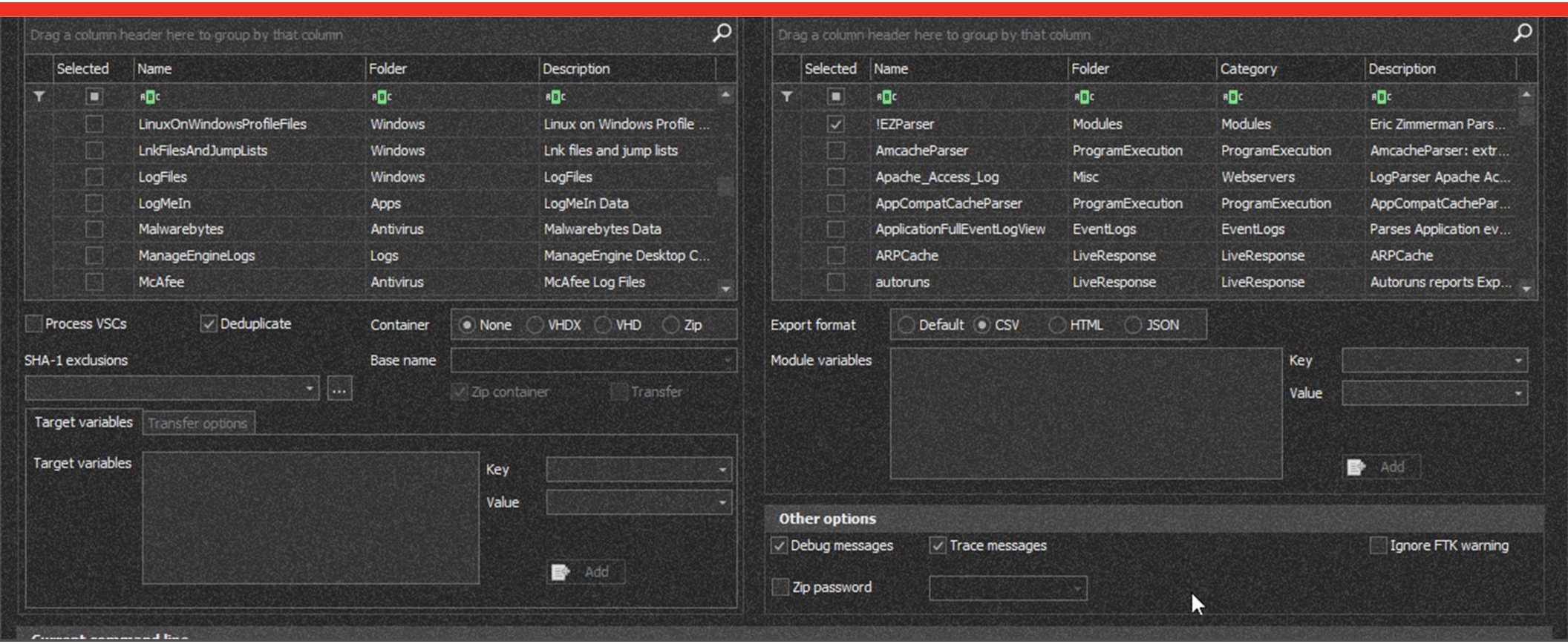


Artifact Analysis and Timelining with **KAPE**

May 2020

Private and Confidential

Kroll | A Division of DUFF & PHELPS

About Mari

- Associate Managing Director at Kroll
- SANS Instructor
- @MariDeGrazia

Overview

Triage Collection

KAPE

Mini Timelines

Analysis

Upcoming KAPE Intensive Training and Certification

- Virtual live sessions
- Max 25 students

bit.ly/kape2020

SCHEDULE	INSTRUCTORS
June 18, 2020 10:00 a.m. – 7:00 p.m. (EST)	Eric Zimmerman Mari DeGrazia Sean Straw
July 7, 2020 9:00 am – 6:00 pm (GMT + 8, Hong Kong/Singapore time)	Eric Zimmerman Paul Jackson Dave Klopp Rob Phillips

Approach

Triage Data

Filesystem

Registry

Event Logs

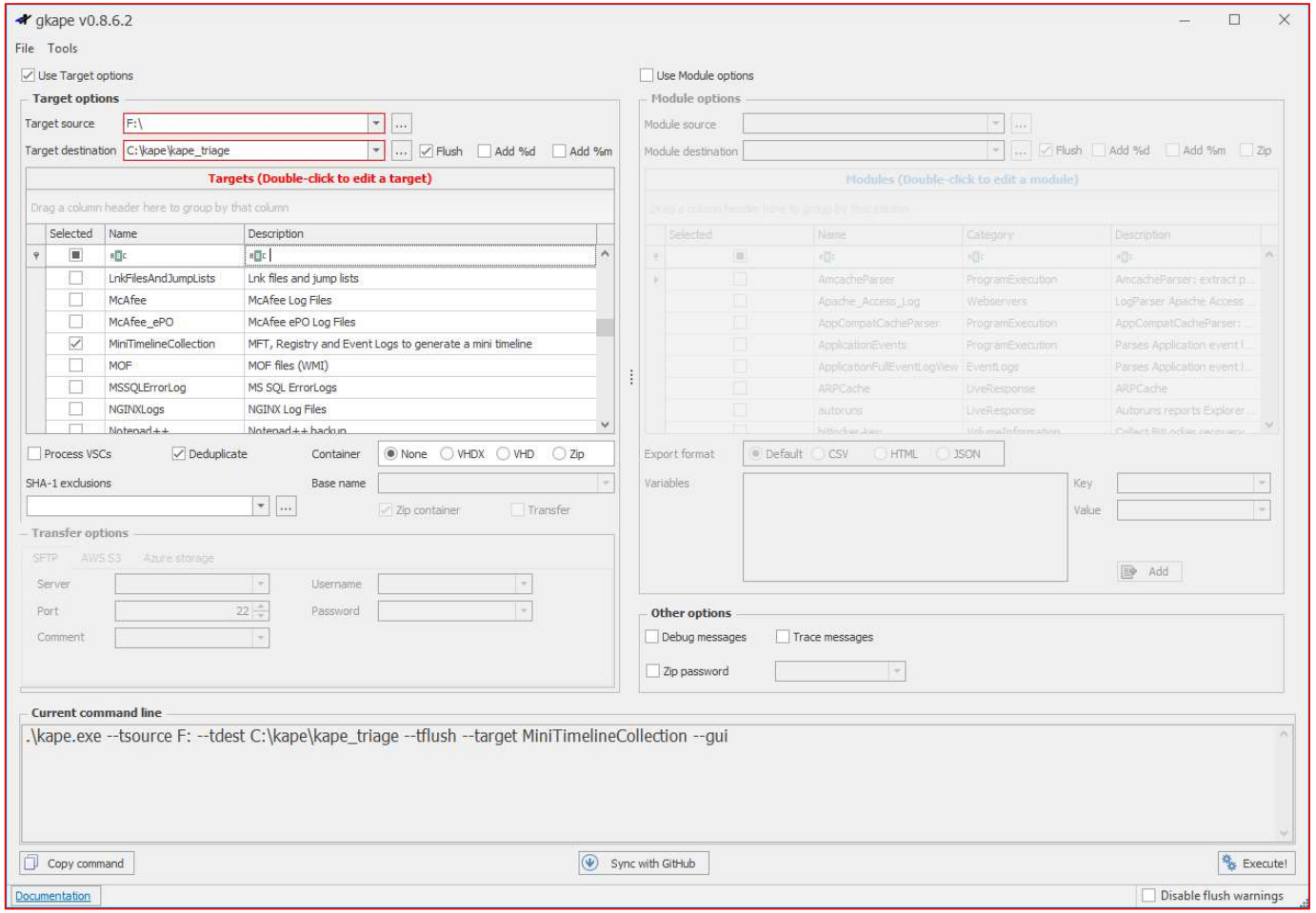
KAPE BASICS

- Targets
- Modules
- Mounted Image
- Live System

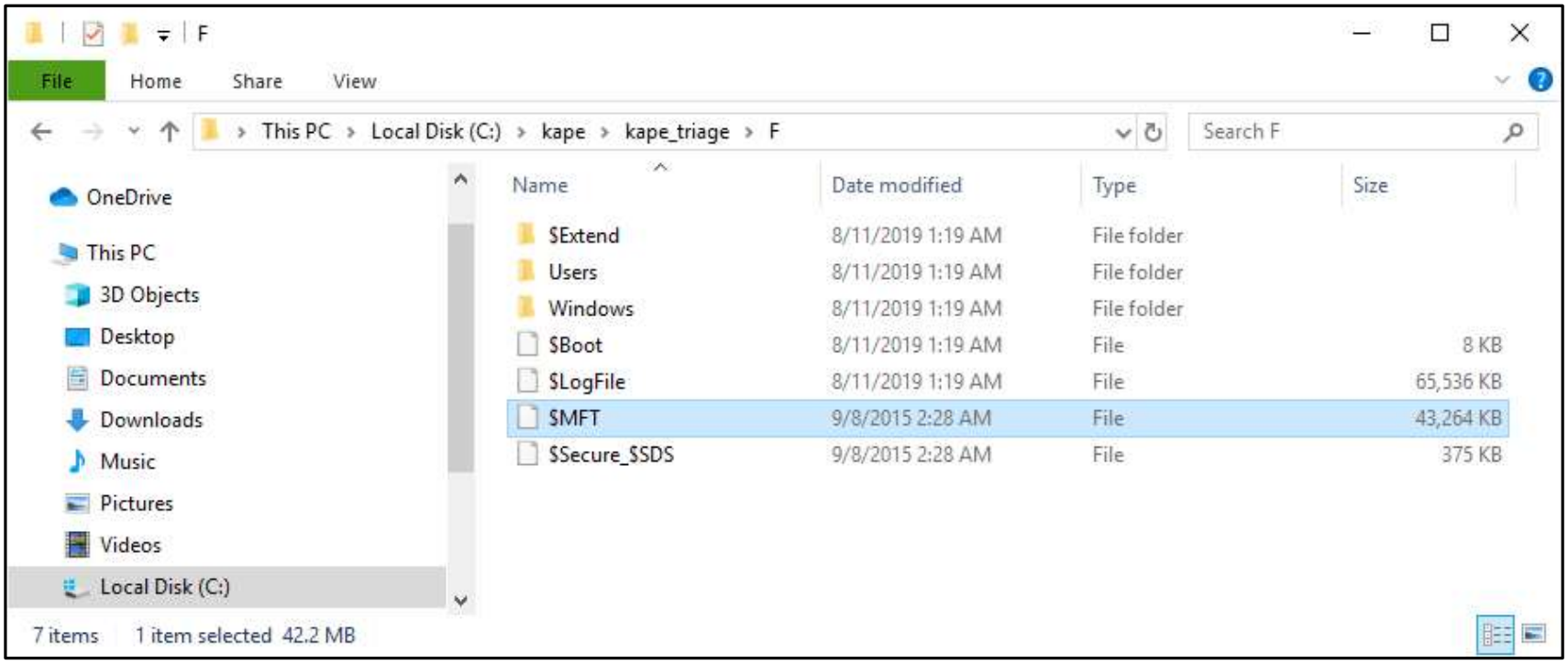
Triage Collection with KAPE

Target:

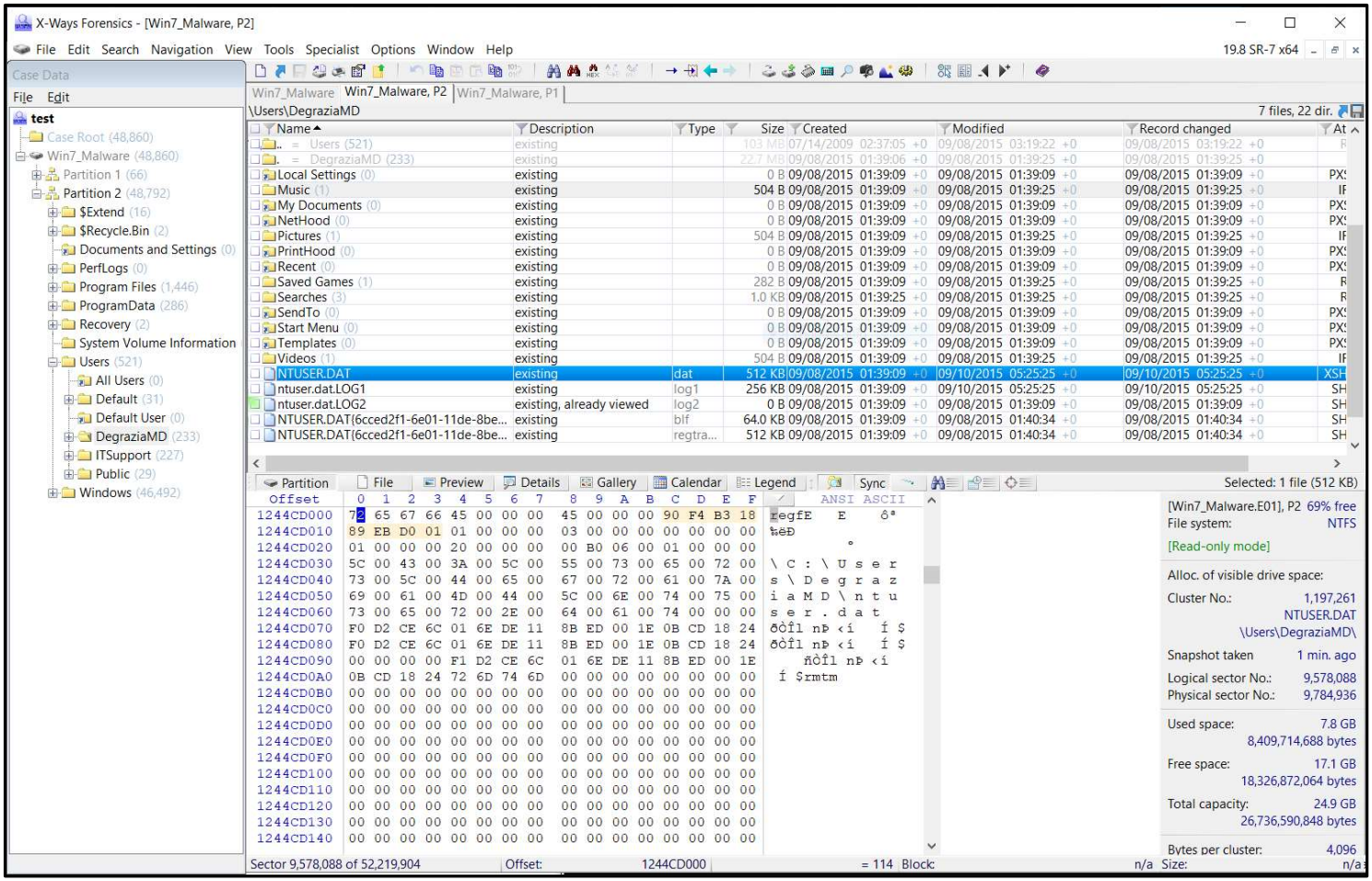
MiniTimelineCollection



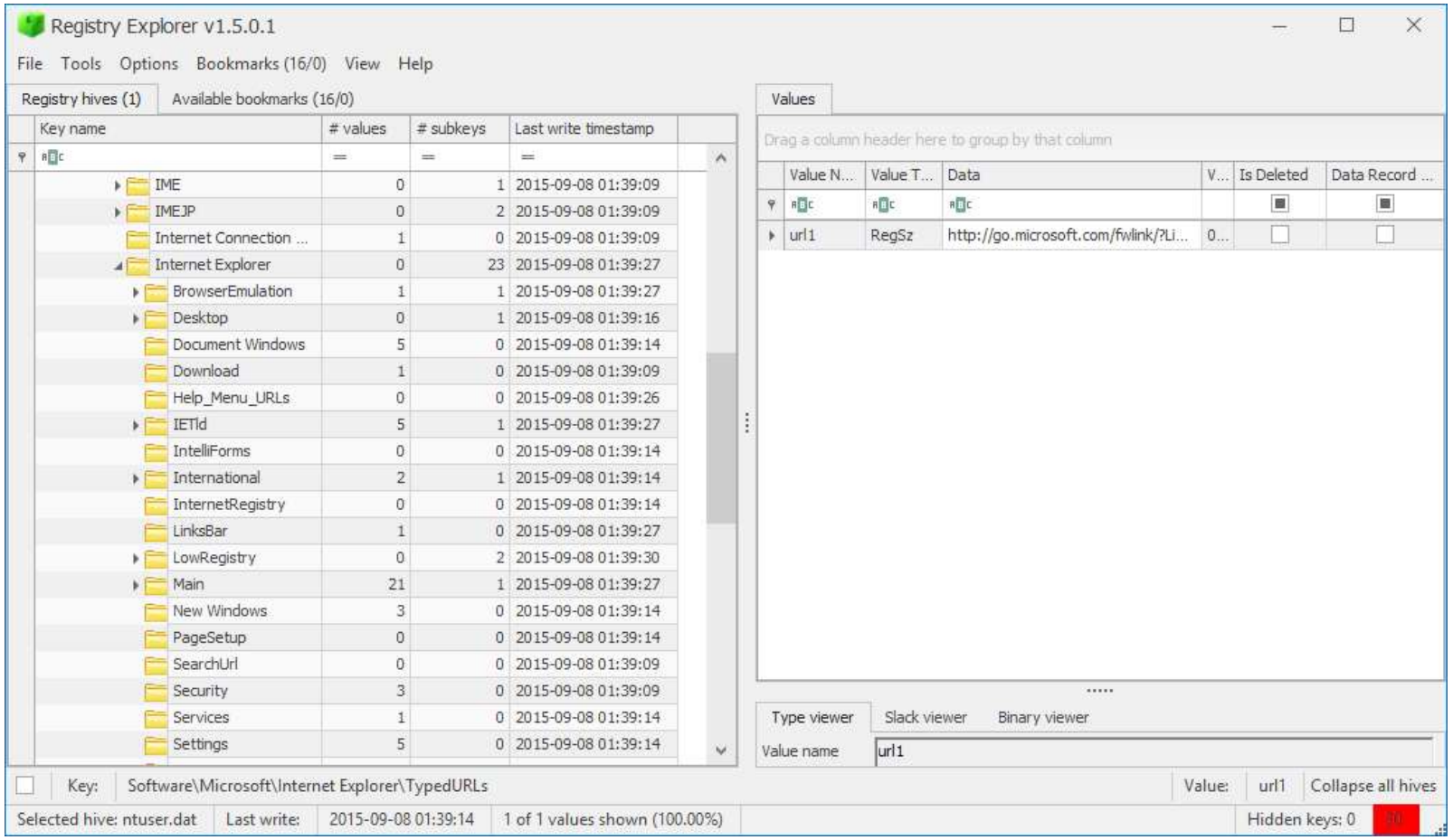
Triage Data Outputs



Data Munging



Data Munging



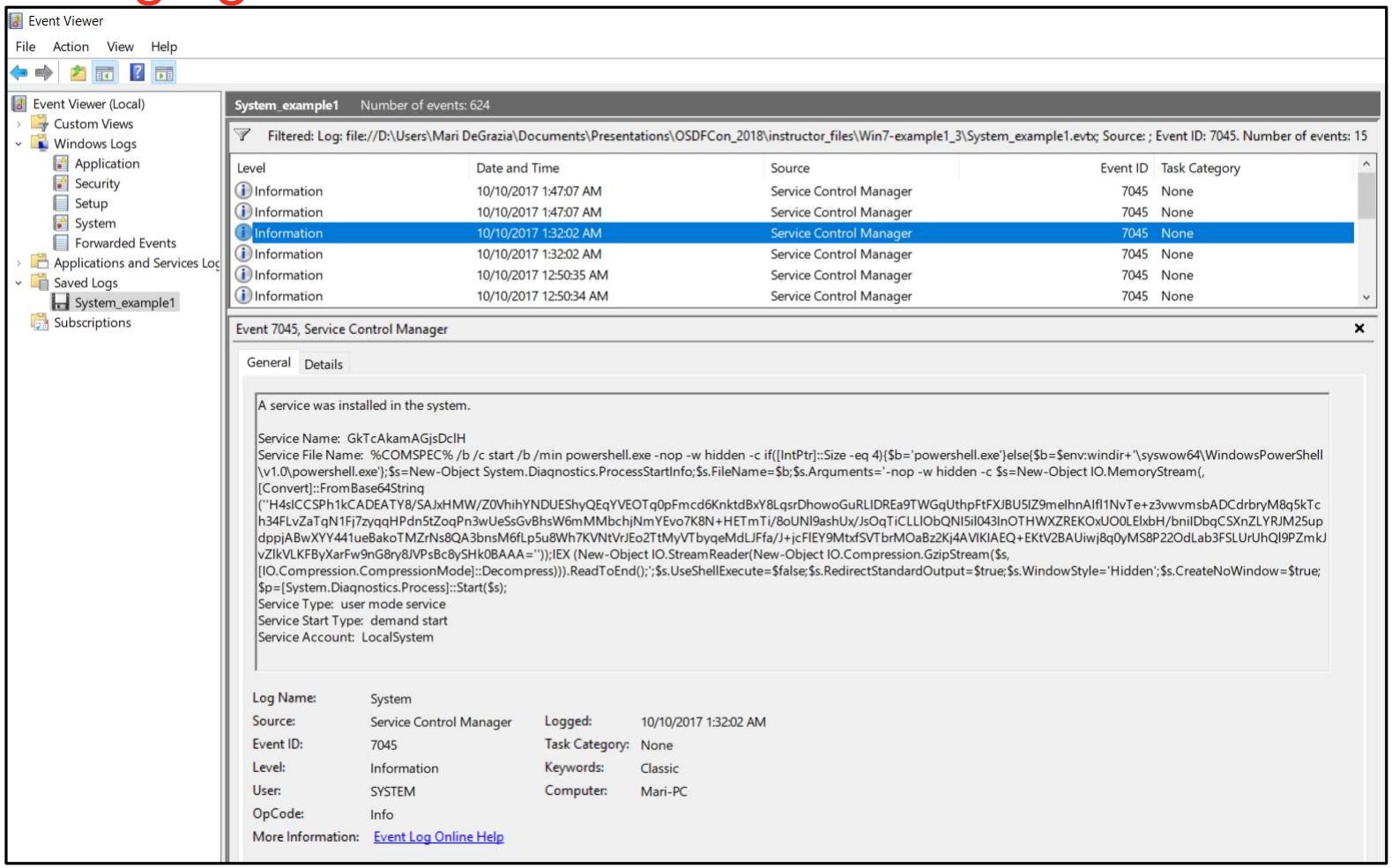
Data Munging

```
----------------------------------------
svc_plus v.20120625
(System) Lists services/drivers in Services key by LastWrite times in a short format with warnings for type mismatche

ControlSet001\Services
Lists services/drivers in Services key by LastWrite times in a short format with warnings for type mismatches; ^^^^ I

Sun Aug 11 00:41:48 2019Z,BITS,@%SystemRoot%\system32\qmgr.dll;-1000,%SystemRoot%\System32\svchost.exe -k netsvcs -p,
Sun Aug 11 00:06:03 2019Z,aimwrfltr,Arsenal Image Mounter Write Filter,System32\drivers\aimwrfltr.sys,,Boot Start,
Sat Aug 10 16:36:26 2019Z,phdskmnt,Arsenal Image Mounter SCSI Miniport,\SystemRoot\System32\drivers\phdskmnt.sys,,Man
Sat Aug 10 02:50:27 2019Z,TrustedInstaller,@%SystemRoot%\servicing\TrustedInstaller.exe;-100,%SystemRoot%\servicing\T
Sat Aug 10 01:37:20 2019Z,HidUsb,@input.inf;%HID.SvcDesc%;Microsoft HID Class Driver,\SystemRoot\System32\drivers\hid
Sat Aug 10 01:37:20 2019Z,kbdhid,@keyboard.inf;%KBDHID.SvcDesc%;Keyboard HID Driver,\SystemRoot\System32\drivers\kbdh
Fri Aug  9 14:50:23 2019Z,GoogleChromeElevationService,Google Chrome Elevation Service,"C:\Program Files (x86)\Google
Thu Aug  8 14:49:16 2019Z,LanmanServer\Parameters,,%SystemRoot%\system32\srvsvc.dll,,,
Thu Aug  8 14:49:16 2019Z,NdisTapi,@%systemroot%\system32\mprmsg.dll;-32001,System32\DRIVERS\ndistapi.sys,,Manual,
Thu Aug  8 14:49:16 2019Z,NdisWan,@%systemroot%\system32\mprmsg.dll;-32002,\SystemRoot\System32\drivers\ndiswan.sys,,
Thu Aug  8 14:49:16 2019Z,PptpMiniport,@%systemroot%\system32\mprmsg.dll;-32006,\SystemRoot\System32\drivers\raspptp.
Thu Aug  8 14:49:16 2019Z,RasAgileVpn,@netavpna.inf;%Svc-Mp-AgileVpn-DispName%;WAN Miniport (IKEv2),\SystemRoot\Syste
Thu Aug  8 14:49:16 2019Z,Rasl2tp,@%systemroot%\system32\mprmsg.dll;-32005,\SystemRoot\System32\drivers\rasl2tp.sys,,
Thu Aug  8 14:49:16 2019Z,RasPppoe,@%systemroot%\system32\mprmsg.dll;-32007,System32\DRIVERS\raspppoe.sys,,Manual,
Thu Aug  8 14:49:16 2019Z,RasSstp,@%systemroot%\system32\sstpsvc.dll;-202,\SystemRoot\System32\drivers\rassstp.sys,,M
Thu Aug  8 14:49:15 2019Z,BcastDVRUserService_35377,BcastDVRUserService_35377,C:\WINDOWS\system32\svchost.exe -k Bcas
Thu Aug  8 14:49:15 2019Z,BluetoothUserService_35377,BluetoothUserService_35377,C:\WINDOWS\system32\svchost.exe -k Bt
Thu Aug  8 14:49:15 2019Z,CaptureService_35377,CaptureService_35377,C:\WINDOWS\system32\svchost.exe -k LocalService -
Thu Aug  8 14:49:15 2019Z,cbdhsvc_35377,cbdhsvc_35377,C:\WINDOWS\system32\svchost.exe -k ClipboardSvcGroup -p,^^^^224
```

Data Munging



Why Timelines

- Combine Artifacts
- Normalize Timestamps
- Build Connections
- Reporting

TLN Timeline Format

Time | Source | Host | User | Description

- Time: 32 Bit Unix Epoch
- Source: EVT, REG, FILE etc.
- Host: Computer Name, IP address, etc.
- User: Username, SID, IM Screen name, etc.
- Description: Description of event

https://forensicswiki.xyz/wiki/index.php?title=TLN

2015-09-10 05:25:18	FILE	DeGraziaMD-PC		MACB [15840] c:/Windows/Prefetch/NOTEPAD.EXE-D8414F97.pf ($FILE_NAME)
2015-09-10 05:25:18	FILE	DeGraziaMD-PC		MACB [15840] c:/Windows/Prefetch/NOTEPAD.EXE-D8414F97.pf
2015-09-10 05:25:18	FILE	DeGraziaMD-PC		MAC. [0] c:/Windows/Prefetch
2015-09-10 05:25:17	EVTX	DegraziaMD-PC		Microsoft-Windows-Security-Auditing/4634;;An account was logged off;Target: DegraziaMD-PC\ITSupport;LogonType: 3;{ EventData":{"D
2015-09-10 05:25:14	FILE	DeGraziaMD-PC		M.C. [1248] c:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.2.Crwl
2015-09-10 05:25:14	FILE	DeGraziaMD-PC		M.C. [8284] c:/ProgramData/Microsoft/Search/Data/Applications/Windows/GatherLogs/SystemIndex/SystemIndex.2.gthr
2015-09-10 05:25:12	REG	DeGraziaMD-PC		M... HKLM_SOFTWARE/Microsoft/Windows Search/Gather/Windows/SystemIndex/Crawls
2015-09-10 05:25:12	FILE	DeGraziaMD-PC		M.C. [11954] c:/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-0CB8CADE.pf
2015-09-10 05:25:12	REG	DeGraziaMD-PC		M... HKLM_SOFTWARE/Microsoft/Windows Search/CatalogNames/Windows/SystemIndex
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat	M... HKEY_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.lnk
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat	M... HKEY_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.lnk/OpenWithProgids
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat	[Program Execution] UserAssist - {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Notepad.lnk (1)
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat	[Program Execution] UserAssist - {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\notepad.exe (1)
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat	M... HKEY_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.lnk/OpenWithList
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat	M... HKEY_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/FileExts

Tools that have the TLN Format

- Harlan Carvey (Free)
- Plaso (Free)
- TZWorks (Commercial)

Tools Used

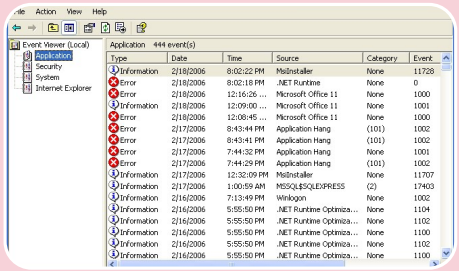
MFTECmd

Bodyfile

Regtime

Rip.exe

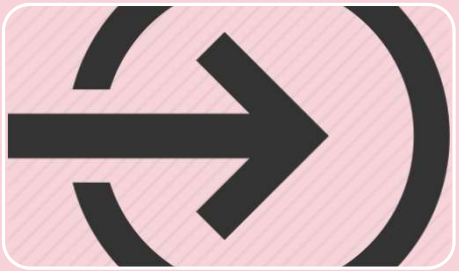
(RegRipper)



Evtparse.exe

EvtxEcmd.exe

evtxECmd_2_tln



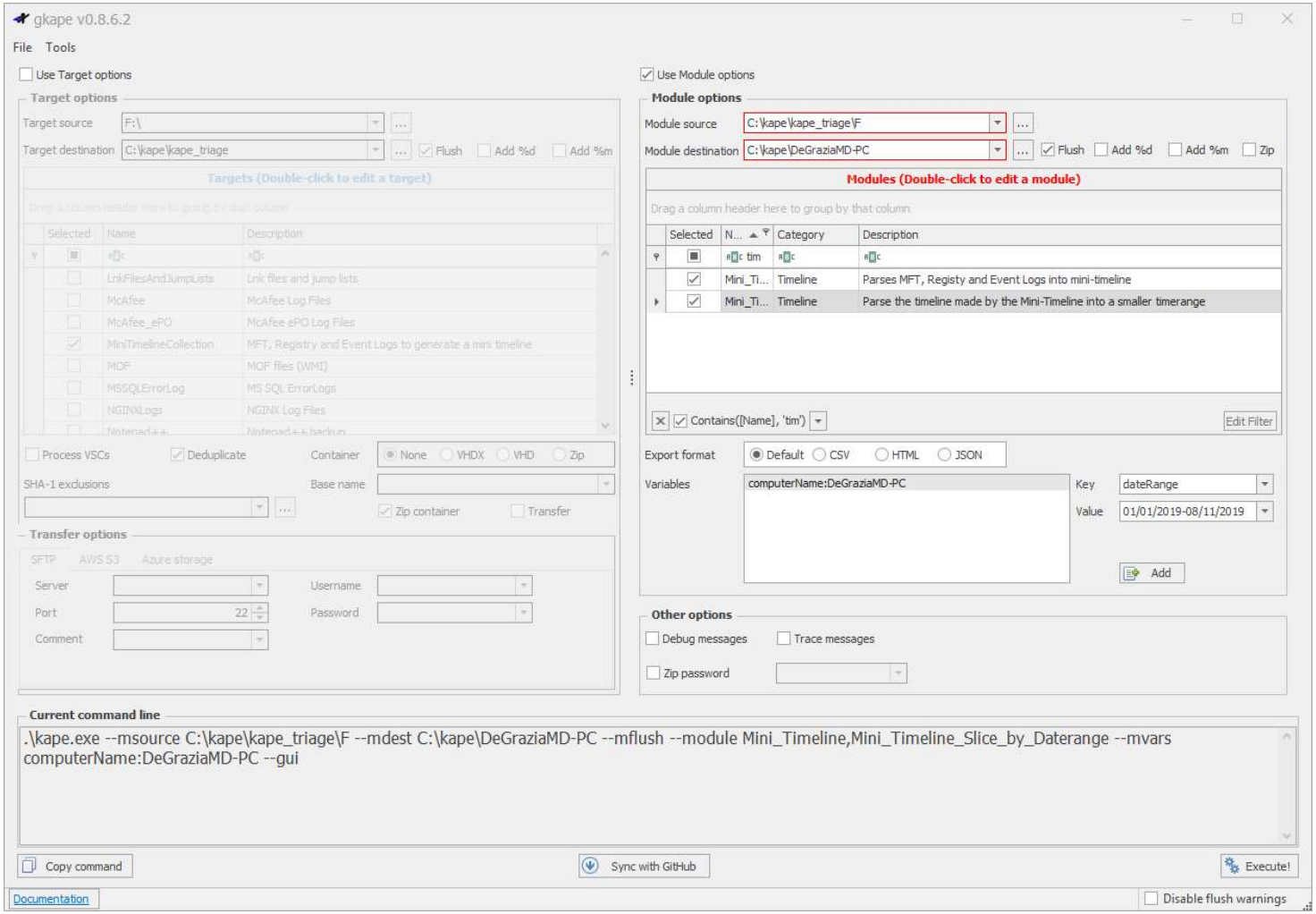
Unicode_2_ascii

Parse.exe

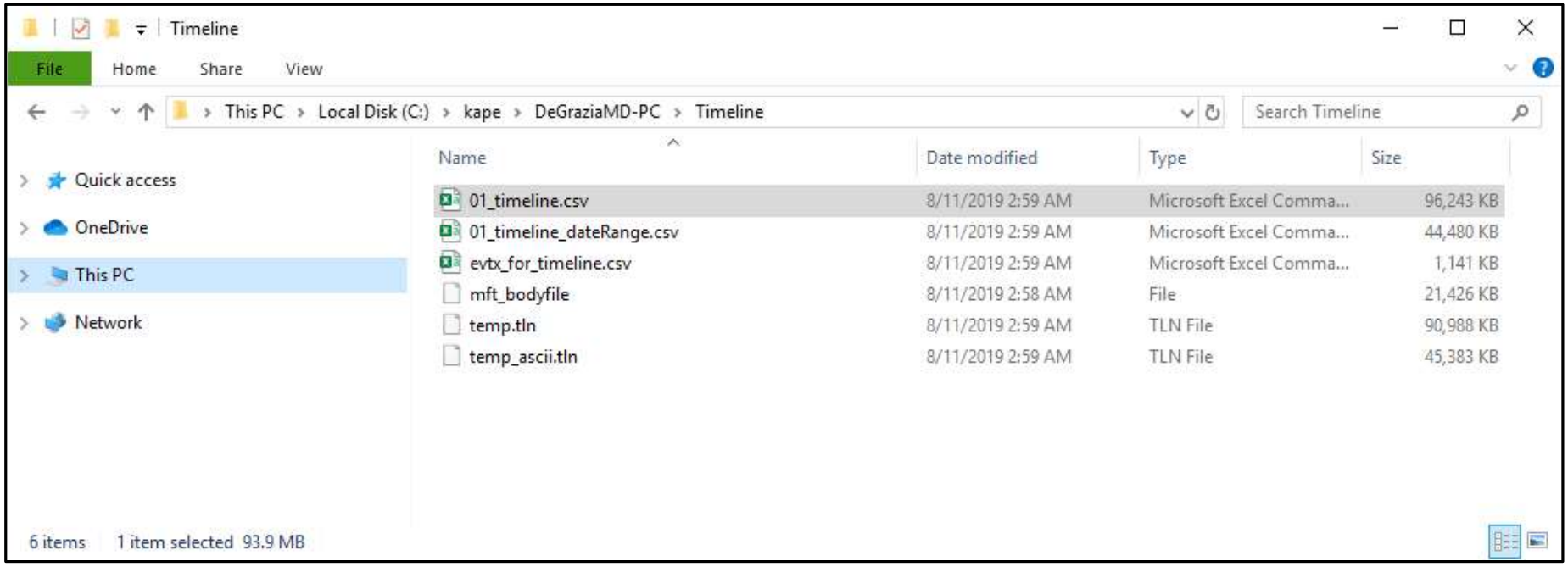
Timelining with KAPE

- Module Name: Mini_Timeline
  Add Key/Value: computerName:Mari-PC

- Module Name: Mini_Timeline_Slice_by_Daterange
  - Add Key/Value: dateRange: 01/01/2019-07/29/2019


gkape v0.8.6.2
File Tools
Use Target options
Target options
Target source F:\
Target destination C:\kape\kape_triage
Flush Add %d Add %m
Targets (Double-click to edit a target)
Drag a column header here to group by that column
Selected Name Description
LnkFilesAndJumpLists Lnk files and jump lists
McAfee McAfee Log Files
McAfee_ePO McAfee ePO Log Files
MiniTimelineCollection MFT, Registry and Event Logs to generate a mini timeline
MOF MOF files (WMI)
MSSQLErrorLog MS SQL ErrorLogs
NGINXLogs NGINX Log Files
Process VSCs Deduplicate Container None VHDX VHD Zip
SHA-1 exclusions Base name
Zip container Transfer
Transfer options
SFTP AWS S3 Azure storage
Server Username
Port 22 Password
Comment
Use Module options
Module options
Module source C:\kape\kape_triage\F
Module destination C:\kape\DeGraziaMD-PC
Flush Add %d Add %m Zip
Modules (Double-click to edit a module)
Drag a column header here to group by that column
Selected N... Category Description
tim
Mini_Ti... Timeline Parses MFT, Registy and Event Logs into mini-timeline
Mini_Ti... Timeline Parse the timeline made by the Mini-Timeline into a smaller timerange
Contains([Name], 'tim')
Edit Filter
Export format Default CSV HTML JSON
Variables computerName:DeGraziaMD-PC
Key dateRange
Value 01/01/2019-08/11/2019
Add
Other options
Debug messages Trace messages
Zip password
Current command line
.\kape.exe --msource C:\kape\kape_triage\F --mdest C:\kape\DeGraziaMD-PC --mflush --module Mini_Timeline,Mini_Timeline_Slice_by_Daterange --mvars computerName:DeGraziaMD-PC --gui
Copy command
Sync with GitHub
Execute!
Documentation
Disable flush warnings

Results


Timeline
File
Home
Share
View
This PC
Local Disk (C:)
kape
DeGraziaMD-PC
Timeline
Search Timeline
Quick access
OneDrive
This PC
Network
Name
Date modified
Type
Size
01_timeline.csv
8/11/2019 2:59 AM
Microsoft Excel Comma...
96,243 KB
01_timeline_dateRange.csv
8/11/2019 2:59 AM
Microsoft Excel Comma...
44,480 KB
evtx_for_timeline.csv
8/11/2019 2:59 AM
Microsoft Excel Comma...
1,141 KB
mft_bodyfile
8/11/2019 2:58 AM
File
21,426 KB
temp.tln
8/11/2019 2:59 AM
TLN File
90,988 KB
temp_ascii.tln
8/11/2019 2:59 AM
TLN File
45,383 KB
6 items
1 item selected 93.9 MB

Analysis

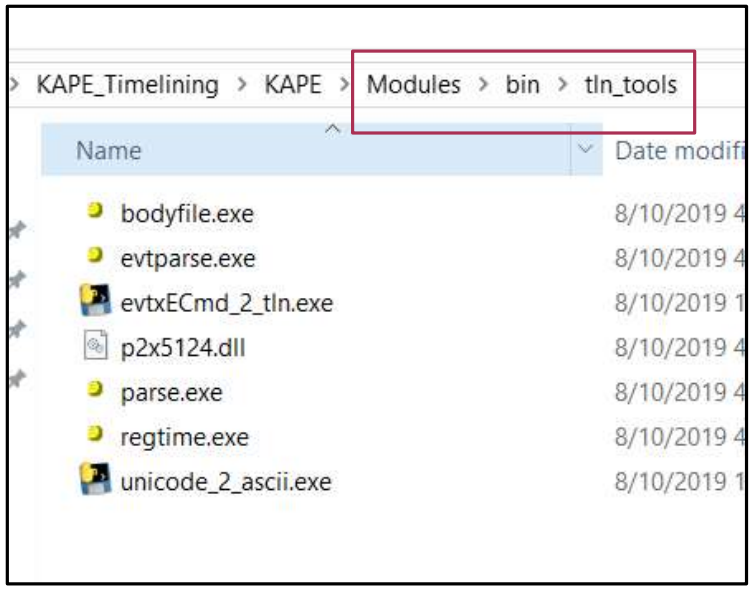
- Pivot Points
- Move up and down for selected time
- Deep dive findings

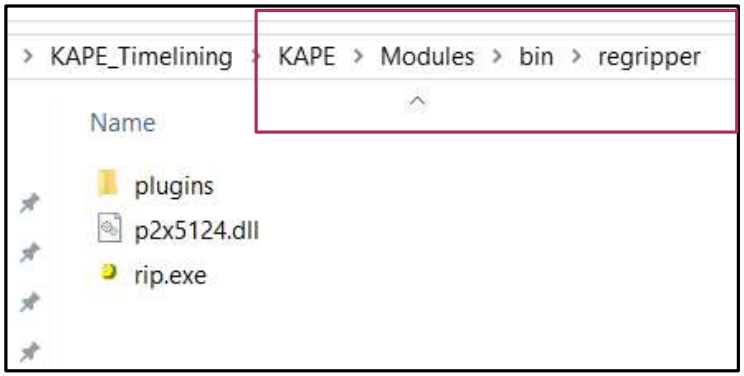
Setup

- Add exe files to the bin folder
  - Check modules for bin path

  Run Get-KAPEUpdate.ps1

  Synch with GitHub





How to make a TLN Module

- Copy existing one
- Modify
  - ExportFile: temp.tln
  - Append: true
  - Change GUID
- Add module to Mini_Timeline.mkape

Questions

- KAPE – free download here
- Eric Zimmerman Tools – https://ericzimmerman.github.io/
- RegRipper – free download: https://github.com/keydet89/RegRipper2.8
- Harlan Carvey's Timeline Tools: https://github.com/keydet89/Tools
- Unicode to Ascii: https://github.com/classicsc/Unicode2Ascii/releases
- evtxECmd_2_tln.exe: https://github.com/mdegrazia/KAPE_Tools

For More **KAPE**:
Intensive Training and Certification

- Virtual live sessions
- Max 25 students

bit.ly/kape2020

SCHEDULE	INSTRUCTORS
June 18, 2020 10:00 a.m. – 7:00 p.m. (EST)	Eric Zimmerman Mari DeGrazia Sean Straw
July 7, 2020 9:00 am – 6:00 pm (GMT + 8, Hong Kong/Singapore time)	Eric Zimmerman Paul Jackson Dave Klopp Rob Phillips

Kroll | A Division of DUFF & PHELPS

For more information about our global locations and services, please visit:
www.kroll.com

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, investigations, disputes, cyber security, compliance and regulatory matters, and other governance-related issues. We work with clients across diverse sectors, mitigating risk to assets, operations and people. With Kroll, a division of Duff & Phelps since 2018, our firm has nearly 3,500 professionals in 28 countries around the world. For more information, visit www.duffandphelps.com.