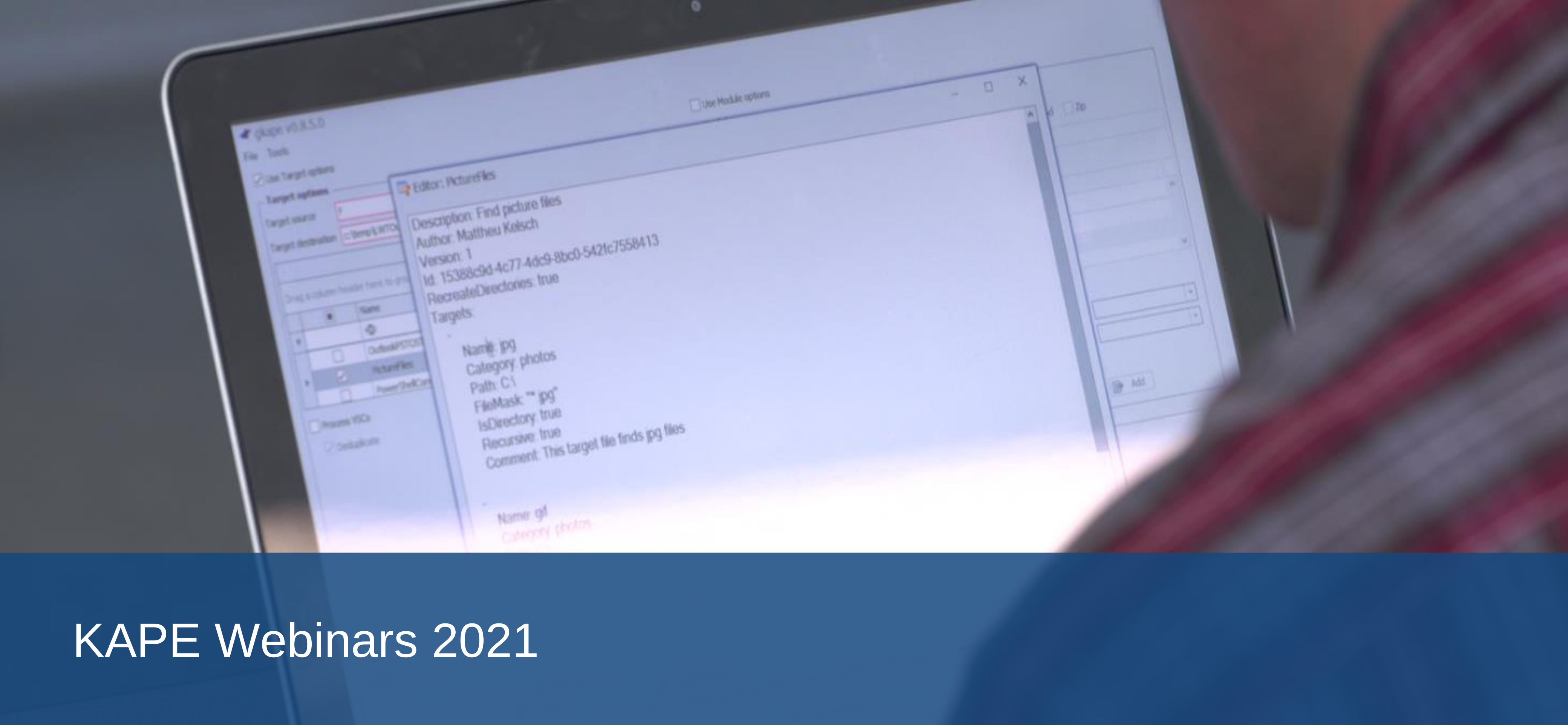


```
Description: Find picture files
Author: Mattheu Kelsch
Version: 1
Id: 15388c9d-4c77-4dc9-8bc0-542fc7558413
RecreateDirectories: true
Targets:
-
    Name: jpg
    Category: photos
    Path: C:\
    FileMask: "*.jpg"
    IsDirectory: true
    Recursive: true
    Comment: This target file finds jpg files
-
    Name: gif
    Category: photos
```

KAPE Webinars 2021

Enhancing Event Log Analysis with EvtxECmd using KAPE

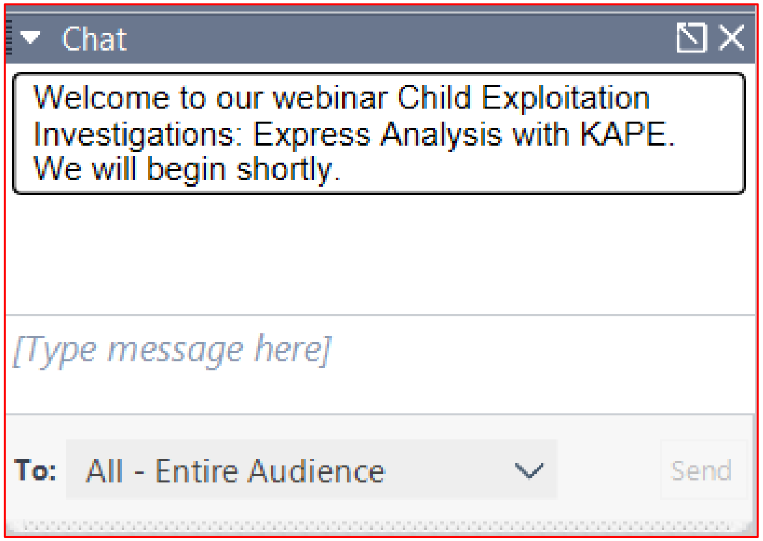
March 2021

Private and Confidential

Notes

- Session is being recorded, You'll receive access to the recording in a couple days

- Ask questions via chat >



Welcome to our webinar Child Exploitation Investigations: Express Analysis with KAPE. We will begin shortly.

- We'll try to answer as many questions as possible

Upcoming KAPE Intensive Training and Certification Sessions

- Virtual live sessions
- Max 25 students

Full Calendar Available here:

bit.ly/KAPE2021

SCHEDULE	INSTRUCTORS
April 13, 2021 10:00 a.m. – 7:00 p.m. (EST)	Eric Zimmerman Sean Straw Scott Zuberbuehler Andrew Rathbun
June 3, 2021 8:00 a.m. – 5:00 p.m. (GMT)	James Thoburn Paul Wells Guillermo Roman
June 17, 2021 10:00 a.m. – 7:00 p.m. (EST)	Sean Straw Scott Zuberbuehler Andrew Rathbun

About Andrew Rathbun

Senior Associate, Kroll Cyber Risk

- 2020-Present: Senior Associate at Kroll, Cyber Risk
  - Digital Forensics & Incident Response (DFIR)
  - KAPE Instructor
- 2019-2020: HHS OIG, Forensic Computer Examiner (2210)
- 2012-2019: Michigan State University Police Department
  - 2012-2015 as a Police Officer
  - 2016-2019 as a Detective (digital forensics and general investigations)
- USMC Veteran (0311)
- Side Projects
  - 2018-Present: Administrator of the Digital Forensics Discord Server
  - 2019-Present: AboutDFIR.com Contributor
  - 2020-Present: GitHub
- LinkedIn (andrewrathbun) or Twitter (@bunsofwrath12) or GitHub (rathbuna)

Presentation Housekeeping/Expectations

Look at this subheading for Information on what the GIFs or Images are displaying

- What to expect?
  - Lots of looping GIFs
    - Repetition will help drive concepts home and how to use the tools
    - Read the subheading of each slide for information relating to the GIF/Image on each slide
  - Short live demo
  - Question and answer session at the end
- Tools Used
  - KAPE – Acquisition/Automation
  - EvtxECmd - Parsing
  - Timeline Explorer - Analysis

Overview

Event Logs (*.EVTX files)

EvtxECmd

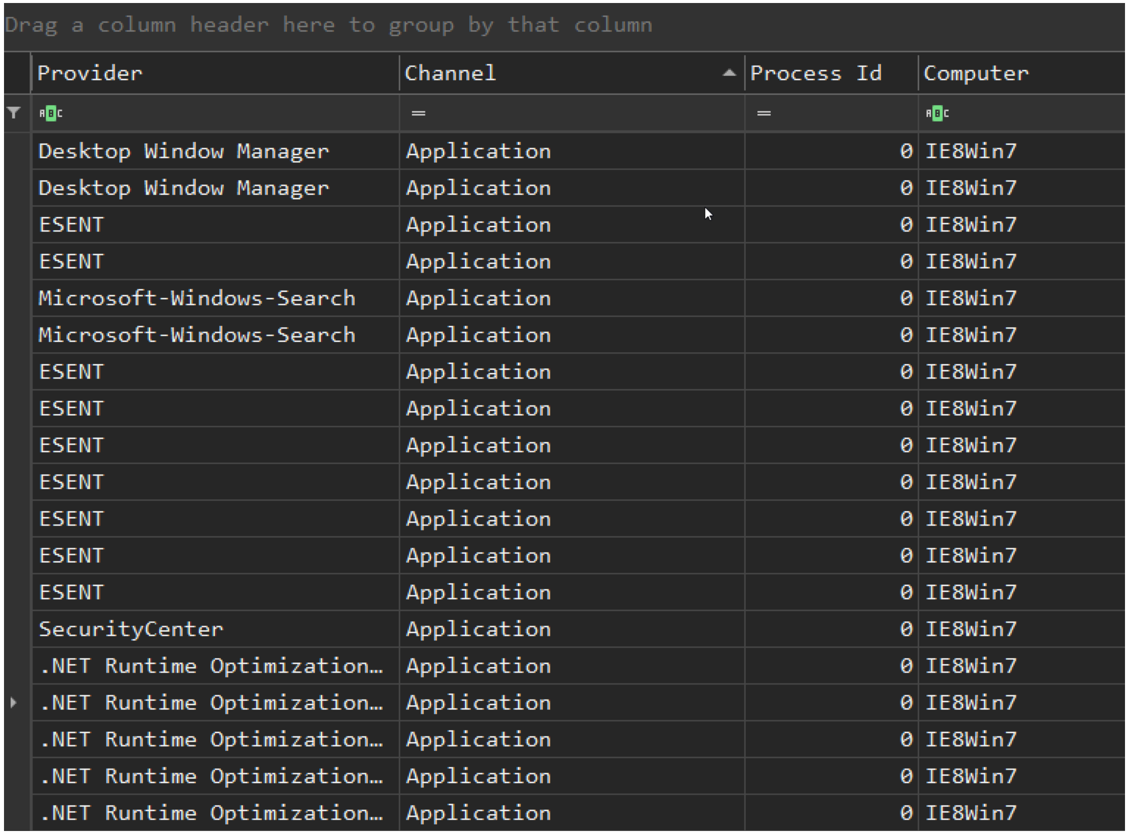
EvtxECmd Maps

Using EvtxECmd with KAPE (!EZParser)

Event Logs

Column Header filter on Channel and Provider columns to display deduped column contents

- Windows XP - .evt
- Windows Vista+ - .evtx
- Location: C:\Windows\System32\winevt\Logs
- 4 key elements
  - Channel
  - Provider
  - Event ID
  - Payload
- *.EVTX files
  - * is the name of the Channel
- Providers log to applicable Channel
- Event IDs are not globally unique
- Example: Application.evtx
  - Dumping ground for Third-Party Applications
  - Lots of duplicate event IDs
- Payload has data we analyze

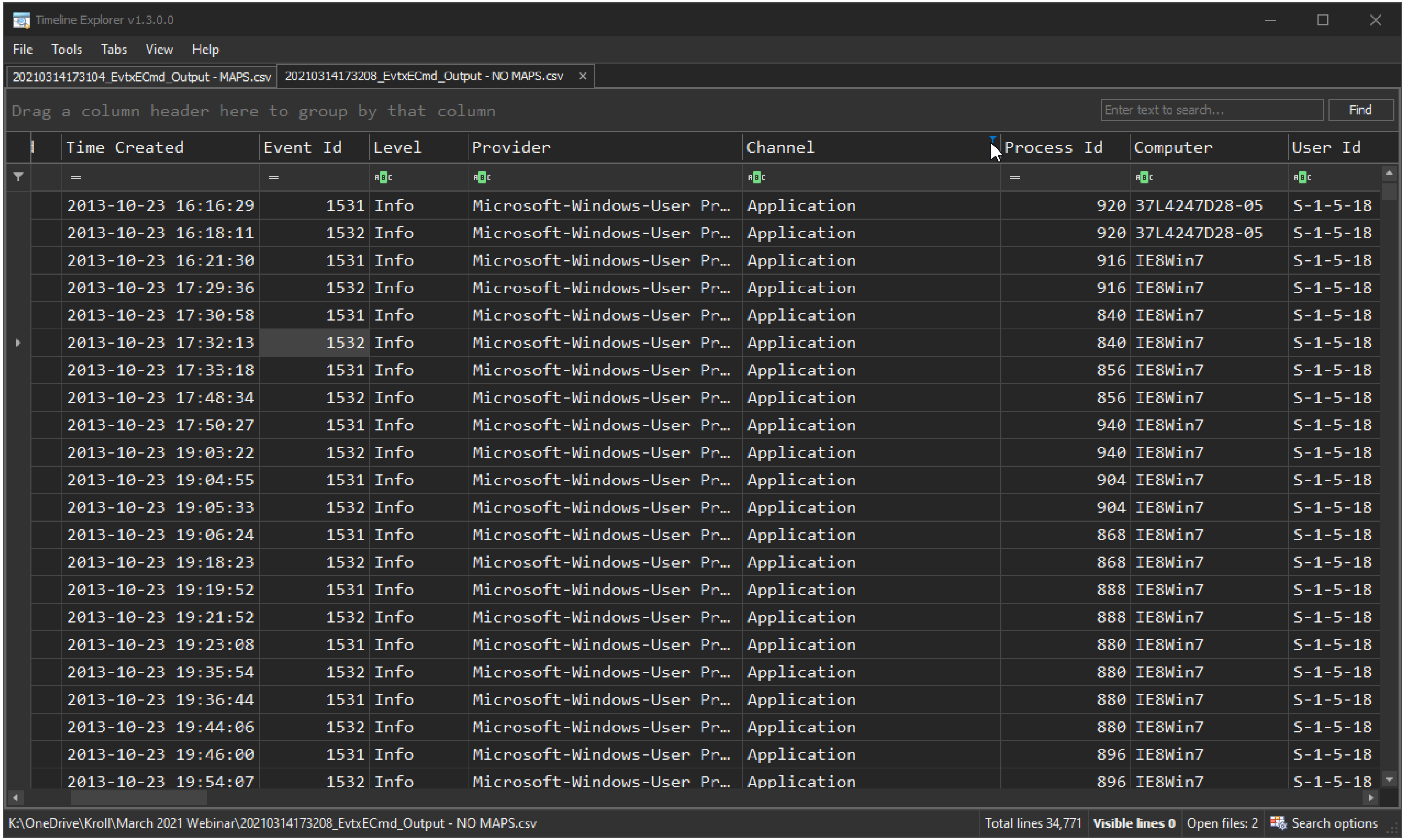


Drag a column header here to group by that column

Provider	Channel	Process Id	Computer
Desktop Window Manager	Application	0	IE8Win7
Desktop Window Manager	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
Microsoft-Windows-Search	Application	0	IE8Win7
Microsoft-Windows-Search	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
ESENT	Application	0	IE8Win7
SecurityCenter	Application	0	IE8Win7
.NET Runtime Optimization…	Application	0	IE8Win7
.NET Runtime Optimization…	Application	0	IE8Win7
.NET Runtime Optimization…	Application	0	IE8Win7
.NET Runtime Optimization…	Application	0	IE8Win7
.NET Runtime Optimization…	Application	0	IE8Win7

Channels May Have Multiple Providers (Application Log)

Column Header filter on Application Channel to display Providers within Application.evtx

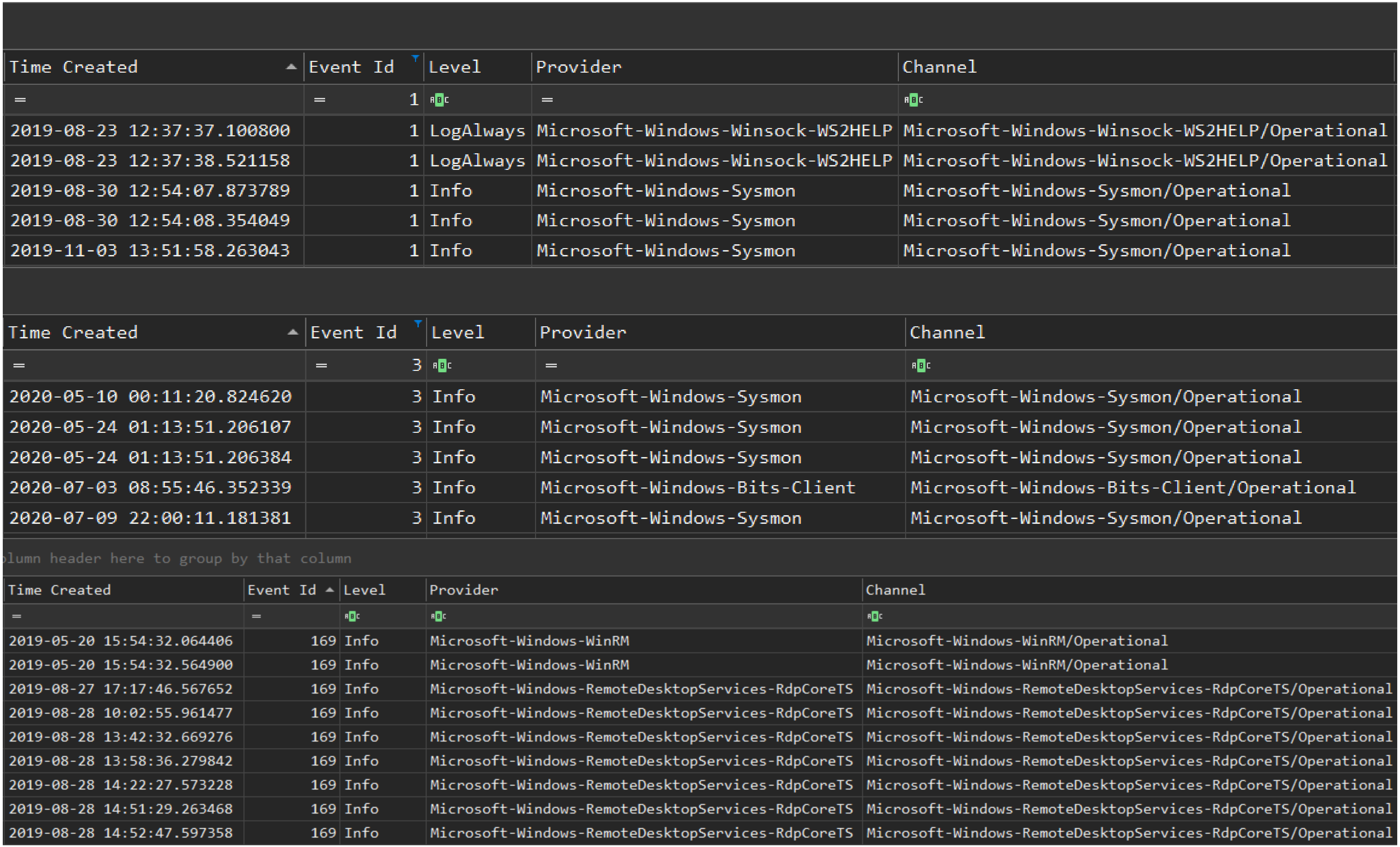

Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
20210314173104_EvtxECmd_Output - MAPS.csv
20210314173208_EvtxECmd_Output - NO MAPS.csv
Drag a column header here to group by that column
Enter text to search...
Find

Time Created	Event Id	Level	Provider	Channel	Process Id	Computer	User Id
2013-10-23 16:16:29	1531	Info	Microsoft-Windows-User Pr...	Application	920	37L4247D28-05	S-1-5-18
2013-10-23 16:18:11	1532	Info	Microsoft-Windows-User Pr...	Application	920	37L4247D28-05	S-1-5-18
2013-10-23 16:21:30	1531	Info	Microsoft-Windows-User Pr...	Application	916	IE8Win7	S-1-5-18
2013-10-23 17:29:36	1532	Info	Microsoft-Windows-User Pr...	Application	916	IE8Win7	S-1-5-18
2013-10-23 17:30:58	1531	Info	Microsoft-Windows-User Pr...	Application	840	IE8Win7	S-1-5-18
2013-10-23 17:32:13	1532	Info	Microsoft-Windows-User Pr...	Application	840	IE8Win7	S-1-5-18
2013-10-23 17:33:18	1531	Info	Microsoft-Windows-User Pr...	Application	856	IE8Win7	S-1-5-18
2013-10-23 17:48:34	1532	Info	Microsoft-Windows-User Pr...	Application	856	IE8Win7	S-1-5-18
2013-10-23 17:50:27	1531	Info	Microsoft-Windows-User Pr...	Application	940	IE8Win7	S-1-5-18
2013-10-23 19:03:22	1532	Info	Microsoft-Windows-User Pr...	Application	940	IE8Win7	S-1-5-18
2013-10-23 19:04:55	1531	Info	Microsoft-Windows-User Pr...	Application	904	IE8Win7	S-1-5-18
2013-10-23 19:05:33	1532	Info	Microsoft-Windows-User Pr...	Application	904	IE8Win7	S-1-5-18
2013-10-23 19:06:24	1531	Info	Microsoft-Windows-User Pr...	Application	868	IE8Win7	S-1-5-18
2013-10-23 19:18:23	1532	Info	Microsoft-Windows-User Pr...	Application	868	IE8Win7	S-1-5-18
2013-10-23 19:19:52	1531	Info	Microsoft-Windows-User Pr...	Application	888	IE8Win7	S-1-5-18
2013-10-23 19:21:52	1532	Info	Microsoft-Windows-User Pr...	Application	888	IE8Win7	S-1-5-18
2013-10-23 19:23:08	1531	Info	Microsoft-Windows-User Pr...	Application	880	IE8Win7	S-1-5-18
2013-10-23 19:35:54	1532	Info	Microsoft-Windows-User Pr...	Application	880	IE8Win7	S-1-5-18
2013-10-23 19:36:44	1531	Info	Microsoft-Windows-User Pr...	Application	880	IE8Win7	S-1-5-18
2013-10-23 19:44:06	1532	Info	Microsoft-Windows-User Pr...	Application	880	IE8Win7	S-1-5-18
2013-10-23 19:46:00	1531	Info	Microsoft-Windows-User Pr...	Application	896	IE8Win7	S-1-5-18
2013-10-23 19:54:07	1532	Info	Microsoft-Windows-User Pr...	Application	896	IE8Win7	S-1-5-18

K:\OneDrive\Kroll\March 2021 Webinar\20210314173208_EvtxECmd_Output - NO MAPS.csv   Total lines 34,771   **Visible lines 0**   Open files: 2   Search options

Examples of Duplicate Event IDs

Different Channel and Provider, but Event ID is identical



Time Created	Event Id	Level	Provider	Channel
=	= 1	ABC	=	ABC
2019-08-23 12:37:37.100800	1	LogAlways	Microsoft-Windows-Winsock-WS2HELP	Microsoft-Windows-Winsock-WS2HELP/Operational
2019-08-23 12:37:38.521158	1	LogAlways	Microsoft-Windows-Winsock-WS2HELP	Microsoft-Windows-Winsock-WS2HELP/Operational
2019-08-30 12:54:07.873789	1	Info	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational
2019-08-30 12:54:08.354049	1	Info	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational
2019-11-03 13:51:58.263043	1	Info	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational

Time Created	Event Id	Level	Provider	Channel
=	= 3	ABC	=	ABC
2020-05-10 00:11:20.824620	3	Info	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational
2020-05-24 01:13:51.206107	3	Info	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational
2020-05-24 01:13:51.206384	3	Info	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational
2020-07-03 08:55:46.352339	3	Info	Microsoft-Windows-Bits-Client	Microsoft-Windows-Bits-Client/Operational
2020-07-09 22:00:11.181381	3	Info	Microsoft-Windows-Sysmon	Microsoft-Windows-Sysmon/Operational

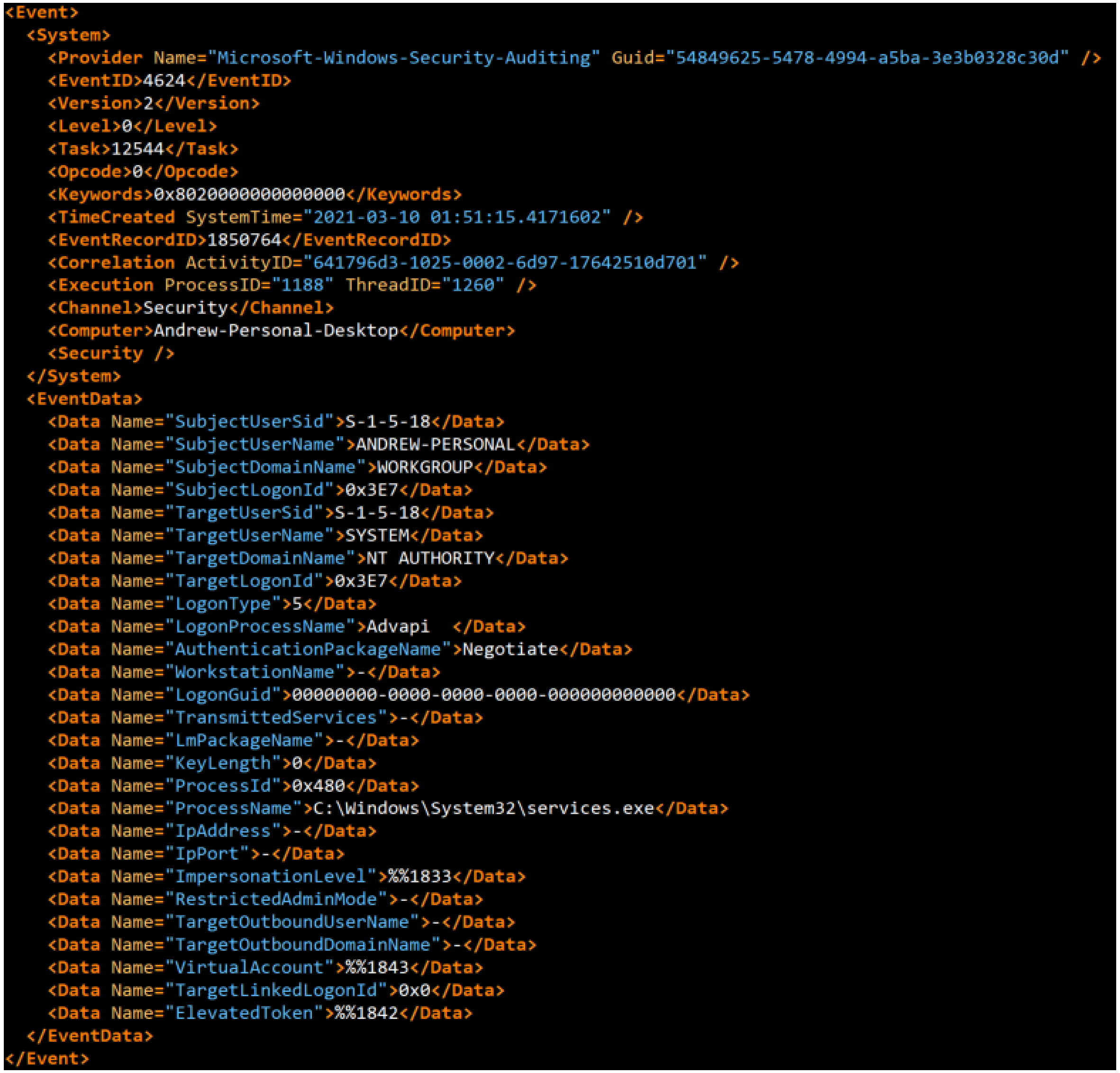
olumn header here to group by that column

Time Created	Event Id	Level	Provider	Channel
=	=	ABC	ABC	ABC
2019-05-20 15:54:32.064406	169	Info	Microsoft-Windows-WinRM	Microsoft-Windows-WinRM/Operational
2019-05-20 15:54:32.564900	169	Info	Microsoft-Windows-WinRM	Microsoft-Windows-WinRM/Operational
2019-08-27 17:17:46.567652	169	Info	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
2019-08-28 10:02:55.961477	169	Info	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
2019-08-28 13:42:32.669276	169	Info	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
2019-08-28 13:58:36.279842	169	Info	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
2019-08-28 14:22:27.573228	169	Info	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
2019-08-28 14:51:29.263468	169	Info	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
2019-08-28 14:52:47.597358	169	Info	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS	Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational

Event Logs are XML files at Heart

evtxecmd.exe --f “C:\path\to\Security.evtx” --xml “C:\output\path, XML output opened in text editor

- Example of what an event looks like in XML format
  - Security:4624
  - An account was successfully logged on
- Each of the Data Name values (blue text) are what can be mapped into various columns that EvtxECmd provides
- All of the data within <EventData> will reside in Payload column regardless of how its mapped within the EvtxECmd Map



```xml
<Event>
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="54849625-5478-4994-a5ba-3e3b0328c30d" />
    <EventID>4624</EventID>
    <Version>2</Version>
    <Level>0</Level>
    <Task>12544</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2021-03-10 01:51:15.4171602" />
    <EventRecordID>1850764</EventRecordID>
    <Correlation ActivityID="641796d3-1025-0002-6d97-17642510d701" />
    <Execution ProcessID="1188" ThreadID="1260" />
    <Channel>Security</Channel>
    <Computer>Andrew-Personal-Desktop</Computer>
    <Security />
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-18</Data>
    <Data Name="SubjectUserName">ANDREW-PERSONAL</Data>
    <Data Name="SubjectDomainName">WORKGROUP</Data>
    <Data Name="SubjectLogonId">0x3E7</Data>
    <Data Name="TargetUserSid">S-1-5-18</Data>
    <Data Name="TargetUserName">SYSTEM</Data>
    <Data Name="TargetDomainName">NT AUTHORITY</Data>
    <Data Name="TargetLogonId">0x3E7</Data>
    <Data Name="LogonType">5</Data>
    <Data Name="LogonProcessName">Advapi  </Data>
    <Data Name="AuthenticationPackageName">Negotiate</Data>
    <Data Name="WorkstationName">-</Data>
    <Data Name="LogonGuid">00000000-0000-0000-0000-000000000000</Data>
    <Data Name="TransmittedServices">-</Data>
    <Data Name="LmPackageName">-</Data>
    <Data Name="KeyLength">0</Data>
    <Data Name="ProcessId">0x480</Data>
    <Data Name="ProcessName">C:\Windows\System32\services.exe</Data>
    <Data Name="IpAddress">-</Data>
    <Data Name="IpPort">-</Data>
    <Data Name="ImpersonationLevel">%%1833</Data>
    <Data Name="RestrictedAdminMode">-</Data>
    <Data Name="TargetOutboundUserName">-</Data>
    <Data Name="TargetOutboundDomainName">-</Data>
    <Data Name="VirtualAccount">%%1843</Data>
    <Data Name="TargetLinkedLogonId">0x0</Data>
    <Data Name="ElevatedToken">%%1842</Data>
  </EventData>
</Event>
```

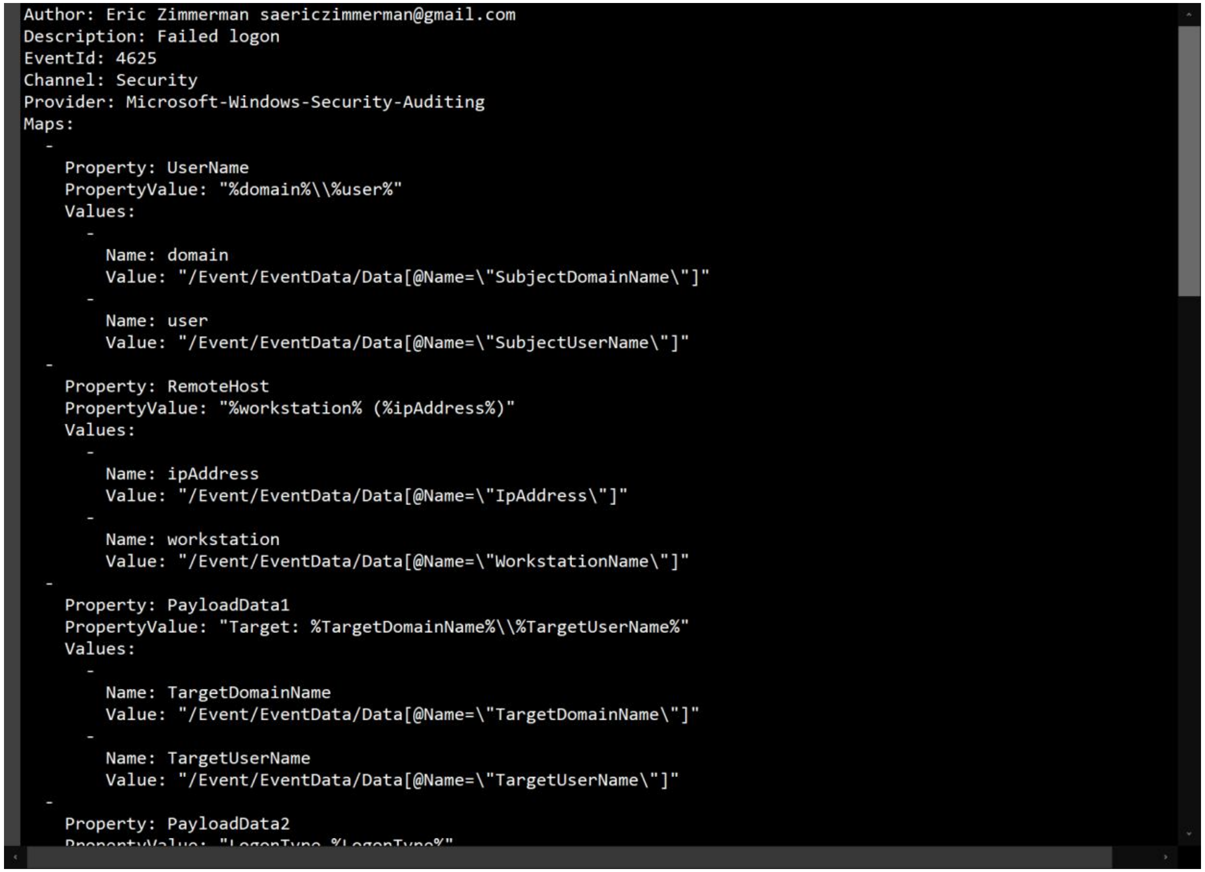
Parsing with EvtxECmd/KAPE

Using KAPE Modules/EvtxECmd Maps

The Secret Sauce - Maps

Security:4625 Map for Failed Logon event

- Maps are used by EvtxECmd to extract data from parsed event logs and display the data into an easily digestible format within various columns
- 329 Maps as of 3/28/2021
- Text files (.map) in YAML
- Parsing for event data utilizes XPath queries
- Populates Map Description, UserName, RemoteHost PayloadData1-6, and ExecutableInfo columns
- Anyone can make them!
- Ideally, the most useful events would be mapped, not EVERY event in existence
- Really cool features like Lookups and Regex

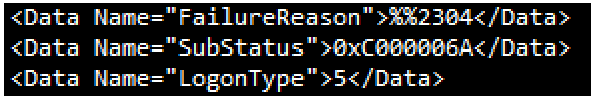


```
Author: Eric Zimmerman saericzimmerman@gmail.com
Description: Failed logon
EventId: 4625
Channel: Security
Provider: Microsoft-Windows-Security-Auditing
Maps:
  -
    Property: UserName
    PropertyValue: "%domain%\\%user%"
    Values:
      -
        Name: domain
        Value: "/Event/EventData/Data[@Name=\"SubjectDomainName\"]"
      -
        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%"
```

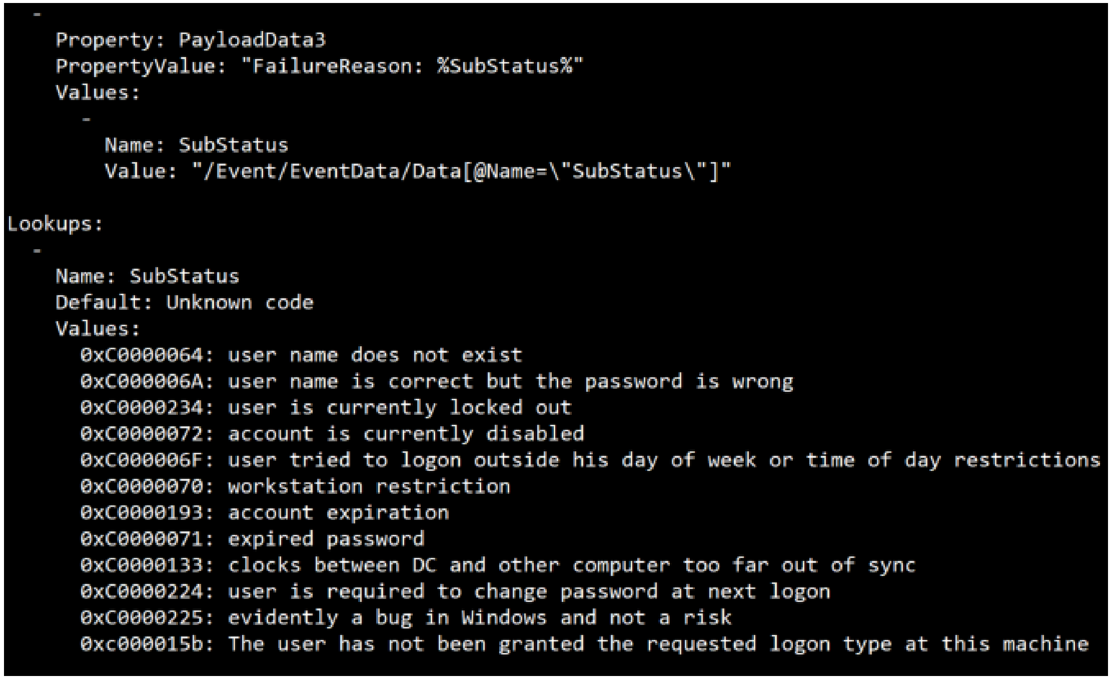
Lookup Tables Example

Breakdown on next slide

- Not all data logged in an event log is human readable!
- Security:4625
  - Failed logon
- Example (PayloadData3):
  - <"SubStatus">0xC000006A</Data>
  - EvtxECmd would substitute the value with the human readable string, and output as “FailureReason: %SubStatus%:” for the PropertyValue
  - FailureReason: user name is correct but the password is wrong



```
<Data Name="FailureReason">%%2304</Data>
<Data Name="SubStatus">0xC000006A</Data>
<Data Name="LogonType">5</Data>
```

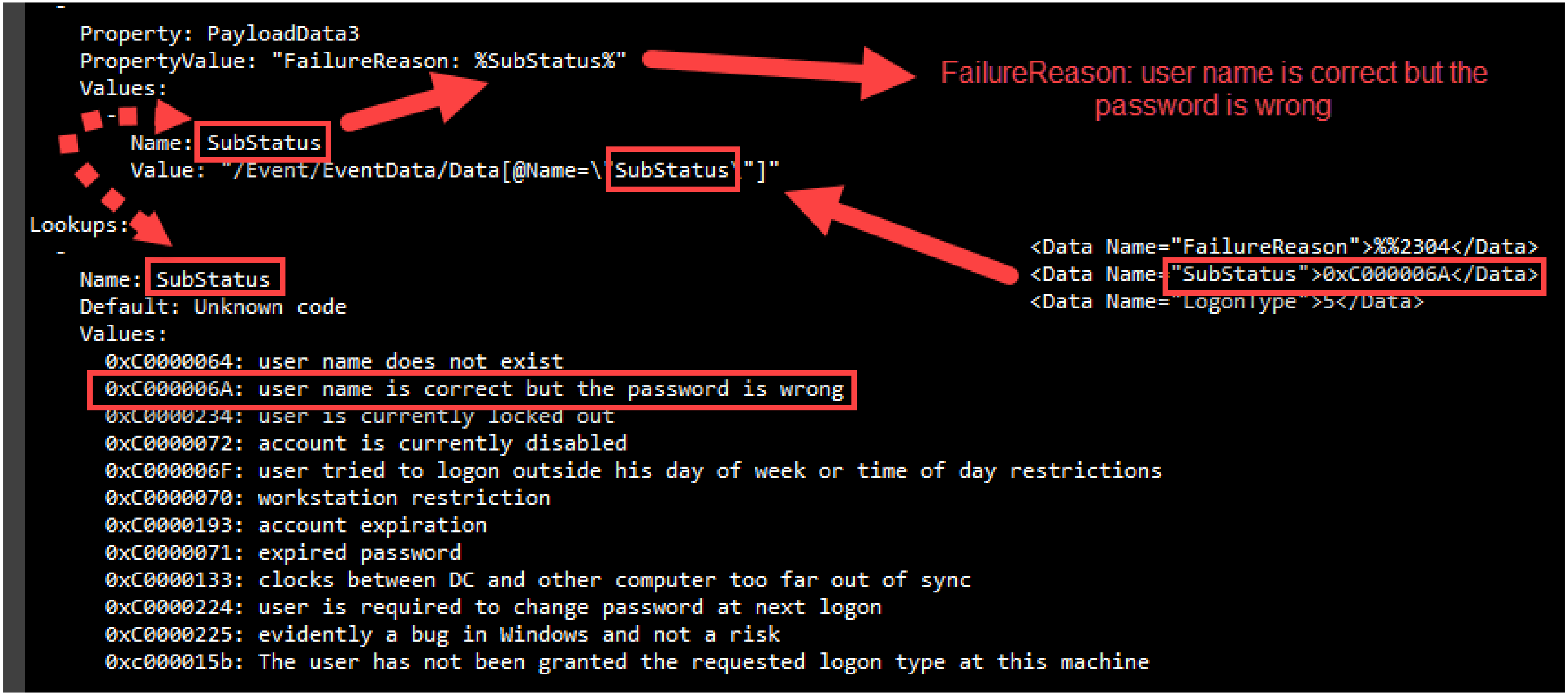


```
  -
    Property: PayloadData3
    PropertyValue: "FailureReason: %SubStatus%"
    Values:
      -
        Name: SubStatus
        Value: "/Event/EventData/Data[@Name=\"SubStatus\"]"

Lookups:
  -
    Name: SubStatus
    Default: Unknown code
    Values:
      0xC0000064: user name does not exist
      0xC000006A: user name is correct but the password is wrong
      0xC0000234: user is currently locked out
      0xC0000072: account is currently disabled
      0xC000006F: user tried to logon outside his day of week or time of day restrictions
      0xC0000070: workstation restriction
      0xC0000193: account expiration
      0xC0000071: expired password
      0xC0000133: clocks between DC and other computer too far out of sync
      0xC0000224: user is required to change password at next logon
      0xC0000225: evidently a bug in Windows and not a risk
      0xc000015b: The user has not been granted the requested logon type at this machine
```

Lookup Table Breakdown

XML Value mapped to Map Value, translated via Lookup Table, mapped to PropertyValue for CSV



```
  -
    Property: PayloadData3
    PropertyValue: "FailureReason: %SubStatus%"
    Values:
      -
        Name: SubStatus
        Value: "/Event/EventData/Data[@Name=\"SubStatus\"]"
Lookups:
  -
    Name: SubStatus
    Default: Unknown code
    Values:
      0xC0000064: user name does not exist
      0xC000006A: user name is correct but the password is wrong
      0xC0000234: user is currently locked out
      0xC0000072: account is currently disabled
      0xC000006F: user tried to logon outside his day of week or time of day restrictions
      0xC0000070: workstation restriction
      0xC0000193: account expiration
      0xC0000071: expired password
      0xC0000133: clocks between DC and other computer too far out of sync
      0xC0000224: user is required to change password at next logon
      0xC0000225: evidently a bug in Windows and not a risk
      0xc000015b: The user has not been granted the requested logon type at this machine
```

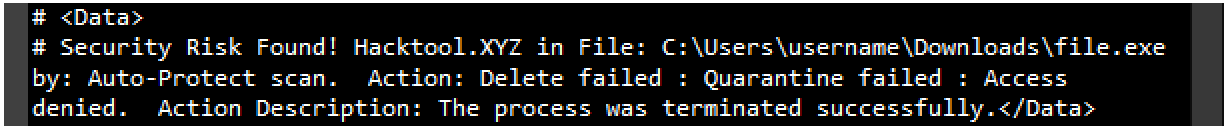
FailureReason: user name is correct but the password is wrong

```
<Data Name="FailureReason">%%2304</Data>
<Data Name="SubStatus">0xC000006A</Data>
<Data Name="LogonType">5</Data>
```

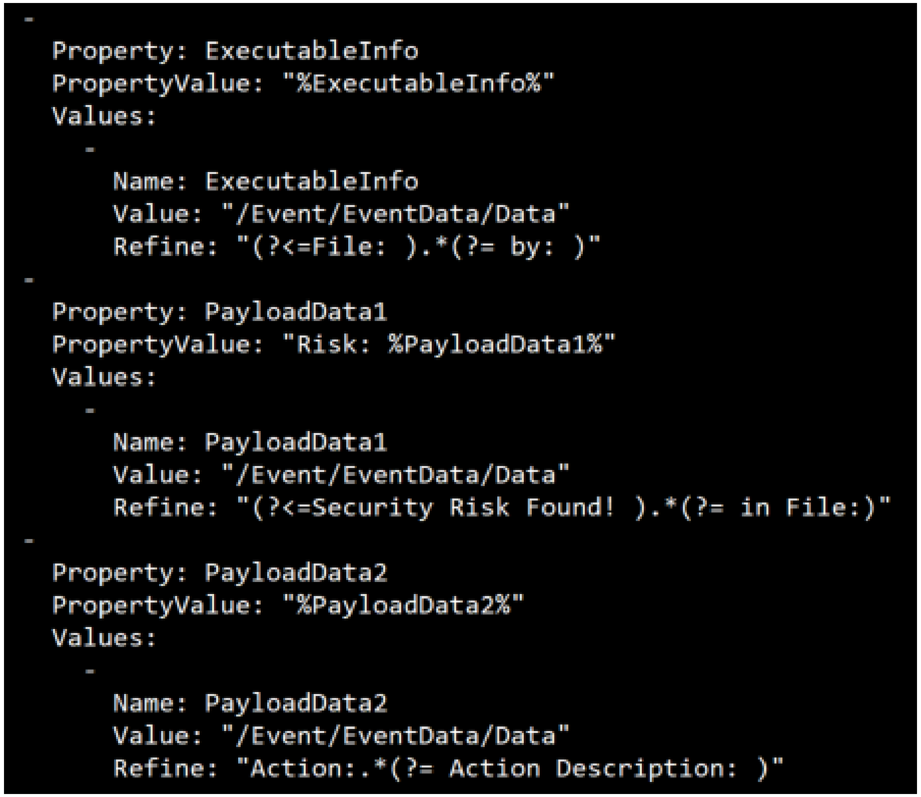
Regex Example

Using Regular Expressions to split up a large blob of event log data

- Symantec:51
  - Security Risk Found
- Example Symantec:51 Event:
  - </Data>Security Risk Found! Hacktool.XYZ in File: C:\Users\username\Downloads\file.exe by: Auto-Protect scan. Action: Delete failed : Quarantine failed : Access denied. Action Description: The process was terminated successfully.</Data>
  - EvtxECmd would substitute the value with the human readable string, and output as “Risk: %PayloadData1% for the PropertyValue, i.e.
    - PayloadData1 - Security Risk Found! Hacktool.XYZ
    - PayloadData2 - The process was terminated successfully.
    - ExecutableInfo - File: C:\Users\username\Downloads\file.exe
    - And so on…



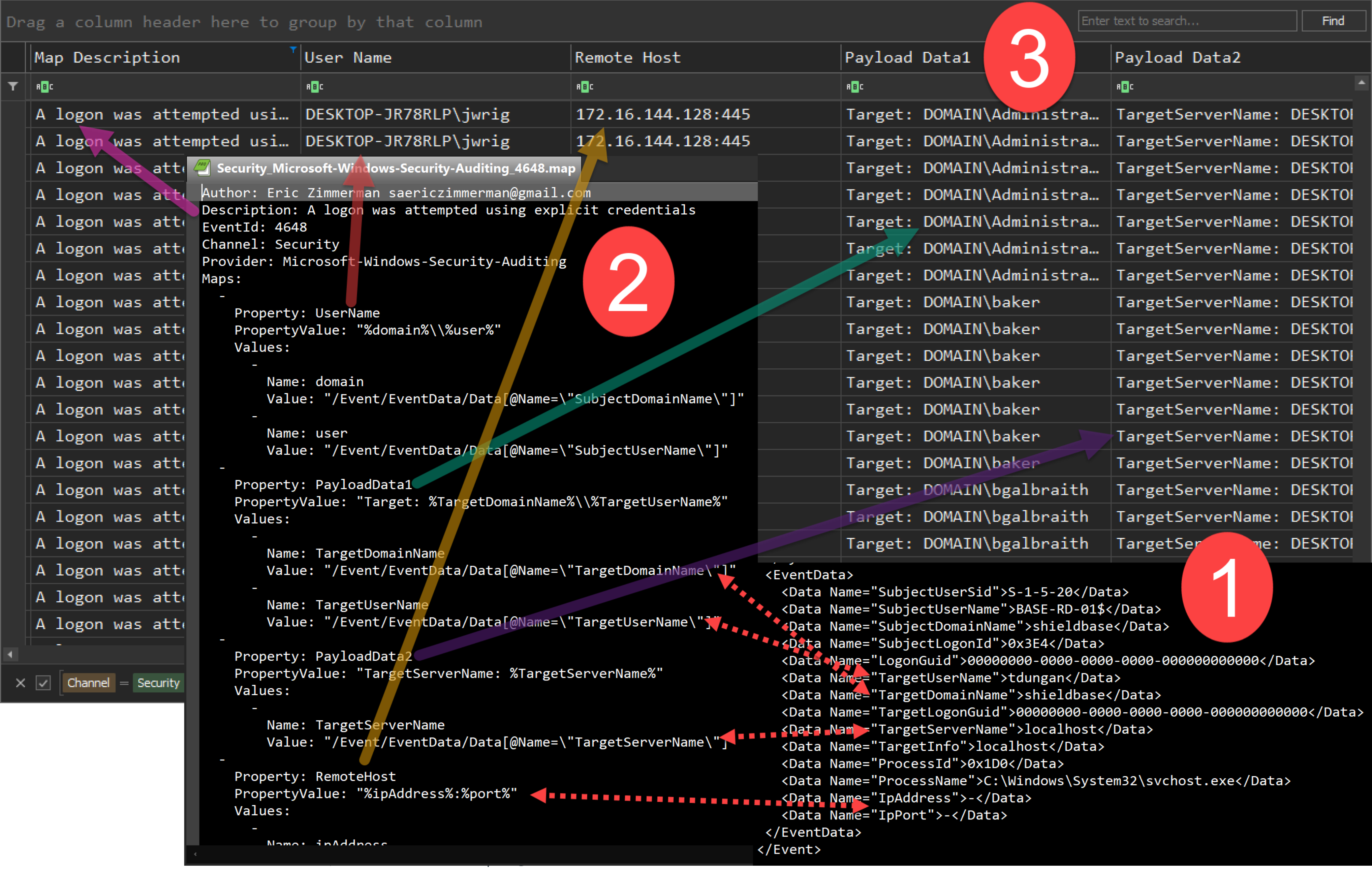
```
# <Data>
# Security Risk Found! Hacktool.XYZ in File: C:\Users\username\Downloads\file.exe
by: Auto-Protect scan.  Action: Delete failed : Quarantine failed : Access
denied.  Action Description: The process was terminated successfully.</Data>
```



```
-
  Property: ExecutableInfo
  PropertyValue: "%ExecutableInfo%"
  Values:
    -
      Name: ExecutableInfo
      Value: "/Event/EventData/Data"
      Refine: "(?<=File: ).*(?= by: )"
-
  Property: PayloadData1
  PropertyValue: "Risk: %PayloadData1%"
  Values:
    -
      Name: PayloadData1
      Value: "/Event/EventData/Data"
      Refine: "(?<=Security Risk Found! ).*(?= in File:)"
-
  Property: PayloadData2
  PropertyValue: "%PayloadData2%"
  Values:
    -
      Name: PayloadData2
      Value: "/Event/EventData/Data"
      Refine: "Action:.*(?= Action Description: )"
```

How do Maps influence CSV Output?

Breakdown on next slide



Map Description	User Name	Remote Host	Payload Data1	Payload Data2
A logon was attempted usi…	DESKTOP-JR78RLP\jwrig	172.16.144.128:445	Target: DOMAIN\Administra…	TargetServerName: DESKTOI
A logon was attempted usi…	DESKTOP-JR78RLP\jwrig	172.16.144.128:445	Target: DOMAIN\Administra…	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\Administra…	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\Administra…	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\Administra…	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\Administra…	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\Administra…	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\baker	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\baker	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\baker	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\baker	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\baker	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\baker	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\baker	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\bgalbraith	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\bgalbraith	TargetServerName: DESKTOI
A logon was att			Target: DOMAIN\bgalbraith	TargetServerName: DESKTOI
A logon was att				
A logon was att				
A logon was att				

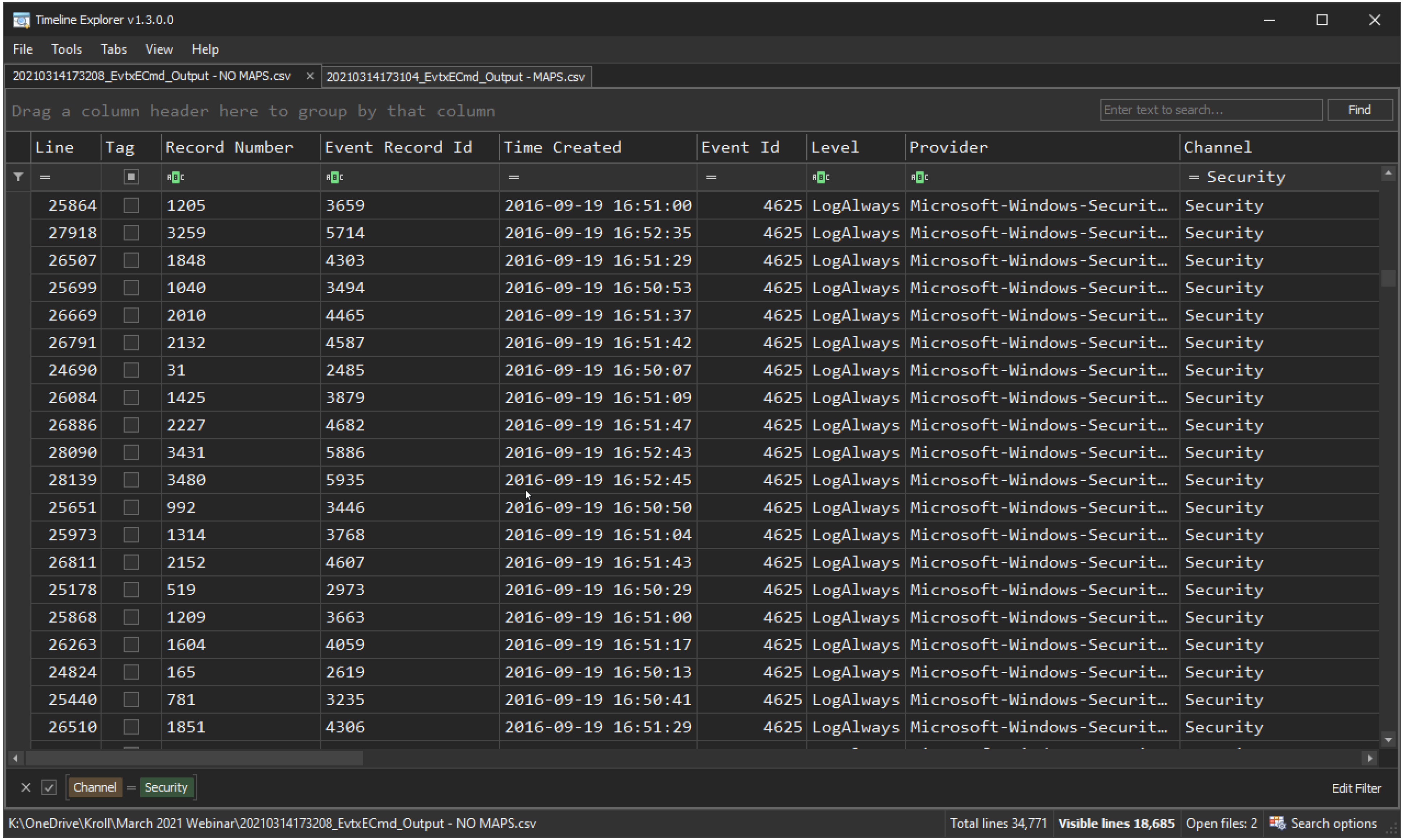
Security_Microsoft-Windows-Security-Auditing_4648.map

```
Author: Eric Zimmerman saericzimmerman@gmail.com
Description: A logon was attempted using explicit credentials
EventId: 4648
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: 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: "TargetServerName: %TargetServerName%"
    Values:
      -
        Name: TargetServerName
        Value: "/Event/EventData/Data[@Name=\"TargetServerName\"]"
  -
    Property: RemoteHost
    PropertyValue: "%ipAddress%:%port%"
    Values:
      -
        Name: ipAddress
```

```
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-20</Data>
    <Data Name="SubjectUserName">BASE-RD-01$</Data>
    <Data Name="SubjectDomainName">shieldbase</Data>
    <Data Name="SubjectLogonId">0x3E4</Data>
    <Data Name="LogonGuid">00000000-0000-0000-0000-000000000000</Data>
    <Data Name="TargetUserName">tdungan</Data>
    <Data Name="TargetDomainName">shieldbase</Data>
    <Data Name="TargetLogonGuid">00000000-0000-0000-0000-000000000000</Data>
    <Data Name="TargetServerName">localhost</Data>
    <Data Name="TargetInfo">localhost</Data>
    <Data Name="ProcessId">0x1D0</Data>
    <Data Name="ProcessName">C:\Windows\System32\svchost.exe</Data>
    <Data Name="IpAddress">-</Data>
    <Data Name="IpPort">-</Data>
  </EventData>
</Event>
```

Event Log Analysis without Maps

Notice how the columns aren’t populated from Map Description onward



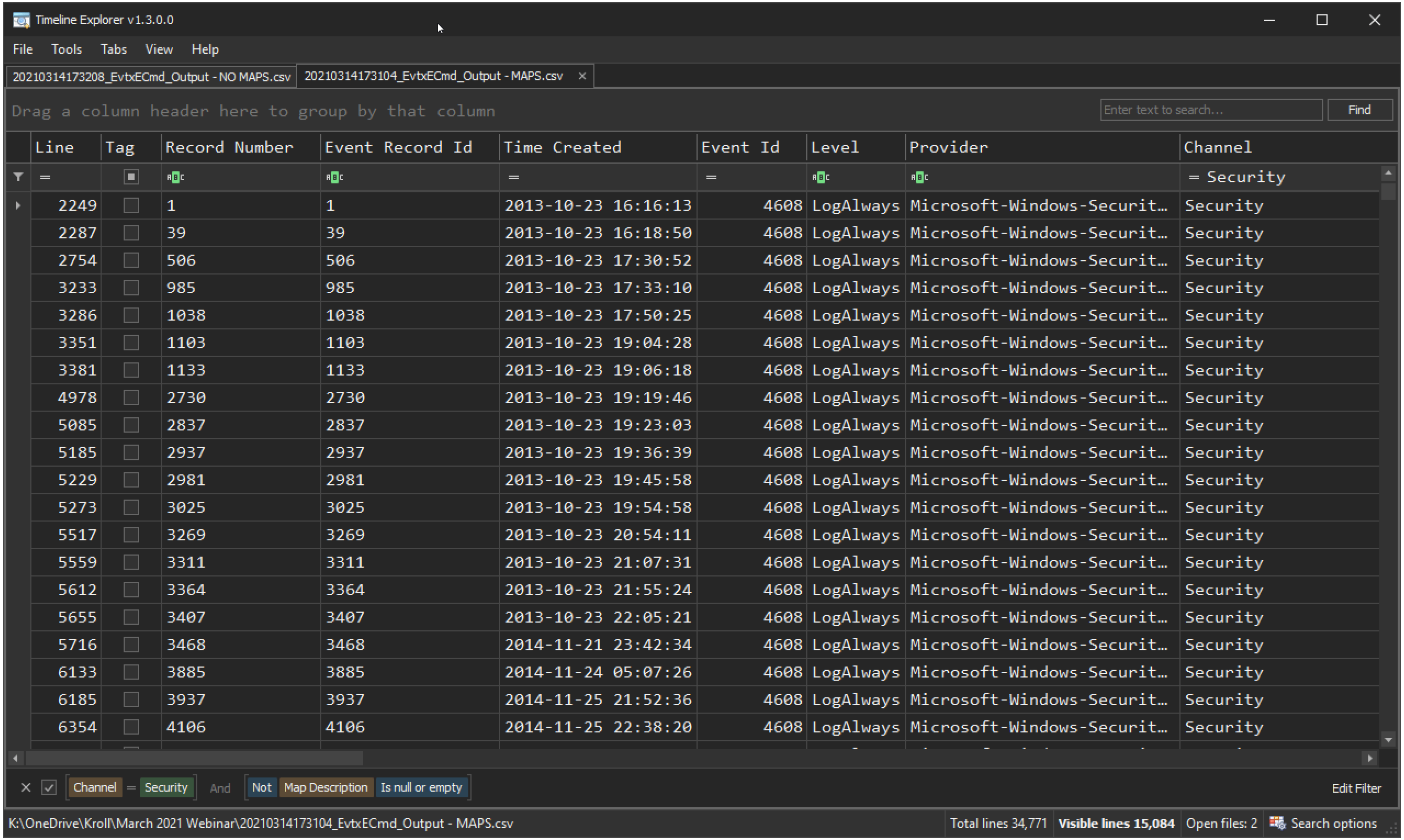
Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
20210314173208_EvtxECmd_Output - NO MAPS.csv
20210314173104_EvtxECmd_Output - MAPS.csv
Drag a column header here to group by that column
Enter text to search...
Find

Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel
=	■	ABC	ABC	=	=	ABC	ABC	= Security
25864	□	1205	3659	2016-09-19 16:51:00	4625	LogAlways	Microsoft-Windows-Securit...	Security
27918	□	3259	5714	2016-09-19 16:52:35	4625	LogAlways	Microsoft-Windows-Securit...	Security
26507	□	1848	4303	2016-09-19 16:51:29	4625	LogAlways	Microsoft-Windows-Securit...	Security
25699	□	1040	3494	2016-09-19 16:50:53	4625	LogAlways	Microsoft-Windows-Securit...	Security
26669	□	2010	4465	2016-09-19 16:51:37	4625	LogAlways	Microsoft-Windows-Securit...	Security
26791	□	2132	4587	2016-09-19 16:51:42	4625	LogAlways	Microsoft-Windows-Securit...	Security
24690	□	31	2485	2016-09-19 16:50:07	4625	LogAlways	Microsoft-Windows-Securit...	Security
26084	□	1425	3879	2016-09-19 16:51:09	4625	LogAlways	Microsoft-Windows-Securit...	Security
26886	□	2227	4682	2016-09-19 16:51:47	4625	LogAlways	Microsoft-Windows-Securit...	Security
28090	□	3431	5886	2016-09-19 16:52:43	4625	LogAlways	Microsoft-Windows-Securit...	Security
28139	□	3480	5935	2016-09-19 16:52:45	4625	LogAlways	Microsoft-Windows-Securit...	Security
25651	□	992	3446	2016-09-19 16:50:50	4625	LogAlways	Microsoft-Windows-Securit...	Security
25973	□	1314	3768	2016-09-19 16:51:04	4625	LogAlways	Microsoft-Windows-Securit...	Security
26811	□	2152	4607	2016-09-19 16:51:43	4625	LogAlways	Microsoft-Windows-Securit...	Security
25178	□	519	2973	2016-09-19 16:50:29	4625	LogAlways	Microsoft-Windows-Securit...	Security
25868	□	1209	3663	2016-09-19 16:51:00	4625	LogAlways	Microsoft-Windows-Securit...	Security
26263	□	1604	4059	2016-09-19 16:51:17	4625	LogAlways	Microsoft-Windows-Securit...	Security
24824	□	165	2619	2016-09-19 16:50:13	4625	LogAlways	Microsoft-Windows-Securit...	Security
25440	□	781	3235	2016-09-19 16:50:41	4625	LogAlways	Microsoft-Windows-Securit...	Security
26510	□	1851	4306	2016-09-19 16:51:29	4625	LogAlways	Microsoft-Windows-Securit...	Security

K:\OneDrive\Kroll\March 2021 Webinar\20210314173208_EvtxECmd_Output - NO MAPS.csv | Total lines 34,771 | **Visible lines 18,685** | Open files: 2 | Search options

Event Log Analysis with Maps

Notice how the columns contain data parsed from each event



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

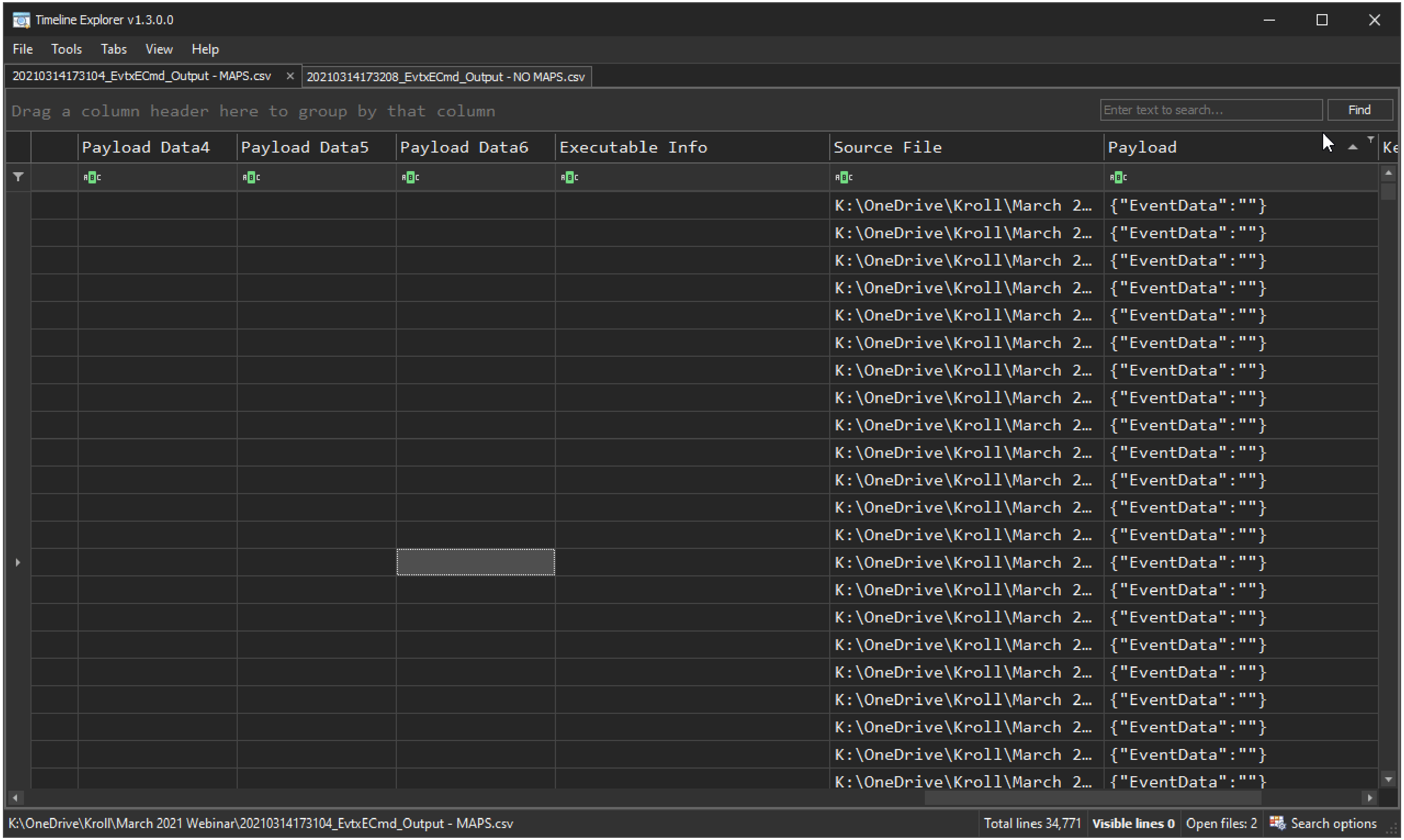
Line	Tag	Record Number	Event Record Id	Time Created	Event Id	Level	Provider	Channel
=	■	ABC	ABC	=	=	ABC	ABC	= Security
2249	□	1	1	2013-10-23 16:16:13	4608	LogAlways	Microsoft-Windows-Securit...	Security
2287	□	39	39	2013-10-23 16:18:50	4608	LogAlways	Microsoft-Windows-Securit...	Security
2754	□	506	506	2013-10-23 17:30:52	4608	LogAlways	Microsoft-Windows-Securit...	Security
3233	□	985	985	2013-10-23 17:33:10	4608	LogAlways	Microsoft-Windows-Securit...	Security
3286	□	1038	1038	2013-10-23 17:50:25	4608	LogAlways	Microsoft-Windows-Securit...	Security
3351	□	1103	1103	2013-10-23 19:04:28	4608	LogAlways	Microsoft-Windows-Securit...	Security
3381	□	1133	1133	2013-10-23 19:06:18	4608	LogAlways	Microsoft-Windows-Securit...	Security
4978	□	2730	2730	2013-10-23 19:19:46	4608	LogAlways	Microsoft-Windows-Securit...	Security
5085	□	2837	2837	2013-10-23 19:23:03	4608	LogAlways	Microsoft-Windows-Securit...	Security
5185	□	2937	2937	2013-10-23 19:36:39	4608	LogAlways	Microsoft-Windows-Securit...	Security
5229	□	2981	2981	2013-10-23 19:45:58	4608	LogAlways	Microsoft-Windows-Securit...	Security
5273	□	3025	3025	2013-10-23 19:54:58	4608	LogAlways	Microsoft-Windows-Securit...	Security
5517	□	3269	3269	2013-10-23 20:54:11	4608	LogAlways	Microsoft-Windows-Securit...	Security
5559	□	3311	3311	2013-10-23 21:07:31	4608	LogAlways	Microsoft-Windows-Securit...	Security
5612	□	3364	3364	2013-10-23 21:55:24	4608	LogAlways	Microsoft-Windows-Securit...	Security
5655	□	3407	3407	2013-10-23 22:05:21	4608	LogAlways	Microsoft-Windows-Securit...	Security
5716	□	3468	3468	2014-11-21 23:42:34	4608	LogAlways	Microsoft-Windows-Securit...	Security
6133	□	3885	3885	2014-11-24 05:07:26	4608	LogAlways	Microsoft-Windows-Securit...	Security
6185	□	3937	3937	2014-11-25 21:52:36	4608	LogAlways	Microsoft-Windows-Securit...	Security
6354	□	4106	4106	2014-11-25 22:38:20	4608	LogAlways	Microsoft-Windows-Securit...	Security

☑ Channel = Security And Not Map Description Is null or empty

K:\OneDrive\Kroll\March 2021 Webinar\20210314173104_EvtxECmd_Output - MAPS.csv | Total lines 34,771 | Visible lines 15,084 | Open files: 2 | Search options

Don’t forget about the Payload Column

Regardless of how data is mapped, the entirety of an event’s data can be found in Payload



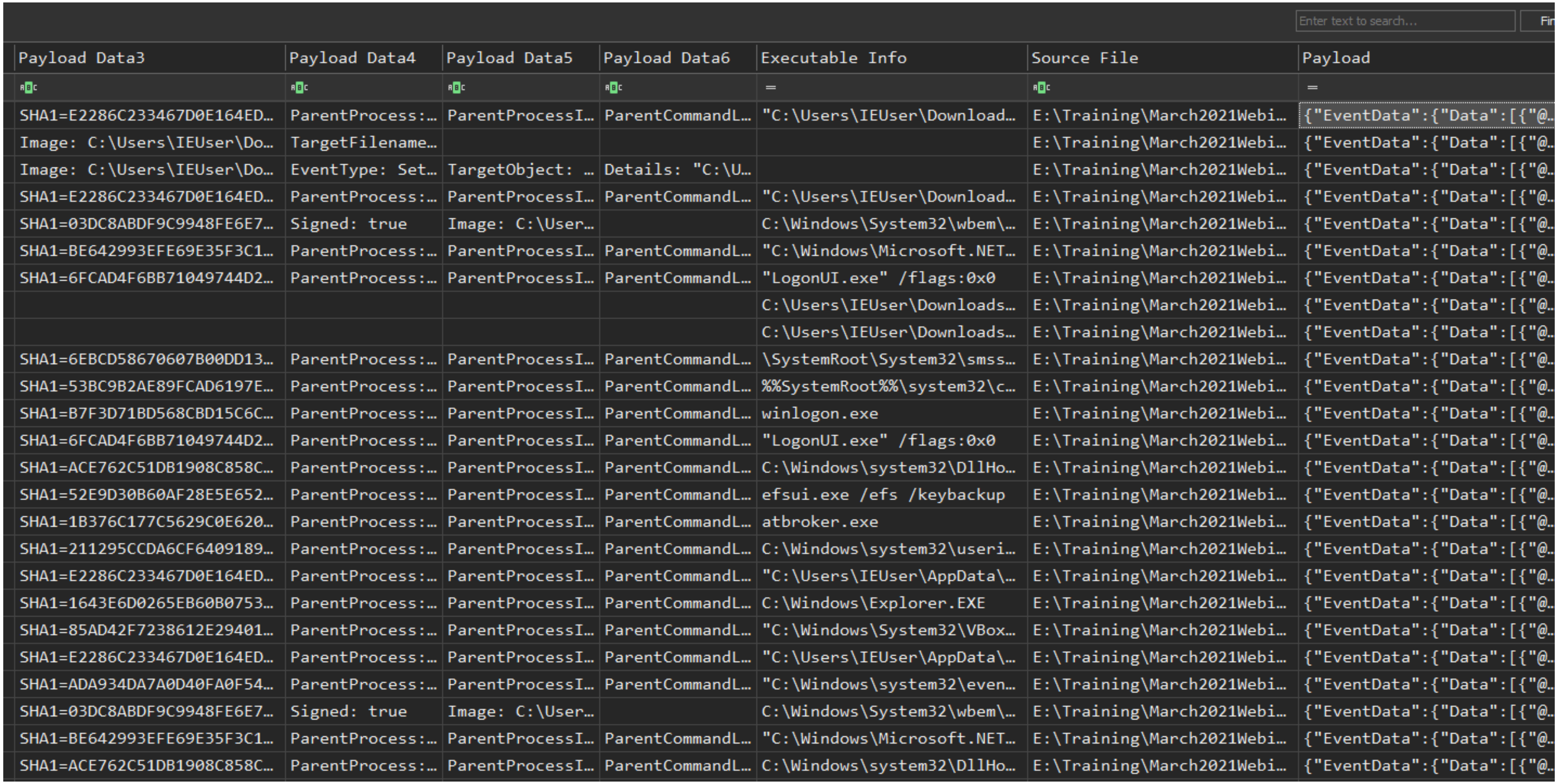
Timeline Explorer v1.3.0.0
File
Tools
Tabs
View
Help
20210314173104_EvtxECmd_Output - MAPS.csv
20210314173208_EvtxECmd_Output - NO MAPS.csv
Drag a column header here to group by that column
Enter text to search...
Find

Payload Data4	Payload Data5	Payload Data6	Executable Info	Source File	Payload	Ke
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	
				K:\OneDrive\Kroll\March 2…	{"EventData":""}	

K:\OneDrive\Kroll\March 2021 Webinar\20210314173104_EvtxECmd_Output - MAPS.csv | Total lines 34,771 | **Visible lines 0** | Open files: 2 | Search options

Formatting the Payload Column – Timeline Explorer

Double click on Cell in Payload Column, Format, and see formatted Event Log data

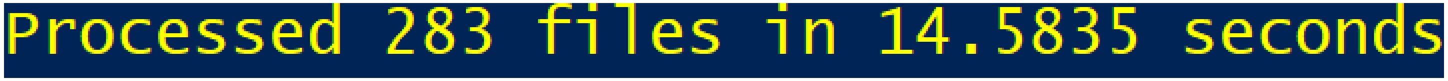


Payload Data3	Payload Data4	Payload Data5	Payload Data6	Executable Info	Source File	Payload
ABC	ABC	ABC	ABC	=	ABC	=
SHA1=E2286C233467D0E164ED…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Users\IEUser\Download…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
Image: C:\Users\IEUser\Do…	TargetFilename…				E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
Image: C:\Users\IEUser\Do…	EventType: Set…	TargetObject: …	Details: "C:\U…		E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=E2286C233467D0E164ED…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Users\IEUser\Download…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=03DC8ABDF9C9948FE6E7…	Signed: true	Image: C:\User…		C:\Windows\System32\wbem\…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=BE642993EFE69E35F3C1…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Windows\Microsoft.NET…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=6FCAD4F6BB71049744D2…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"LogonUI.exe" /flags:0x0	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
				C:\Users\IEUser\Downloads…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
				C:\Users\IEUser\Downloads…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=6EBCD58670607B00DD13…	ParentProcess:…	ParentProcessI…	ParentCommandL…	\SystemRoot\System32\smss…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=53BC9B2AE89FCAD6197E…	ParentProcess:…	ParentProcessI…	ParentCommandL…	%%SystemRoot%%\system32\c…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=B7F3D71BD568CBD15C6C…	ParentProcess:…	ParentProcessI…	ParentCommandL…	winlogon.exe	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=6FCAD4F6BB71049744D2…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"LogonUI.exe" /flags:0x0	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=ACE762C51DB1908C858C…	ParentProcess:…	ParentProcessI…	ParentCommandL…	C:\Windows\system32\DllHo…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=52E9D30B60AF28E5E652…	ParentProcess:…	ParentProcessI…	ParentCommandL…	efsui.exe /efs /keybackup	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=1B376C177C5629C0E620…	ParentProcess:…	ParentProcessI…	ParentCommandL…	atbroker.exe	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=211295CCDA6CF6409189…	ParentProcess:…	ParentProcessI…	ParentCommandL…	C:\Windows\system32\useri…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=E2286C233467D0E164ED…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Users\IEUser\AppData\…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=1643E6D0265EB60B0753…	ParentProcess:…	ParentProcessI…	ParentCommandL…	C:\Windows\Explorer.EXE	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=85AD42F7238612E29401…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Windows\System32\VBox…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=E2286C233467D0E164ED…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Users\IEUser\AppData\…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=ADA934DA7A0D40FA0F54…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Windows\system32\even…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=03DC8ABDF9C9948FE6E7…	Signed: true	Image: C:\User…		C:\Windows\System32\wbem\…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=BE642993EFE69E35F3C1…	ParentProcess:…	ParentProcessI…	ParentCommandL…	"C:\Windows\Microsoft.NET…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…
SHA1=ACE762C51DB1908C858C…	ParentProcess:…	ParentProcessI…	ParentCommandL…	C:\Windows\system32\DllHo…	E:\Training\March2021Webi…	{"EventData":{"Data":[{"@…

Statistics

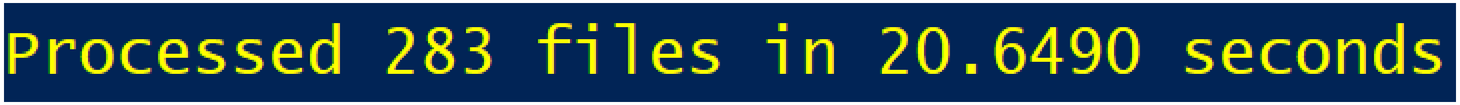
Measuring results of parsing Event Logs with and without Maps

- Elapsed time to parse without Maps (deleted Maps folder prior to parsing)



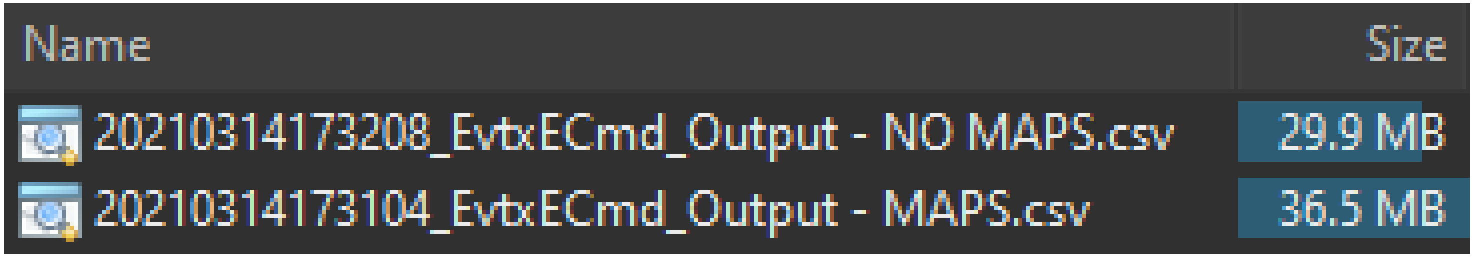
```
Processed 283 files in 14.5835 seconds
```

- Elapsed time to parse with Maps (synced with GitHub prior to parsing)



```
Processed 283 files in 20.6490 seconds
```

- 6mb larger of CSV with Maps



Name	Size
20210314173208_EvtxECmd_Output - NO MAPS.csv	29.9 MB
20210314173104_EvtxECmd_Output - MAPS.csv	36.5 MB

- Worth the extra time/file size for the quick wins

Creating Maps for EvtxECmd

Guide, Template, Text Editor

Creating Maps

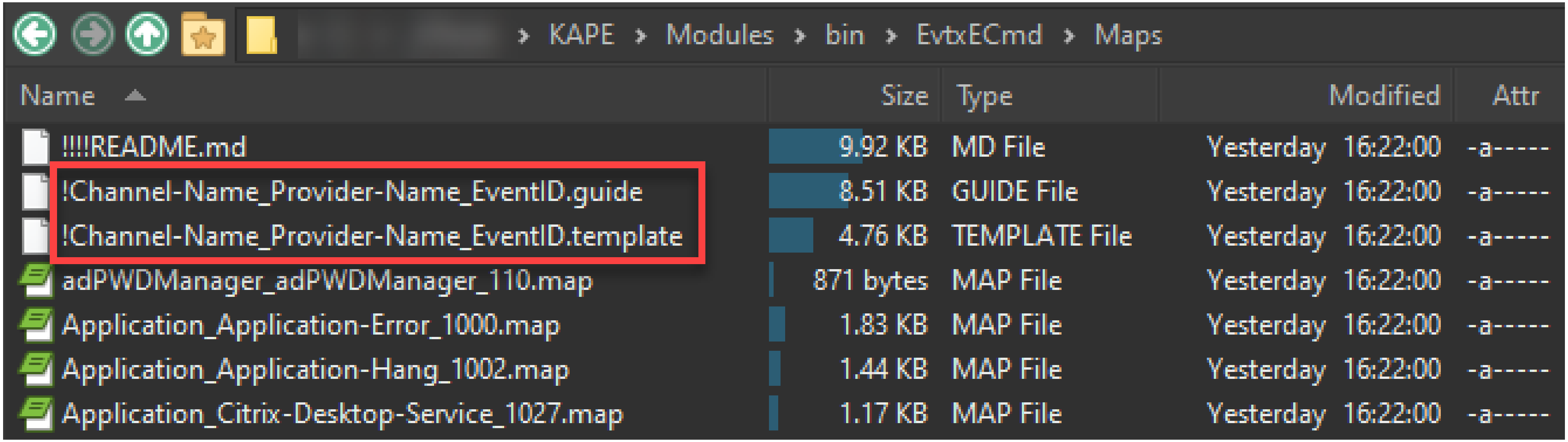
The first one is the hardest

- Follow the Guide and Template provided in the EvtxECmd folder
  - .\KAPE\Modules\bin\EvtxECmd\Maps\**!Channel-Name_Provider-Name_EventID.guide**
  - .\KAPE\Modules\bin\EvtxECmd\Maps\**!Channel-Name_Provider-Name_EventID.template**
- KapeResearch Modules automate .EVTX -> XML conversion
  - **KapeResearch_EventLogs.mkape** automates parsing to XML format
    - Evtxecmd.exe –f “C:\path\to\event\log\here.evtx” –xml “C:\output\path”
- Use your text editor of choice and GitHub Desktop or an alternative Git solution
- If possible, use a Map from a similar Channel or Provider as a starting point
  - For example, if you’re making a Map for a Security event, then copy and rename a preexisting Security Map as a template and modify it as needed
- Channel, Provider, and EventID must match what is in the XML
- Trial and error to make sure data is mapping correctly in CSV output
- Example event data should be included in every Map for everyone’s benefit
- Document your findings when creating Maps!

EvtxECmd Map Guide and Template

Located in .\KAPE\Modules\bin\EvtxECmd\Maps

- Can be opened with any text editor or viewed on GitHub



[redacted] › KAPE › Modules › bin › EvtxECmd › Maps

Name	Size	Type	Modified	Attr
!!!!README.md	9.92 KB	MD File	Yesterday 16:22:00	-a-----
!Channel-Name_Provider-Name_EventID.guide	8.51 KB	GUIDE File	Yesterday 16:22:00	-a-----
!Channel-Name_Provider-Name_EventID.template	4.76 KB	TEMPLATE File	Yesterday 16:22:00	-a-----
adPWDManager_adPWDManager_110.map	871 bytes	MAP File	Yesterday 16:22:00	-a-----
Application_Application-Error_1000.map	1.83 KB	MAP File	Yesterday 16:22:00	-a-----
Application_Application-Hang_1002.map	1.44 KB	MAP File	Yesterday 16:22:00	-a-----
Application_Citrix-Desktop-Service_1027.map	1.17 KB	MAP File	Yesterday 16:22:00	-a-----

Keeping EvtxECmd Maps Updated

Sync for new Maps with Github

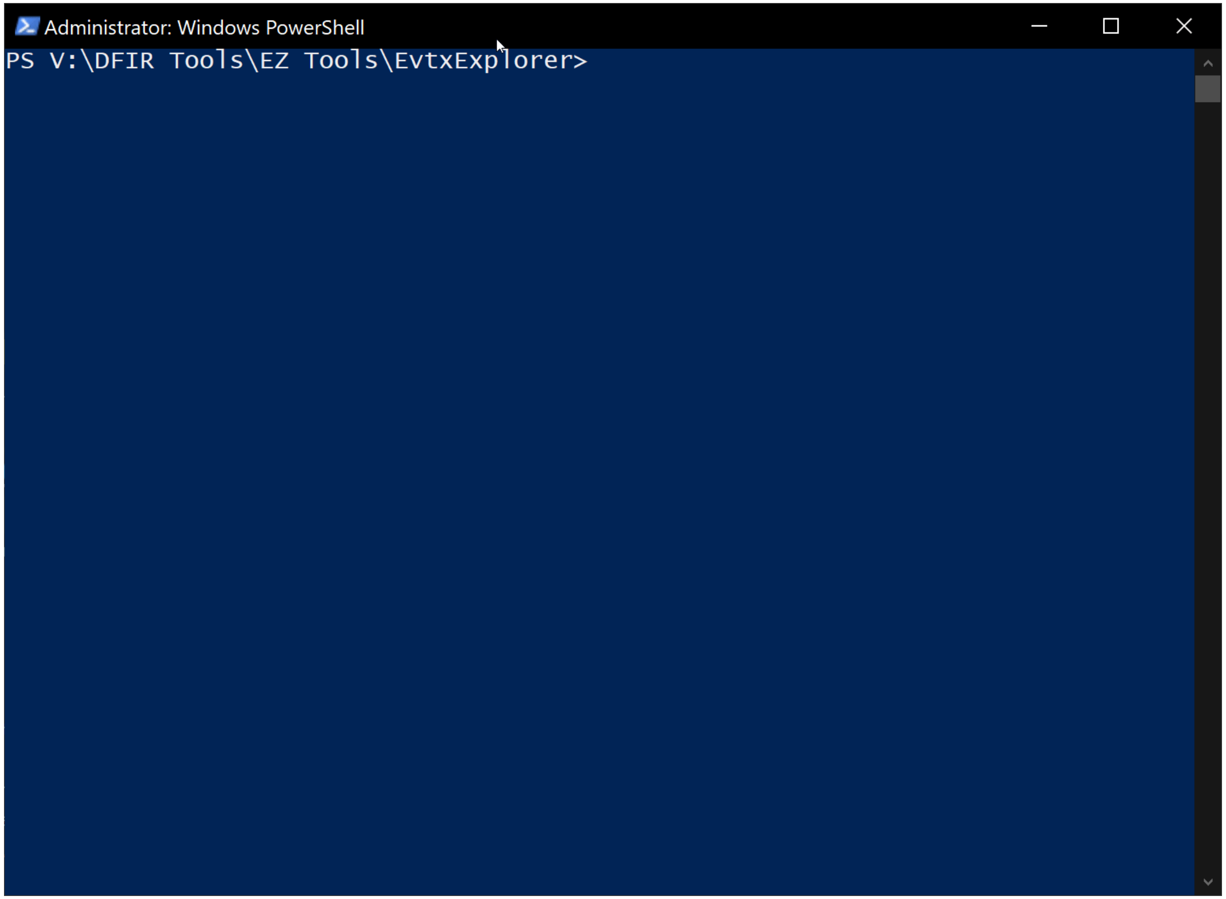
Manual Process

Automating with a KAPE Module

Keeping EvtxECmd Maps Updated – EZ Tools

Running evtxecmd.exe --sync in PS from EZ Tools folder

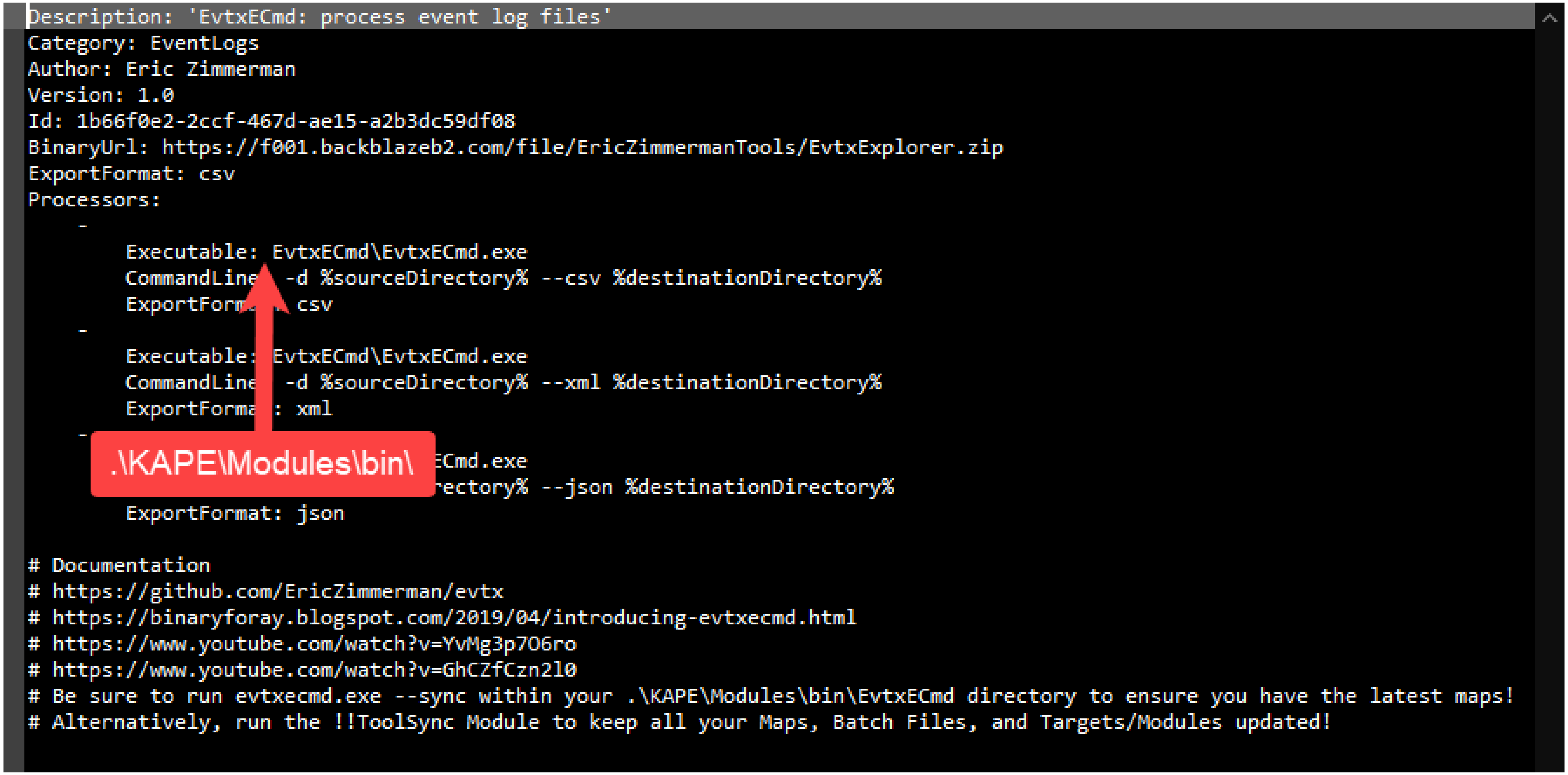
- EZ Tools
  - .\EZ Tools\EvtxExplorer\
  - Evtxecmd.exe --sync
- This syncs for new and updated Maps from GitHub (EricZimmerman\evtx)
- Doing this command at this location doesn't mean your KAPE instance has updated Maps



```
PS V:\DFIR Tools\EZ Tools\EvtxExplorer>
```

EvtxECmd.mkape

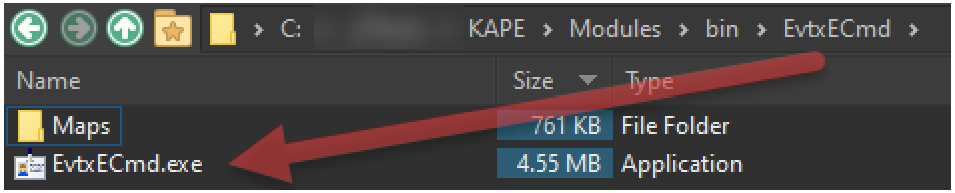
EvtxECmd.mkape in EditPad Pro, EvtxECmd.exe in Directory Opus



```
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
    -
                            Cmd.exe
                            ectory% --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 directory to ensure you have the latest maps!
# Alternatively, run the !!ToolSync Module to keep all your Maps, Batch Files, and Targets/Modules updated!
```

.\KAPE\Modules\bin\

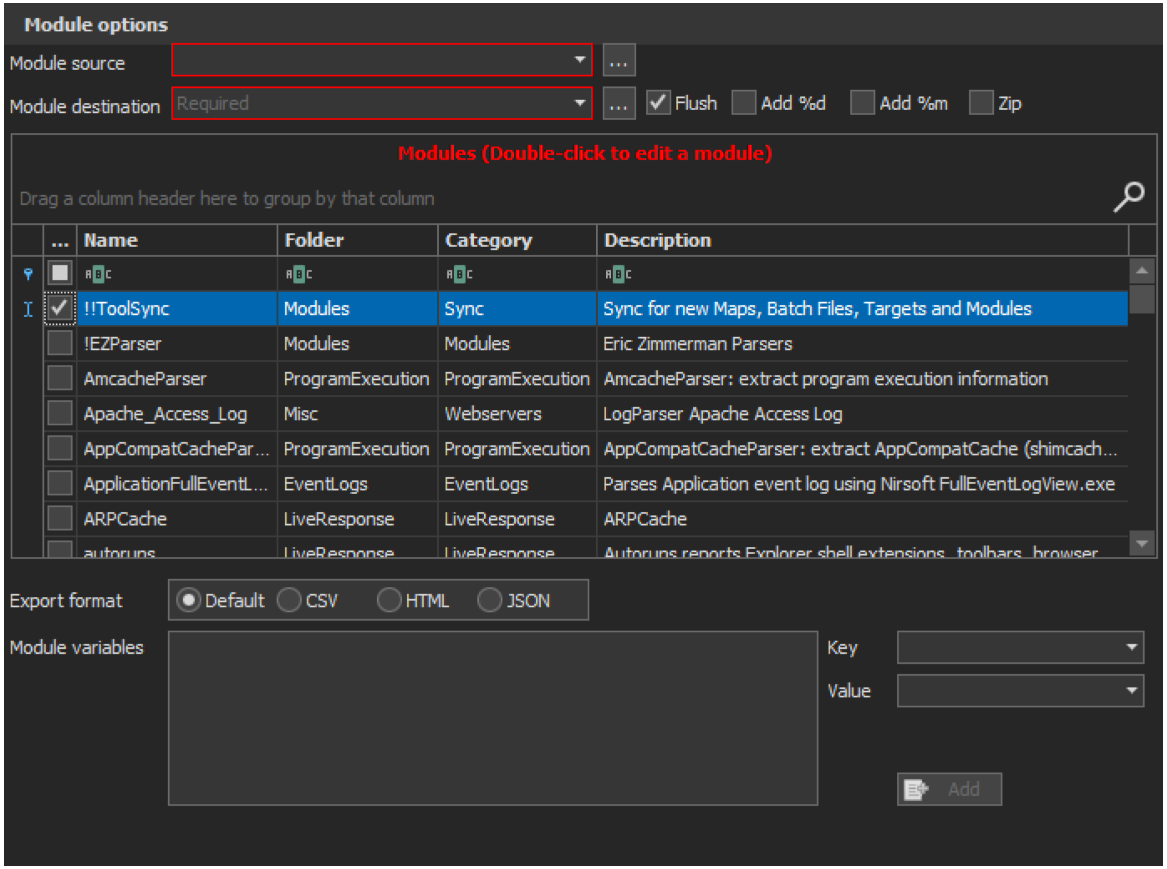


C: › [redacted] KAPE › Modules › bin › EvtxECmd ›

Name	Size	Type
Maps	761 KB	File Folder
EvtxECmd.exe	4.55 MB	Application

Keeping EvtxECmd Maps Updated – KAPE

- KAPE
  - Option 1
    - .\KAPE\Modules\Bin\Evtx Explorer\
    - EvtxECmd.exe --sync
  - Option 2 – The EZ Button
    - KAPE Module
      - !!ToolSync.mkape
      - Run on its own or include in your Module(s) when running KAPE



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

...	Name	Folder	Category	Description
☑	!!ToolSync	Modules	Sync	Sync for new Maps, Batch Files, Targets and Modules
□	!EZParser	Modules	Modules	Eric Zimmerman Parsers
□	AmcacheParser	ProgramExecution	ProgramExecution	AmcacheParser: extract program execution information
□	Apache_Access_Log	Misc	Webservers	LogParser Apache Access Log
□	AppCompatCachePar...	ProgramExecution	ProgramExecution	AppCompatCacheParser: extract AppCompatCache (shimcach...
□	ApplicationFullEventL...	EventLogs	EventLogs	Parses Application event log using Nirsoft FullEventLogView.exe
□	ARPCache	LiveResponse	LiveResponse	ARPCache
□	autoruns	LiveResponse	LiveResponse	Autoruns reports Explorer shell extensions, toolbars, browser

Export format: ● Default ○ CSV ○ HTML ○ JSON

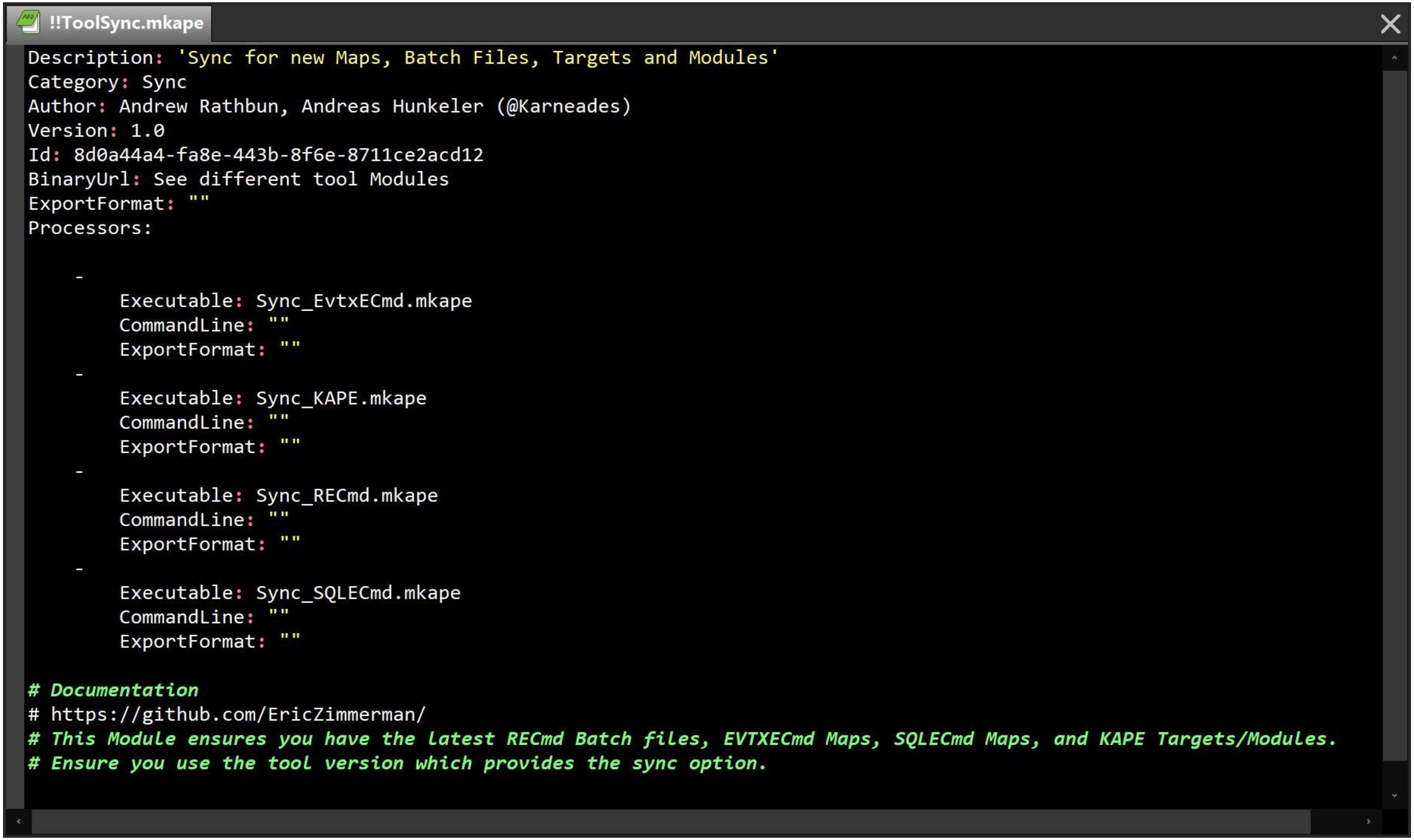
Module variables

Key

Value

!!ToolSync Module

!!ToolSync Module (!!ToolSync.mkape) opened in EditPad Pro



```
Description: 'Sync for new Maps, Batch Files, Targets and Modules'
Category: Sync
Author: Andrew Rathbun, Andreas Hunkeler (@Karneades)
Version: 1.0
Id: 8d0a44a4-fa8e-443b-8f6e-8711ce2acd12
BinaryUrl: See different tool Modules
ExportFormat: ""
Processors:

    -
        Executable: Sync_EvtxECmd.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: Sync_KAPE.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: Sync_RECmd.mkape
        CommandLine: ""
        ExportFormat: ""
    -
        Executable: Sync_SQLECmd.mkape
        CommandLine: ""
        ExportFormat: ""

# Documentation
# https://github.com/EricZimmerman/
# This Module ensures you have the latest RECmd Batch files, EVTXECmd Maps, SQLECmd Maps, and KAPE Targets/Modules.
# Ensure you use the tool version which provides the sync option.
```

Basic KAPE Workflow

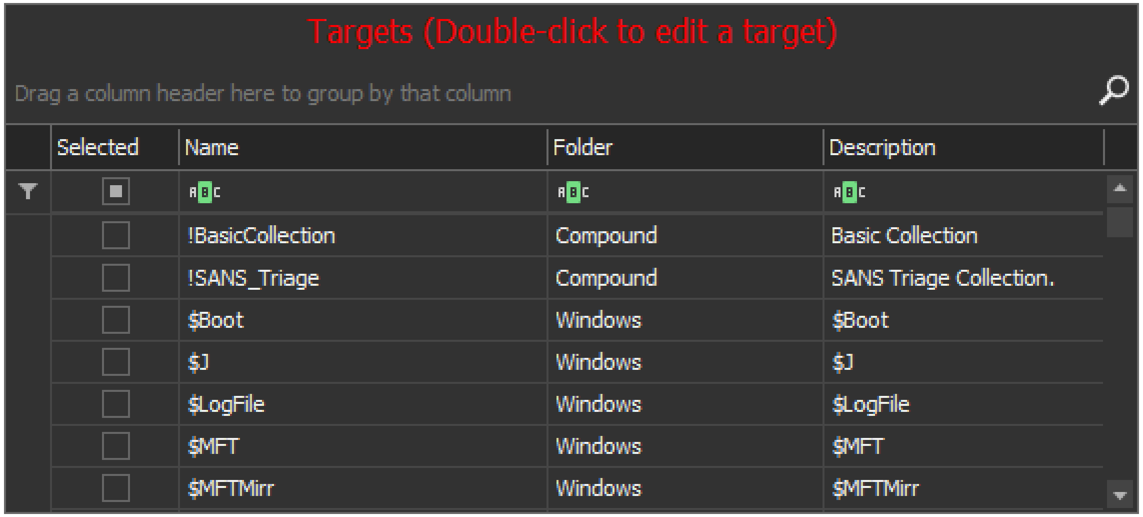
Overview with Visual Aids

April 12, 2021

Basic KAPE Workflow

Standard Incident Response (IR) Workflow

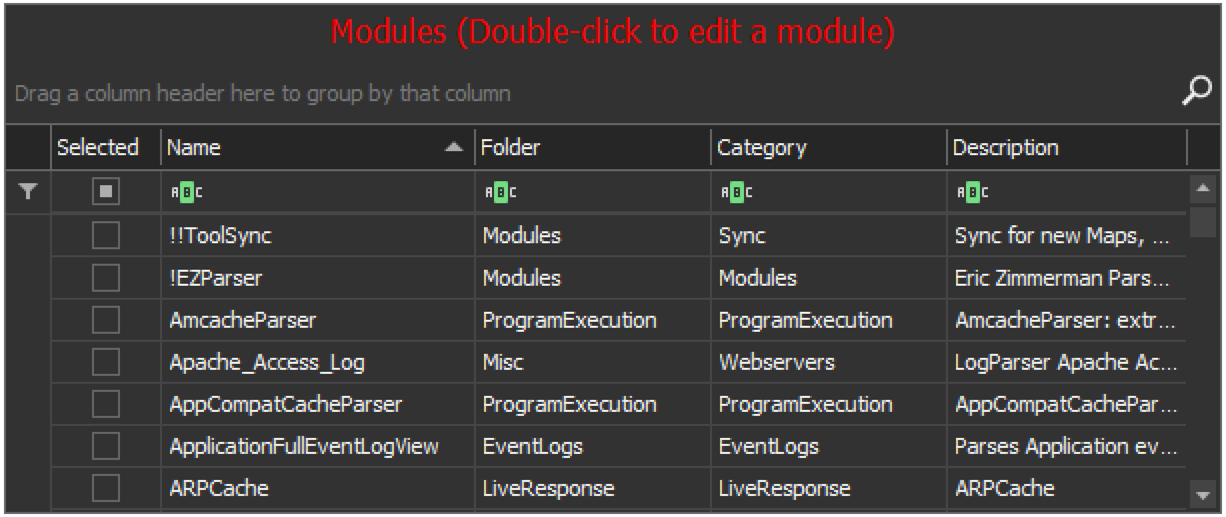
- Select a Target that grabs Event Logs, i.e.
  - !BasicCollection.tkape
  - KapeTriage.tkape
  - EventLogs.tkape
  - EventLogs-RDP.tkape
- Make sure your tools are synced!
  - !!ToolSync.mkape
- Select a Module that parses Event Logs, i.e.
  - !EZParser.mkape
  - EvtxECmd.mkape
  - EvtxECmd_RDP.mkape



Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
☐	!BasicCollection	Compound	Basic Collection
☐	!SANS_Triage	Compound	SANS Triage Collection.
☐	$Boot	Windows	$Boot
☐	$J	Windows	$J
☐	$LogFile	Windows	$LogFile
☐	$MFT	Windows	$MFT
☐	$MFTMirr	Windows	$MFTMirr



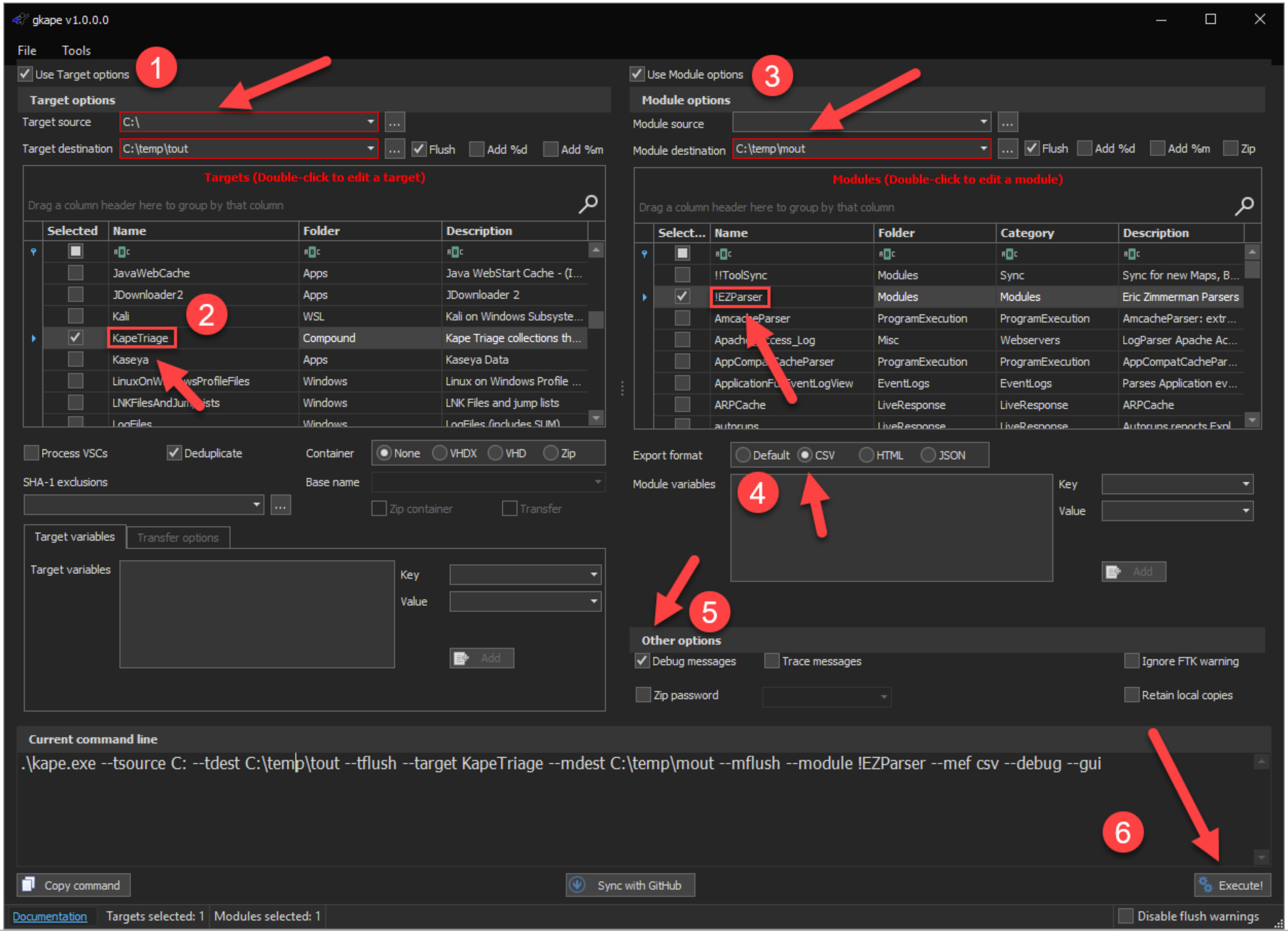
Modules (Double-click to edit a module)

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...
☐	ApplicationFullEventLogView	EventLogs	EventLogs	Parses Application ev...
☐	ARPCache	LiveResponse	LiveResponse	ARPCache

Basic KAPE Workflow

tsource, tdest, KapeTriage (Target), mdest, !EZParser, CSV, Debug (optional), Execute



☑ Use Target options

Target options

Target source: C:\

Target destination: C:\temp\tout ☑ Flush ☐ Add %d ☐ Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
☐	JavaWebCache	Apps	Java WebStart Cache - (I...
☐	JDownloader2	Apps	JDownloader 2
☐	Kali	WSL	Kali on Windows Subsyste...
☑	KapeTriage	Compound	Kape Triage collections th...
☐	Kaseya	Apps	Kaseya Data
☐	LinuxOnW...wsProfileFiles	Windows	Linux on Windows Profile ...
☐	LNKFilesAndJum...ists	Windows	LNK Files and jump lists
☐	LogFiles	Windows	LogFiles (includes SUM)

☐ Process VSCs ☑ Deduplicate

Container: ● None ○ VHDX ○ VHD ○ Zip

SHA-1 exclusions

Base name

☐ Zip container ☐ Transfer

Target variables | Transfer options

Target variables

Key

Value

Add

☑ Use Module options

Module options

Module source:

Module destination: C:\temp\mout ☑ Flush ☐ Add %d ☐ Add %m ☐ Zip

Modules (Double-click to edit a module)

Drag a column header here to group by that column

Select...	Name	Folder	Category	Description
☐	!!ToolSync	Modules	Sync	Sync for new Maps, B...
☑	!EZParser	Modules	Modules	Eric Zimmerman Parsers
☐	AmcacheParser	ProgramExecution	ProgramExecution	AmcacheParser: extr...
☐	Apach...ccess_Log	Misc	Webservers	LogParser Apache Ac...
☐	AppCompa...acheParser	ProgramExecution	ProgramExecution	AppCompatCachePar...
☐	ApplicationF...ventLogView	EventLogs	EventLogs	Parses Application ev...
☐	ARPCache	LiveResponse	LiveResponse	ARPCache
☐	autoruns	LiveResponse	LiveResponse	Autoruns reports Expl...

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

Current command line

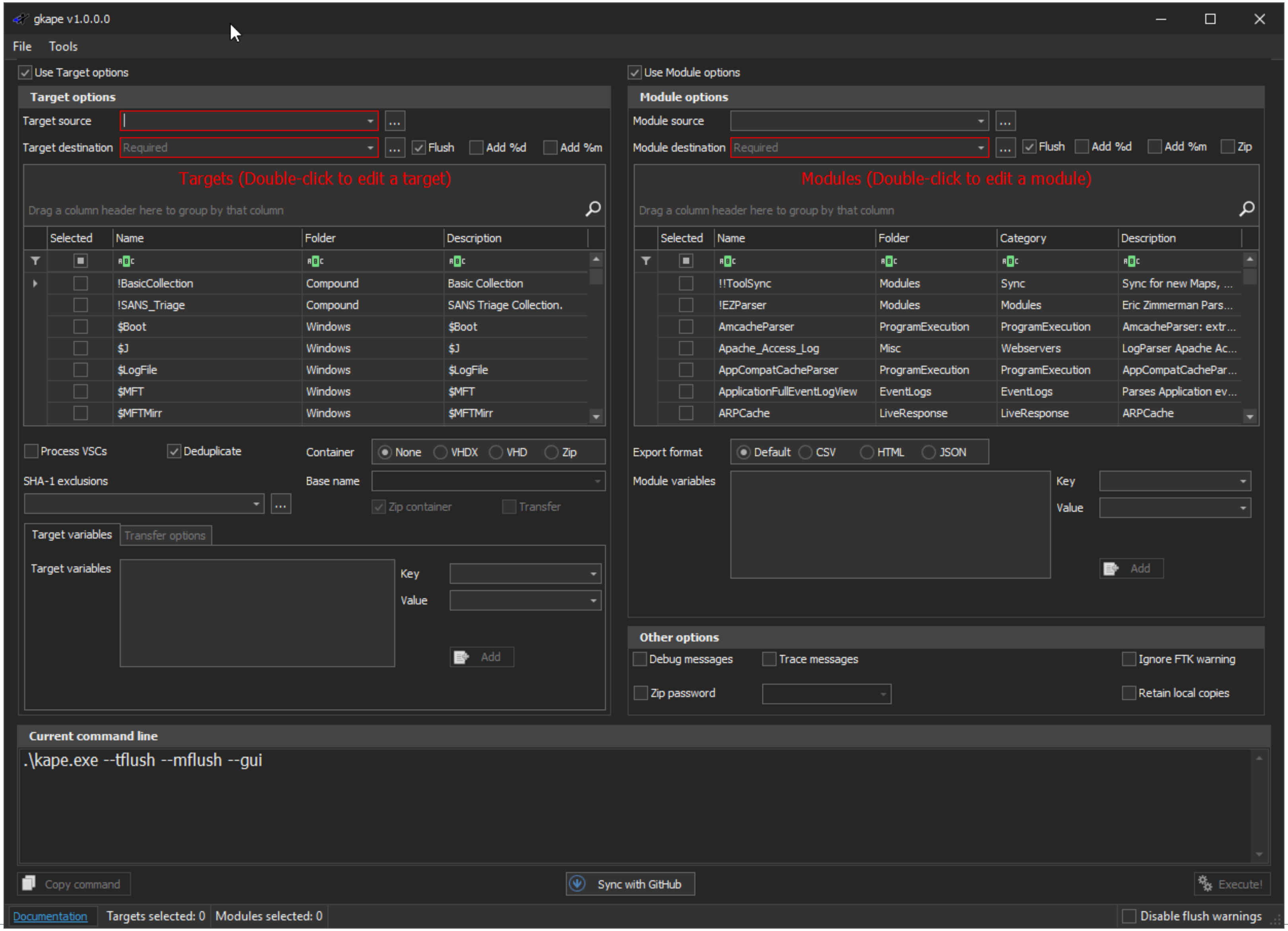
```
.\kape.exe --tsource C: --tdest C:\temp\tout --tflush --target KapeTriage --mdest C:\temp\mout --mflush --module !EZParser --mef csv --debug --gui
```

Copy command | Sync with GitHub | Execute!

Documentation | Targets selected: 1 | Modules selected: 1 | ☐ Disable flush warnings

Basic KAPE Workflow (In Motion)

tsource, tdest, mdest, KapeTriage (Target), !EZParser (Module), CSV, Debug (optional), Execute



☑ Use Target options

Target options

Target source: |

Target destination: Required ☑ Flush □ Add %d □ Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
□	!BasicCollection	Compound	Basic Collection
□	!SANS_Triage	Compound	SANS Triage Collection.
□	$Boot	Windows	$Boot
□	$J	Windows	$J
□	$LogFile	Windows	$LogFile
□	$MFT	Windows	$MFT
□	$MFTMirr	Windows	$MFTMirr

□ Process VSCs ☑ Deduplicate

Container: ● None ○ VHDX ○ VHD ○ Zip

SHA-1 exclusions

Base name

☑ Zip container □ Transfer

Target variables | Transfer options

Target variables

Key

Value

Add

☑ 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...
□	ApplicationFullEventLogView	EventLogs	EventLogs	Parses Application ev...
□	ARPCache	LiveResponse	LiveResponse	ARPCache

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

Current command line

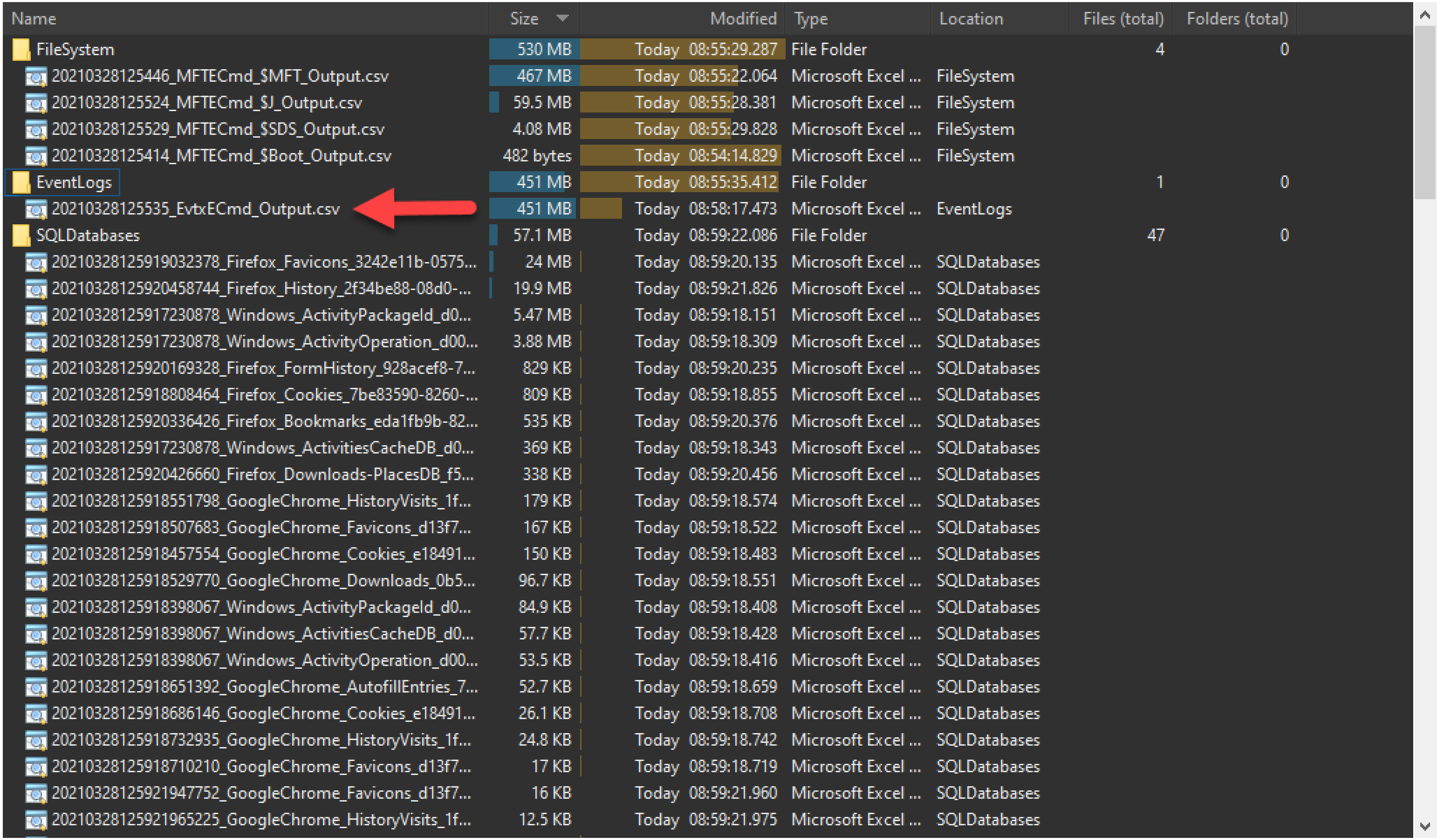
```
.\kape.exe --tflush --mflush --gui
```

Copy command | Sync with GitHub | Execute!

Documentation | Targets selected: 0 | Modules selected: 0 | □ Disable flush warnings

KAPE Output

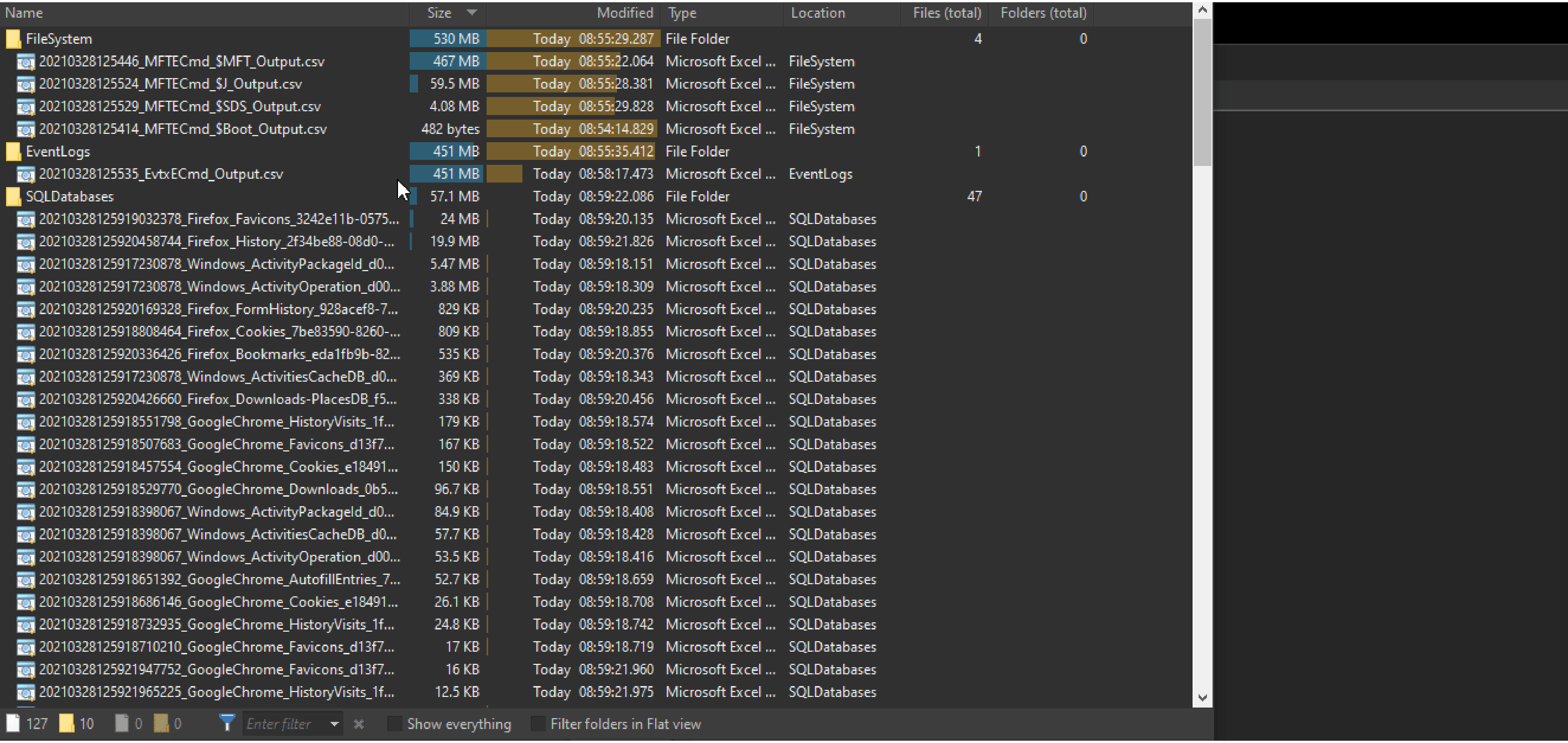
Flat View on mout folder to view all KAPE CSV output to use in Timeline Explorer



Name	Size	Modified	Type	Location	Files (total)	Folders (total)
FileSystem	530 MB	Today 08:55:29.287	File Folder		4	0
20210328125446_MFTECmd_$MFT_Output.csv	467 MB	Today 08:55:22.064	Microsoft Excel ...	FileSystem		
20210328125524_MFTECmd_$J_Output.csv	59.5 MB	Today 08:55:28.381	Microsoft Excel ...	FileSystem		
20210328125529_MFTECmd_$SDS_Output.csv	4.08 MB	Today 08:55:29.828	Microsoft Excel ...	FileSystem		
20210328125414_MFTECmd_$Boot_Output.csv	482 bytes	Today 08:54:14.829	Microsoft Excel ...	FileSystem		
EventLogs	451 MB	Today 08:55:35.412	File Folder		1	0
20210328125535_EvtxECmd_Output.csv	451 MB	Today 08:58:17.473	Microsoft Excel ...	EventLogs		
SQLDatabases	57.1 MB	Today 08:59:22.086	File Folder		47	0
20210328125919032378_Firefox_Favicons_3242e11b-0575...	24 MB	Today 08:59:20.135	Microsoft Excel ...	SQLDatabases		
20210328125920458744_Firefox_History_2f34be88-08d0-...	19.9 MB	Today 08:59:21.826	Microsoft Excel ...	SQLDatabases		
20210328125917230878_Windows_ActivityPackageId_d0...	5.47 MB	Today 08:59:18.151	Microsoft Excel ...	SQLDatabases		
20210328125917230878_Windows_ActivityOperation_d00...	3.88 MB	Today 08:59:18.309	Microsoft Excel ...	SQLDatabases		
20210328125920169328_Firefox_FormHistory_928acef8-7...	829 KB	Today 08:59:20.235	Microsoft Excel ...	SQLDatabases		
20210328125918808464_Firefox_Cookies_7be83590-8260-...	809 KB	Today 08:59:18.855	Microsoft Excel ...	SQLDatabases		
20210328125920336426_Firefox_Bookmarks_eda1fb9b-82...	535 KB	Today 08:59:20.376	Microsoft Excel ...	SQLDatabases		
20210328125917230878_Windows_ActivitiesCacheDB_d0...	369 KB	Today 08:59:18.343	Microsoft Excel ...	SQLDatabases		
20210328125920426660_Firefox_Downloads-PlacesDB_f5...	338 KB	Today 08:59:20.456	Microsoft Excel ...	SQLDatabases		
20210328125918551798_GoogleChrome_HistoryVisits_1f...	179 KB	Today 08:59:18.574	Microsoft Excel ...	SQLDatabases		
20210328125918507683_GoogleChrome_Favicons_d13f7...	167 KB	Today 08:59:18.522	Microsoft Excel ...	SQLDatabases		
20210328125918457554_GoogleChrome_Cookies_e18491...	150 KB	Today 08:59:18.483	Microsoft Excel ...	SQLDatabases		
20210328125918529770_GoogleChrome_Downloads_0b5...	96.7 KB	Today 08:59:18.551	Microsoft Excel ...	SQLDatabases		
20210328125918398067_Windows_ActivityPackageId_d0...	84.9 KB	Today 08:59:18.408	Microsoft Excel ...	SQLDatabases		
20210328125918398067_Windows_ActivitiesCacheDB_d0...	57.7 KB	Today 08:59:18.428	Microsoft Excel ...	SQLDatabases		
20210328125918398067_Windows_ActivityOperation_d00...	53.5 KB	Today 08:59:18.416	Microsoft Excel ...	SQLDatabases		
20210328125918651392_GoogleChrome_AutofillEntries_7...	52.7 KB	Today 08:59:18.659	Microsoft Excel ...	SQLDatabases		
20210328125918686146_GoogleChrome_Cookies_e18491...	26.1 KB	Today 08:59:18.708	Microsoft Excel ...	SQLDatabases		
20210328125918732935_GoogleChrome_HistoryVisits_1f...	24.8 KB	Today 08:59:18.742	Microsoft Excel ...	SQLDatabases		
20210328125918710210_GoogleChrome_Favicons_d13f7...	17 KB	Today 08:59:18.719	Microsoft Excel ...	SQLDatabases		
20210328125921947752_GoogleChrome_Favicons_d13f7...	16 KB	Today 08:59:21.960	Microsoft Excel ...	SQLDatabases		
20210328125921965225_GoogleChrome_HistoryVisits_1f...	12.5 KB	Today 08:59:21.975	Microsoft Excel ...	SQLDatabases		

KAPE Output Ingested into Timeline Explorer

Using Flat View to select multiple CSVs (including EvtxECmd output) and drag into TLE



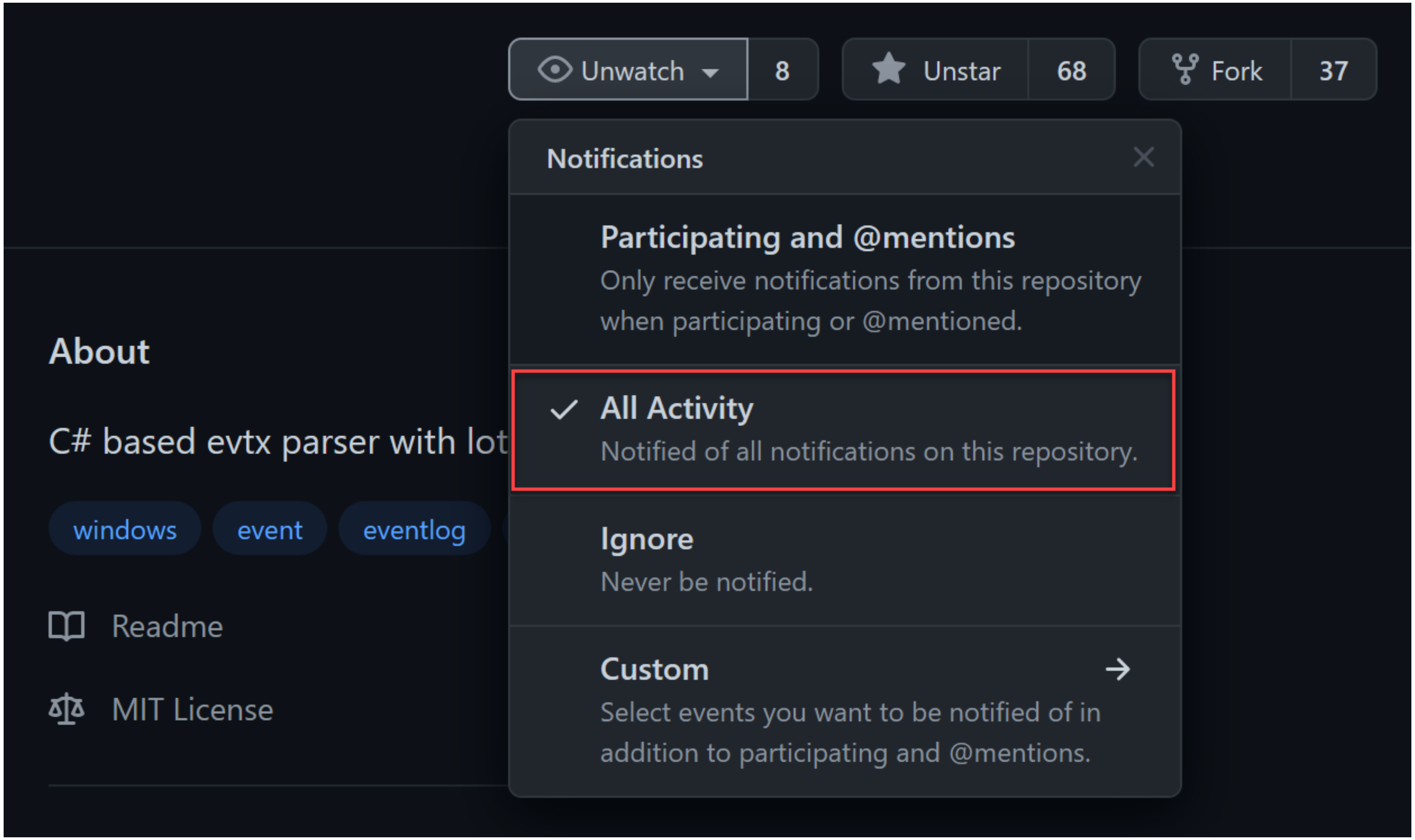
Name	Size	Modified	Type	Location	Files (total)	Folders (total)
FileSystem	530 MB	Today 08:55:29.287	File Folder		4	0
20210328125446_MFTECmd_$MFT_Output.csv	467 MB	Today 08:55:22.064	Microsoft Excel ...	FileSystem		
20210328125524_MFTECmd_$J_Output.csv	59.5 MB	Today 08:55:28.381	Microsoft Excel ...	FileSystem		
20210328125529_MFTECmd_$SDS_Output.csv	4.08 MB	Today 08:55:29.828	Microsoft Excel ...	FileSystem		
20210328125414_MFTECmd_$Boot_Output.csv	482 bytes	Today 08:54:14.829	Microsoft Excel ...	FileSystem		
EventLogs	451 MB	Today 08:55:35.412	File Folder		1	0
20210328125535_EvtxECmd_Output.csv	451 MB	Today 08:58:17.473	Microsoft Excel ...	EventLogs		
SQLDatabases	57.1 MB	Today 08:59:22.086	File Folder		47	0
20210328125919032378_Firefox_Favicons_3242e11b-0575...	24 MB	Today 08:59:20.135	Microsoft Excel ...	SQLDatabases		
20210328125920458744_Firefox_History_2f34be88-08d0-...	19.9 MB	Today 08:59:21.826	Microsoft Excel ...	SQLDatabases		
20210328125917230878_Windows_ActivityPackageId_d0...	5.47 MB	Today 08:59:18.151	Microsoft Excel ...	SQLDatabases		
20210328125917230878_Windows_ActivityOperation_d00...	3.88 MB	Today 08:59:18.309	Microsoft Excel ...	SQLDatabases		
20210328125920169328_Firefox_FormHistory_928acef8-7...	829 KB	Today 08:59:20.235	Microsoft Excel ...	SQLDatabases		
20210328125918808464_Firefox_Cookies_7be83590-8260-...	809 KB	Today 08:59:18.855	Microsoft Excel ...	SQLDatabases		
20210328125920336426_Firefox_Bookmarks_eda1fb9b-82...	535 KB	Today 08:59:20.376	Microsoft Excel ...	SQLDatabases		
20210328125917230878_Windows_ActivitiesCacheDB_d0...	369 KB	Today 08:59:18.343	Microsoft Excel ...	SQLDatabases		
20210328125920426660_Firefox_Downloads-PlacesDB_f5...	338 KB	Today 08:59:20.456	Microsoft Excel ...	SQLDatabases		
20210328125918551798_GoogleChrome_HistoryVisits_1f...	179 KB	Today 08:59:18.574	Microsoft Excel ...	SQLDatabases		
20210328125918507683_GoogleChrome_Favicons_d13f7...	167 KB	Today 08:59:18.522	Microsoft Excel ...	SQLDatabases		
20210328125918457554_GoogleChrome_Cookies_e18491...	150 KB	Today 08:59:18.483	Microsoft Excel ...	SQLDatabases		
20210328125918529770_GoogleChrome_Downloads_0b5...	96.7 KB	Today 08:59:18.551	Microsoft Excel ...	SQLDatabases		
20210328125918398067_Windows_ActivityPackageId_d0...	84.9 KB	Today 08:59:18.408	Microsoft Excel ...	SQLDatabases		
20210328125918398067_Windows_ActivitiesCacheDB_d0...	57.7 KB	Today 08:59:18.428	Microsoft Excel ...	SQLDatabases		
20210328125918398067_Windows_ActivityOperation_d00...	53.5 KB	Today 08:59:18.416	Microsoft Excel ...	SQLDatabases		
20210328125918651392_GoogleChrome_AutofillEntries_7...	52.7 KB	Today 08:59:18.659	Microsoft Excel ...	SQLDatabases		
20210328125918686146_GoogleChrome_Cookies_e18491...	26.1 KB	Today 08:59:18.708	Microsoft Excel ...	SQLDatabases		
20210328125918732935_GoogleChrome_HistoryVisits_1f...	24.8 KB	Today 08:59:18.742	Microsoft Excel ...	SQLDatabases		
20210328125918710210_GoogleChrome_Favicons_d13f7...	17 KB	Today 08:59:18.719	Microsoft Excel ...	SQLDatabases		
20210328125921947752_GoogleChrome_Favicons_d13f7...	16 KB	Today 08:59:21.960	Microsoft Excel ...	SQLDatabases		
20210328125921965225_GoogleChrome_HistoryVisits_1f...	12.5 KB	Today 08:59:21.975	Microsoft Excel ...	SQLDatabases		

Final Thoughts

- Maps are very useful, but the Payload column is still useful as well.
- The Maps are only as good as the author made them to be.
- Not all data an event logs can fit into 6 columns (Payload column).
- During your analysis, if you find badness in an undocumented/unmapped event and there’s value to be had for all, either:
    - Make the map yourself and do a PR on GitHub
    - Reach out on GitHub and I’ll make the map myself

Follow the project(s) on GitHub!

- https://github.com/EricZimmerman/evtx
- https://github.com/EricZimmerman/KapeFiles



C# based evtx parser with lot

Notifications

Participating and @mentions
Only receive notifications from this repository when participating or @mentioned.

✓ All Activity
Notified of all notifications on this repository.

Ignore
Never be notified.

Custom →
Select events you want to be notified of in addition to participating and @mentions.

Live Demo

Using EvtxECmd with KAPE

Demonstrating the power of EvtxECmd Maps

Analysis with Timeline Explorer

Questions

Type in the Chat or unmute yourself

For More KAPE:

Intensive Training and Certification Sessions

- Virtual live sessions
- Max 25 students

Full Calendar Available here:

bit.ly/KAPE2021

SCHEDULE	INSTRUCTORS
April 13, 2021 10:00 a.m. – 7:00 p.m. (EST)	Eric Zimmerman Sean Straw Scott Zuberbuehler Andrew Rathbun
June 3, 2021 8:00 a.m. – 5:00 p.m. (GMT)	James Thoburn Paul Wells Guillermo Roman
June 17, 2021 10:00 a.m. – 7:00 p.m. (EST)	Sean Straw Scott Zuberbuehler Andrew Rathbun

Tools Displayed During Presentation

- Tools Used During Presentation
  - KAPE
  - EvtxECmd
  - Timeline Explorer
- Eric Zimmerman's Tools
  - PowerShell script to download them all
- GitHub Repos
  - EVTX-ATTACK-SAMPLES
  - SANS DeepBlueCLI
    - Lots of infected EVTX files to test EvtxECmd/KAPE with
- Directory Opus
  - Windows File Explorer replacement
- EditPad Pro
  - One of my favorite text editors
- Snagit
  - Used to mark up the screenshots in this presentation

Useful Resources

Curated by Andrew Rathbun

- AboutDFIR
  - Owned and operated by Kroll’s Devon Ackerman
  - Timeline Explorer Guide
- Digital Forensics Discord Server
  - A Beginner’s Guide to the Digital Forensics Discord Server
- Forensic 4:cast Awards
  - Nominations are open! Submit nominees for the 2021 Awards here. Be sure to vote on the final ballot in a couple months!
- This Week in 4n6
  - Subscribe for a weekly email digest of everything DFIR delivered to your email inbox!
- Twitter
  - #dfir

Keeping EZ Tools and KAPE Updated

Proper tool maintenance ensures you have the latest and greatest

- !!ToolSync
  - Covers --sync for the following tools in your .\KAPE\Modules\bin
    - KAPE (Targets/Modules)
    - .\KAPE\Modules\bin\EvtxECmd (Maps)
    - .\KAPE\Modules\bin\RECmd (Batch Files)
    - .\KAPE\Modules\bin\SQLECmd (Maps)
- EZ Tools Binaries
  - Downloaded with PS1 script
  - Downloads to directory separate from .\KAPE\Modules\bin
- KAPE Module Binaries
  - Located in .\KAPE\Modules\bin
    - Keep these updated if you’re using KAPE!
    - KAPE calls upon the binaries in this location, not your EZ Tools folder

KROLL

For more information, please contact:

KAPE@Kroll.com

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.

© 2021 Duff & Phelps, LLC. All rights reserved. Kroll is a trade name for Duff & Phelps, LLC and its affiliates.