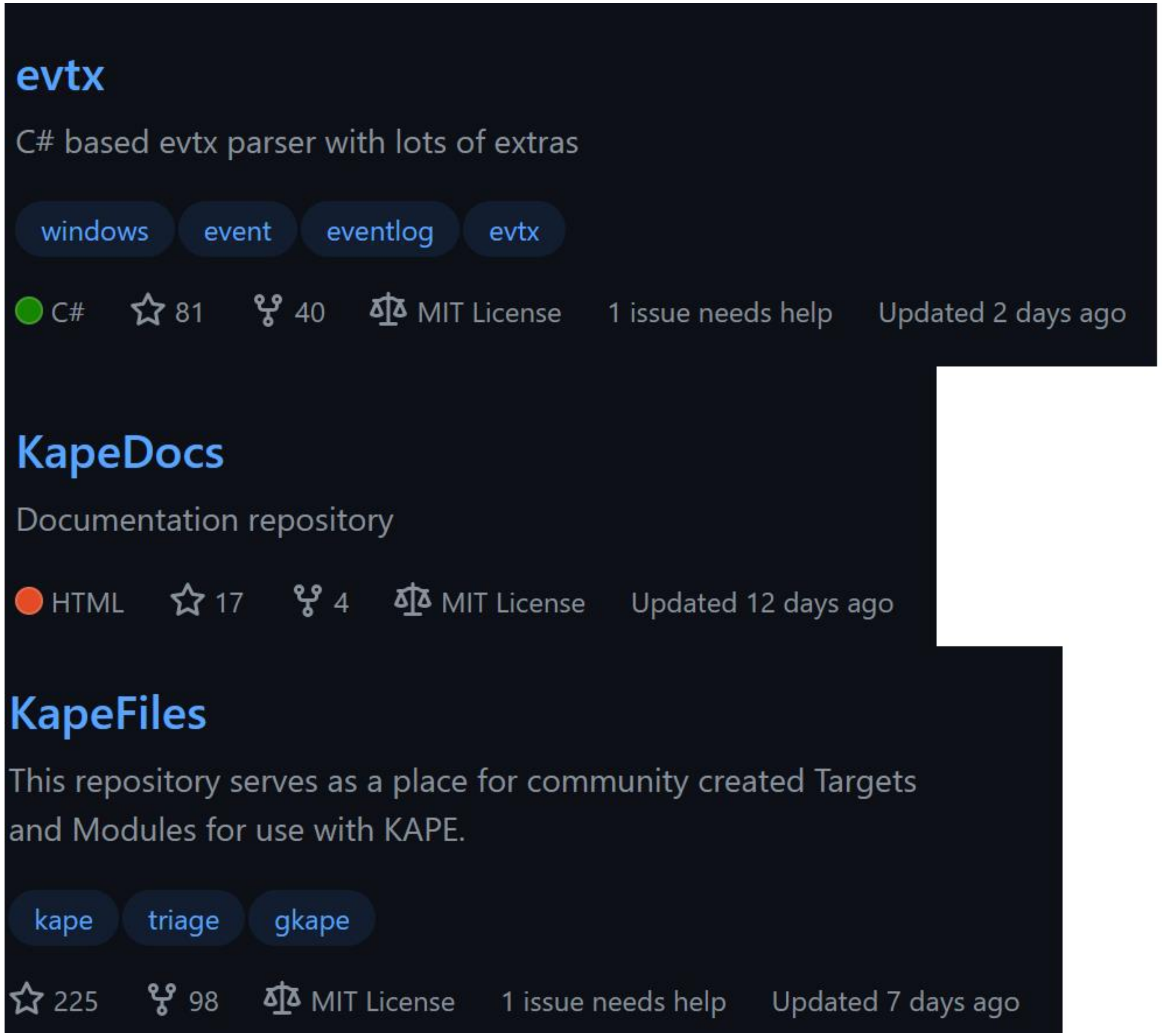
2 README.md

```
@@ -57,6 +57,8 @@ If you need help with creating Targets, check out [this guide](https://ericzimme
57  57
58  58      ## Modules
```

- Follow the Pull Request template that has been established for any given GitHub repo you're contributing to
- The steps are there for a reason to maintain quality control and reduce the amount of corrective action needed to approve and merge new content/code

Important EZ Tools/KAPE GitHub Repositories

EvtxECmd, RECmd, SQLECmd, and KAPE



evtx

C# based evtx parser with lots of extras

windows event eventlog evtx

● C# ☆ 81 40 MIT License 1 issue needs help Updated 2 days ago

KapeDocs

Documentation repository

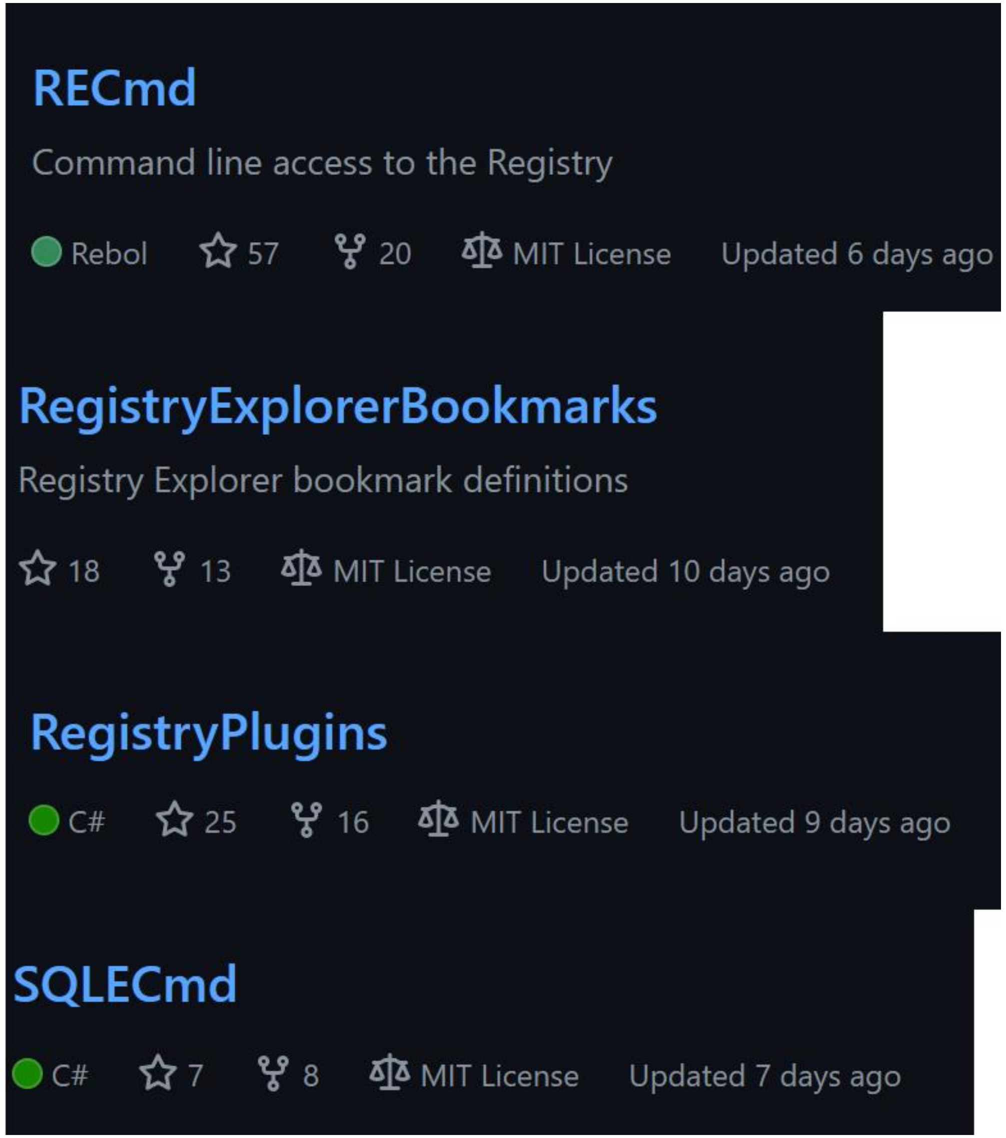
● HTML ☆ 17 4 MIT License Updated 12 days ago

KapeFiles

This repository serves as a place for community created Targets and Modules for use with KAPE.

kape triage gkape

☆ 225 98 MIT License 1 issue needs help Updated 7 days ago



RECmd

Command line access to the Registry

● Rebol ☆ 57 20 MIT License Updated 6 days ago

RegistryExplorerBookmarks

Registry Explorer bookmark definitions

☆ 18 13 MIT License Updated 10 days ago

RegistryPlugins

● C# ☆ 25 16 MIT License Updated 9 days ago

SQLECmd

● C# ☆ 7 8 MIT License Updated 7 days ago

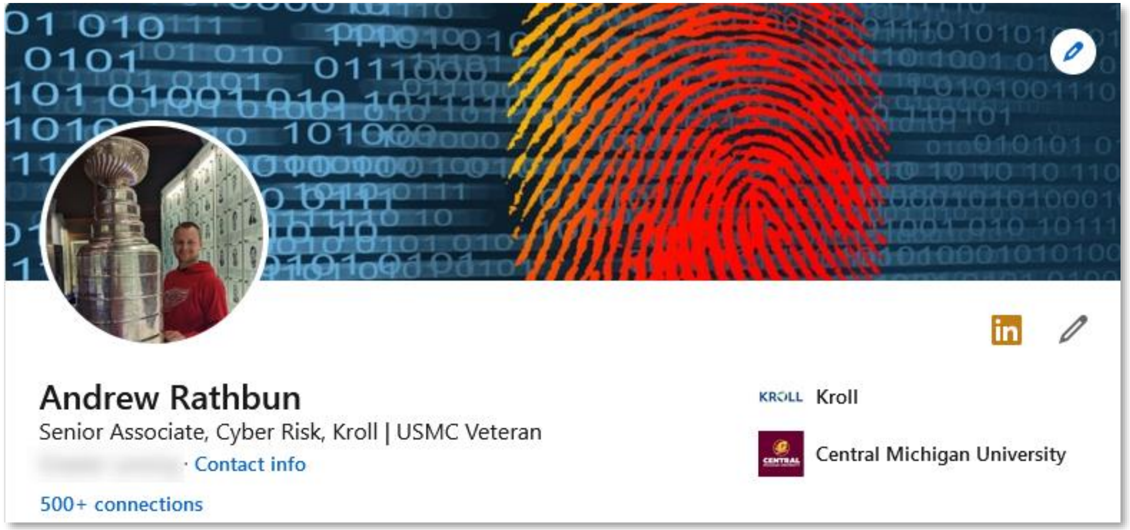
Key Takeaways

Thank you for your time and attention!

- Keeping EZ Tools binaries updated is very important!
  - Within EZ Tools **AND** KAPE directories, if you actively use both!
    - Use the PS script to automate the boring stuff
- Keeping the ancillary files synced with GitHub is very important as they are constantly evolving, being updated, and added to!
  - EvtxECmd Maps
  - SQLECmd Maps
  - RECmd Batch Files
  - KAPE Targets and Modules
- Check for new binaries on a weekly basis (at least) using the PS script mentioned in this presentation
  - Scheduled task, maybe?
- Add !!ToolSync to every KAPE run so long as the machine KAPE is running on is connected to the internet
  - Ancillary files are typically added and updated more often than binaries
- Watch the repos!
- Contribute when you find something new. Sharing is caring!

Q&A Time

Feel free to connect with me! See you on Slack (hallway-andrew-rathbun)



Andrew Rathbun

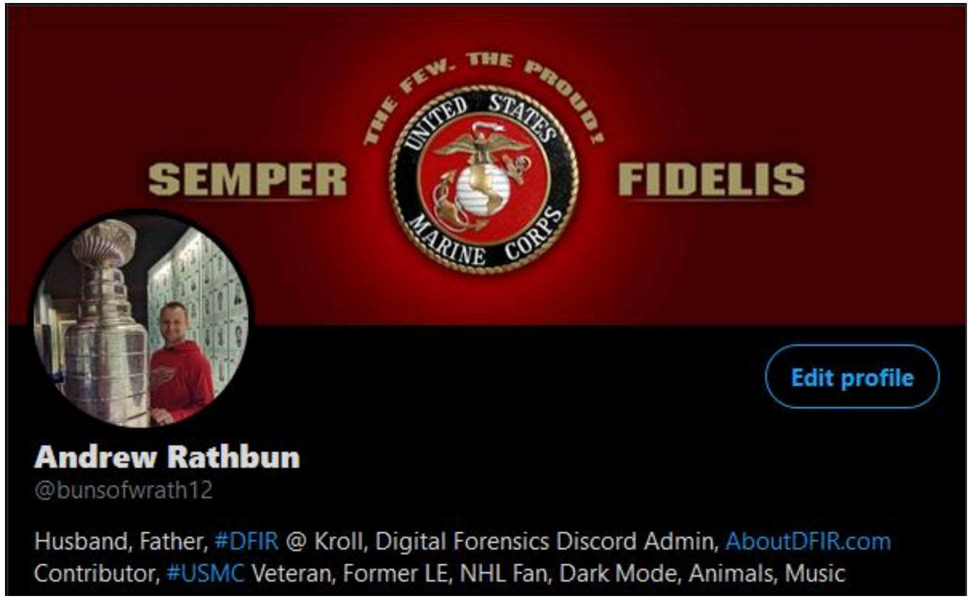
Senior Associate, Cyber Risk, Kroll | USMC Veteran

[redacted] · Contact info

500+ connections

Kroll

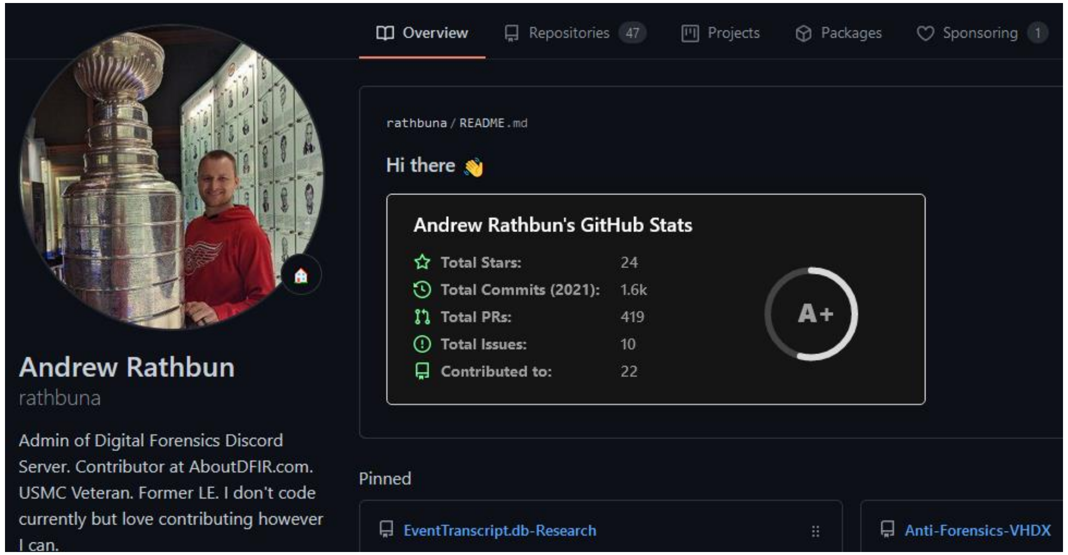
Central Michigan University



Andrew Rathbun

@bunsofwrath12

Husband, Father, #DFIR @ Kroll, Digital Forensics Discord Admin, AboutDFIR.com Contributor, #USMC Veteran, Former LE, NHL Fan, Dark Mode, Animals, Music



Andrew Rathbun

rathbuna

Admin of Digital Forensics Discord Server. Contributor at AboutDFIR.com. USMC Veteran. Former LE. I don't code currently but love contributing however I can.

rathbuna / README.md

Hi there 👋

Andrew Rathbun's GitHub Stats

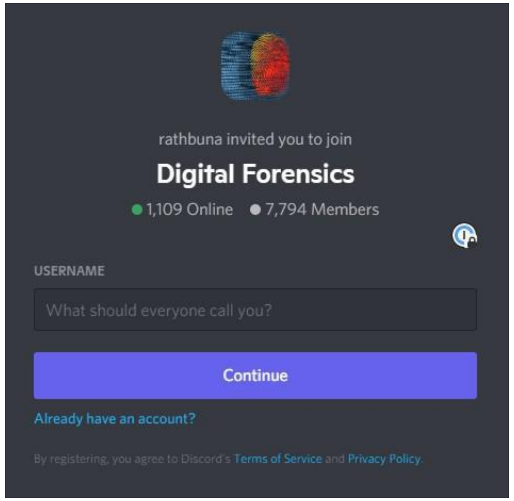
Total Stars:	24
Total Commits (2021):	1.6k
Total PRs:	419
Total Issues:	10
Contributed to:	22

A+

Pinned

EventTranscript.db-Research

Anti-Forensics-VHDX



rathbuna invited you to join

Digital Forensics

● 1,109 Online ● 7,794 Members

USERNAME

What should everyone call you?

By registering, you agree to Discord's Terms of Service and Privacy Policy.