KAPE

What's all the Buzz About?

A little bit about me

Email:	mark.hallman@gmail.com
	mhallman@sans.org
Skype:	mhallman
Twitter:	@mhallman
GitHub:	bit.ly/KAPE-Portland

Overview

- There is a GitHub page at bit.ly/KAPE-Portland that contains:
  - All the code shown in the slides
  - The hands Labs; question and code to get to the solution
  - Lots of helpful links to useful KAPE documentation
  - These slides
- There will be three hands on sections:
  - Targets
  - Target Output & Timeline Explorer
  - Modules
- Demos of KAPE and other tools along the way

If you have not installed KAPE, try to do it as we start the workshop

Agenda

- What is KAPE?
- Targets & Modules Configurations
- Working with Targets
- Hands On – Targets
- Target Output
- Hands on – Target Output
- Working with Modules
- Hands on - Modules
- Batch Mode
- Questions

What does KAPE Stand for?

Kroll Artifact Parser and Extractor (KAPE)

Huge Thanks to Kroll !!

- Allowing Eric to release KAPE to the DFIR community
- Vision and belief that giving back to the DFIR community by supporting/funding projects like KAPE is extremely important

Evolution of Triage Collection Tools

- Pre-Triage – Full Disk Image
- A properly targeted triage image will capture 95%+ evidentiary significant artifacts … the good stuff
- RoboCopy / Xcopy - copying while maintaining the attributes, timestamps and other properties
  - Scriptable but no Read Only Container
- FTK Imager – Custom Content Images
  - Not Scriptable, but Read Only Container
- CyLR
  - Scriptable, no Read Only Container, limited post collection processing

Introducing KAPE

Search

for files & folders using target configurations

Collect

responsive files & folders

Process

Collected files based on Module Configurations

- Can Search the Following
  - Mounted E01
  - Live System Drive(s)
  - Directory
  - F-Response
  - Optional VSCs
- Forensically sound
- Detailed copy log
- Optional VHD(x) or Zip container
- SFTP transfer
- Extract actionable intelligence
- Facilitate artifact correlation/pivoting
- Consistent and Repeatable Output for Analysis

Highly Configurable & Scriptable

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Targets & Modules

- KAPE divides its functionality into two parts:
  - Targets
  - Modules
- Targets collect files/folders
- Modules process files/folders
  - Can also run programs to collect memory or other live response data
- These operations can be done independently of each other, or combined

KAPE Component Interaction

Target Config Files

Granular, targeted searches are defined in these files.

KAPE Engine

KAPE is the engine that makes everything happen, but only with direction via Targets, Modules and command line switches.

CLI Options

KAPE command line options pull everything together to produce your results, in the format you choose.

Modules

Modules define the processing tools and options that will be run against source data.

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Why is it different?

- Fast - Collecting and processing times are measurably faster
- GUI & Command Line – portable, no install
- Can Collect Locked files like registry hives
- Can Process collected data
- Highly Configurable & Scriptable
- Batch Mode
- Output Options including zipped and VHDX
- DFIR Community support - adding new targets and modules
- Eric's openness to feedback and responsiveness to updating the code

Configuration Files

Target Configs

- Define What We Collect
- File and Folder File Masks that Define Artifacts to Search For
- Can be broad or very focused
- Granular == Flexibility == Speed
- Large Set of Existing Configs
- Create your own

$KAPE_HOME/kape/targets

Module Configs

- Defines the What / How to process
  - Scripts
  - Programs
- Single exe / Module
- Assigned to a Single “Category”

$KAPE_HOME/kape/modules

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Configurations File Examples

Target Configs

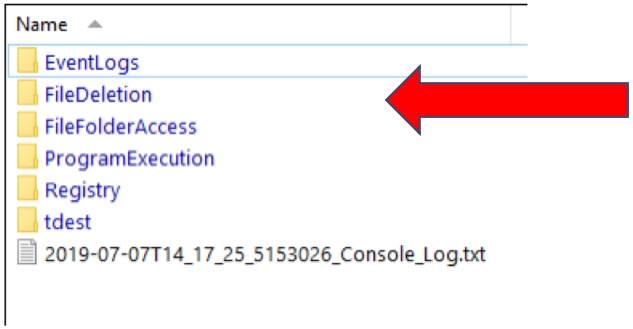
```
Description: Amcache.hve
Author: Eric Zimmerman
Version: 1
Id: 13ba1e33-4899-4843-adf1-c7e6b20d759a
RecreateDirectories: true
Targets:
  -
    Name: Amcache
    Category: ApplicationCompatibility
    Path: C:\Windows\AppCompat\Programs\Amcache.hve
    IsDirectory: false
    Recursive: false
    Comment: ""
  -
    Name: Amcache transaction files
    Category: ApplicationCompatibility
    Path: C:\Windows\AppCompat\Programs\Amcache.hve.LOG*
    IsDirectory: false
    Recursive: false
    Comment: ""
```

Module Configs

```
Description: 'AmcacheParser: extract program execution
information'
Category: ProgramExecution
Author: Eric Zimmerman
Version: 1
Id: 4190c518-524f-4623-8038-a014784c018c
BinaryUrl:
https://f001.backblazeb2.com/file/EricZimmermanTools/AmcacheP
arser.zip
ExportFormat: csv
FileMask: Amcache.hve
Processors:
  -
    Executable: AmcacheParser.exe
    CommandLine: -f %sourceFile% --csv %destinationDirectory% -i
    ExportFormat: csv
```

Module Categories

- Grouping Module output Relies on Categories
- SANS Evidence of Categories are good categories to use
- You can create your own, but…



Existing Module Categories

1. AntiVirus
2. EventLogs
3. ExifData
4. FileDeletion
5. FileFolderAccess
6. ProgramExecution
7. Registry
8. IOCs
9. LiveResponse
10. Memory
11. Passwords
12. Webservers
13. RemoteAccess
14. SystemActivity
15. VolumeInformation

User Communications

File Download

Program Execution

Deleted File or File Knowledge

Network Activity / Physical Location

File/Folder Opening

Account Usage

External Device / USB Usage

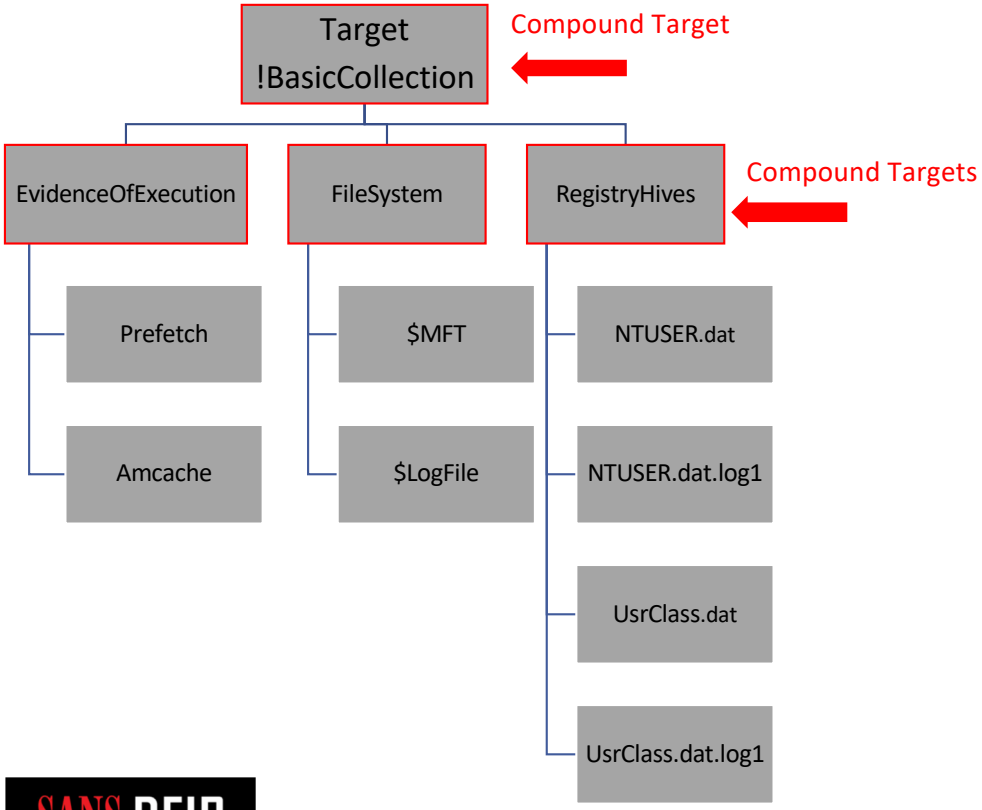
Browser Usage

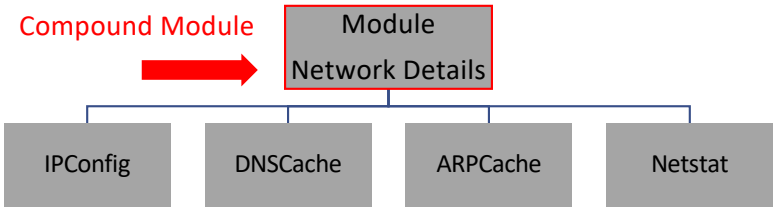
SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

YAML is used for Configuration Files

- Pro Tips
  - Copy an Existing Config file and edit
  - On-line YAML Validation
    - https://codebeautify.org/yaml-validator
    - https://jsonformatter.org/yaml-validator
  - With YAML, the tiniest things matter
  - Tabs == BAD

Compound Target & Module Configs





SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Current List of Available Targets

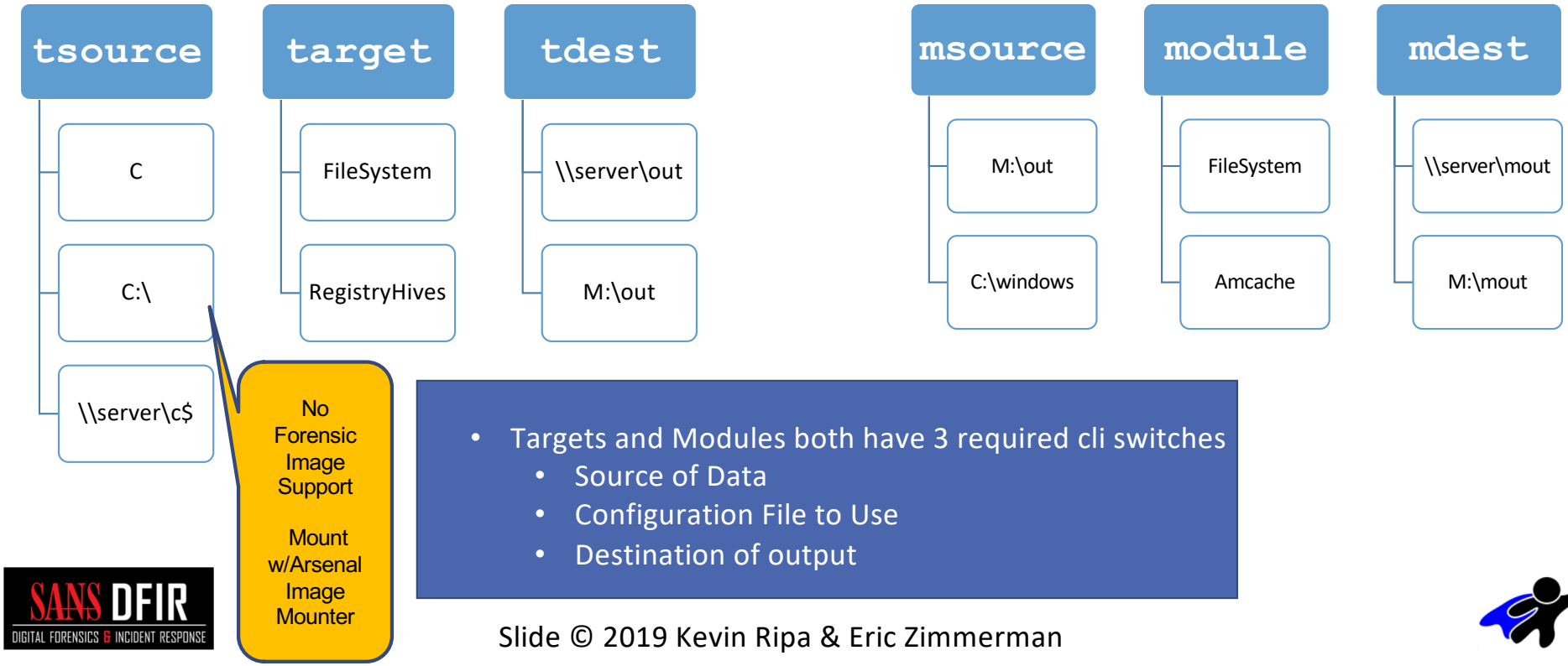
ApacheAccessLog.tkape
BCD.tkape
Chrome.tkape
CiscoJabber.tkape
CombinedLogs.tkape
ConfluenceLogs.tkape
Edge.tkape
EncapsulationLogging.tkape
EventLogs.tkape
EventTraceLogs.tkape
EvidenceOfExecution.tkape
Exchange.tkape
ExchangeClientAccess.tkape
ExchangeTransport.tkape
FileSystem.tkape
Firefox.tkape
Gigatribe.tkape
IISLogFiles.tkape
InternetExplorer.tkape
iTunesBackup.tkape
LinuxOnWindowsProfileFiles.tkape
LnkFilesAndJumpLists.tkape
McAfee.tkape
MOF.tkape
MSSQLErrorLog.tkape
NGINXLogs.tkape
Notepad++.tkape
OutlookPSTOST.tkape
PowerShellConsole.tkape
RDPCache.tkape
Recycle.tkape
RegistryHives.tkape
ScheduledTasks.tkape
SDB.tkape
SignatureCatalog.tkape
Skype.tkape
SRUM.tkape
StartupInfo.tkape
Symantec_AV_Logs.tkape
Symantec_Daily_AV.tkape
Syscache.tkape
TeamViewerLogs.tkapeTeraCopy.tkape
ThumbCache.tkape
TorrentClients.tkape
Torrents.tkape
USBDevicesLogs.tkape
VirtualDisks.tkape
VNCLogs.tkape
WBEM.tkape
WebBrowsers.tkape
WER.tkape
WindowsFirewall.tkape
WindowsIndexSearch.tkape
WindowsNotifcationsDB.tkape
XPRestorePoints.tkape

Current List of Available Modules

AmcacheParser
Apache_Access_Log
AppCompatCacheParser
ApplicationEvents
ApplicationFullEventLogView
ARPCache
autoruns
bitlocker-key
BrowsingHistoryView
CCM-RUA
DensityScout
Detailed-Network-Share-Access
DNSCache
DumpIt
EvtxECmd
exiftool
Get-DoSvcExternalIP
Get-InjectedThread
Get-NetworkConnection
handle
Hashes
Hindsight
IPConfig
iTunesBackup
JLECmd
LECmd
Logon-Logoff-events
manage-bde
MFTECmd
MFTECmd_$Boot
MFTECmd_$J
MFTECmd_$MFT
MFTECmd_$SDS
NBTStat_NetBIOS_Cache
NBTStat_NetBIOS_Sessions
NetStat
NetworkDetails
PECmd
Plaso
PowerShell
PowershellOperationalFullEventLogView
PrintServiceOperationalFullEventLogView
ProcessDetails
psfile
psinfo
pslist
psloggedon
psservice
pstree
PWSH-Get-ProcessList
RBCmd
RDP-Usage-events
RDPCoreTS
RecentFileCacheParser
RECmd
Registry_System
RegRipper-ALL
RegRipper-ntuser
RegRipper-sam
RegRipper-security
RegRipper-software
RegRipper-system
RoutingTable.mkape
SBECmd.mkape
ScheduledTasksFullEventLogView.mkape
SecurityEvents.mkape
SecurityFullEventLogView.mkape
SEPM_Logs.mkape
SigCheck.mkape
SMB-Server-Anonymous-Logon.mkape
SparkCore.mkape
srum-dump.mkape
Symantec_Control_Log.mkape
Symantec_Daily_AV.mkape
Symantec_Security_Log.mkape
Symantec_System_Log.mkape
Symantec_Tamper_Protection_Log.mkape
SystemEvents.mkape
SystemFullEventLogView.mkape
TaskScheduler.mkape
tcpvcon.mkape
TeraCopy-history.mkape
TeraCopy-main.mkape
TS-LSM.mkape
TS-RCM.mkape
usbdeviceforensics.mkape
WindowsEventLogs.mkape
WinPmem.mkape
WxTCmd.mkape

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

Required Parameters

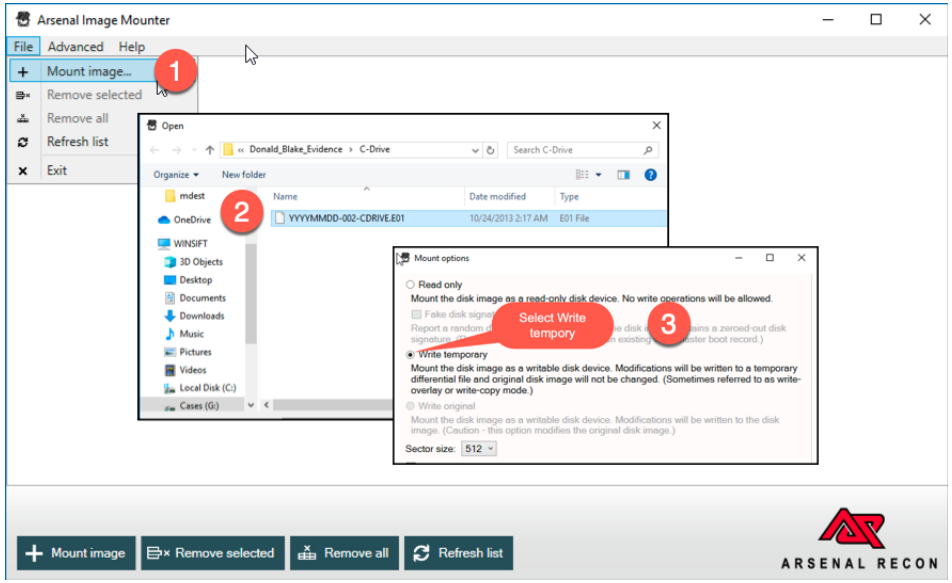


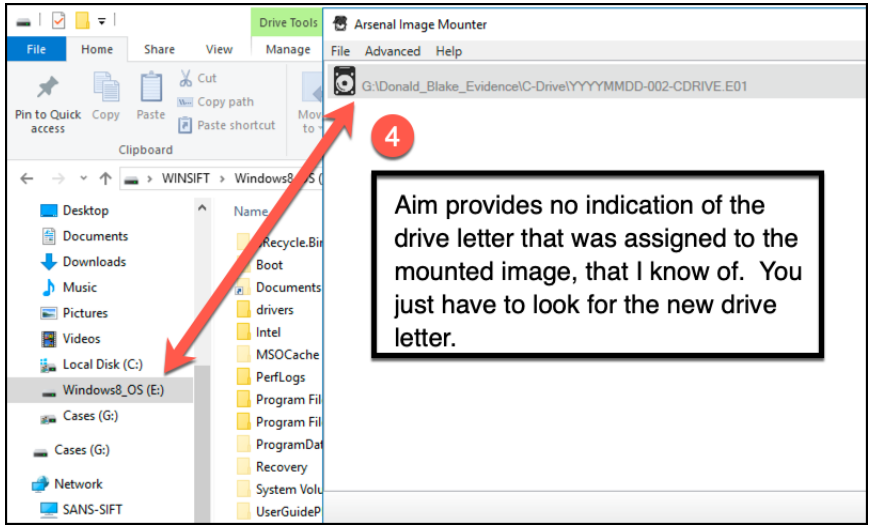
- Targets and Modules both have 3 required cli switches
  - Source of Data
  - Configuration File to Use
  - Destination of output

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

KAPE– Mounting Forensic Images

- KAPE can't read forensics images like an E01
- Mount images with free Arsenal Image Mounter tool





Command Line Basics

Required cli switches

tsource	Target source drive to copy files from (C, D:, or G:\ for example)
target	Target configuration to use
tdest	Destination directory to copy files to. %d will be expanded to a timestamp (yyyyMMddTHHmmss). If --vhdx, --vhd or --zip is set, files will end up in VHD(X) container or zip file

```
kape --tsource <target C:> --target <target-name(s)>
--tdest <target-destination>
```

```
kape --tsource C: --target LnkFilesAndJumpLists
--tdest G:\kape_out\tdest
```

More Target cli

- Single Compound Target
- Flush – delete all the data from the target destination
- Save the files in a VHDX (which is compressed by default)
- Use an environment variable for the base part of the VHDX file name

```
kape --tsource C: --target EvidenceOfExecution
--tflush
--tdest G:\kape_out\tdest
--vhdx $env:ComputerName
```

```
Description: Evidence of execution related files
Author: Eric Zimmerman
Version: 1
Id: 13ba1e33-4899-4843-adf0-c7e6a20d758a
RecreateDirectories: true
Targets:
   -
      Name: Prefetch
      Category: Prefetch
      Path: C:\Windows\prefetch\*.pf
      IsDirectory: false
      Recursive: false
      Comment: ""
   -
      Name: RecentFileCache
      Category: ApplicationCompatability
      Path:
C:\Windows\AppCompat\Programs\RecentFileCache.bcf
      IsDirectory: false
      Recursive: false
      Comment: ""
   -
      Name: Amcache
      Category: ApplicationCompatability
      Path: Amcache.tkape
      IsDirectory: false
      Recursive: false
      Comment: ""
   -
      Name: Syscache
      Category: Syscache
      Path: Syscache.tkape
      IsDirectory: false
      Recursive: false
      Comment: ""
```

More Target cli

- Single Compound Target
- Destination is a UNC Path
- Extracts targets from Volume Shadow Copies

```
kape --tsource C --target RegistryHives --vss
--tflush --tdest \\share\DFIR\kape_out\tdest
--vhdx $env:ComputerName
```

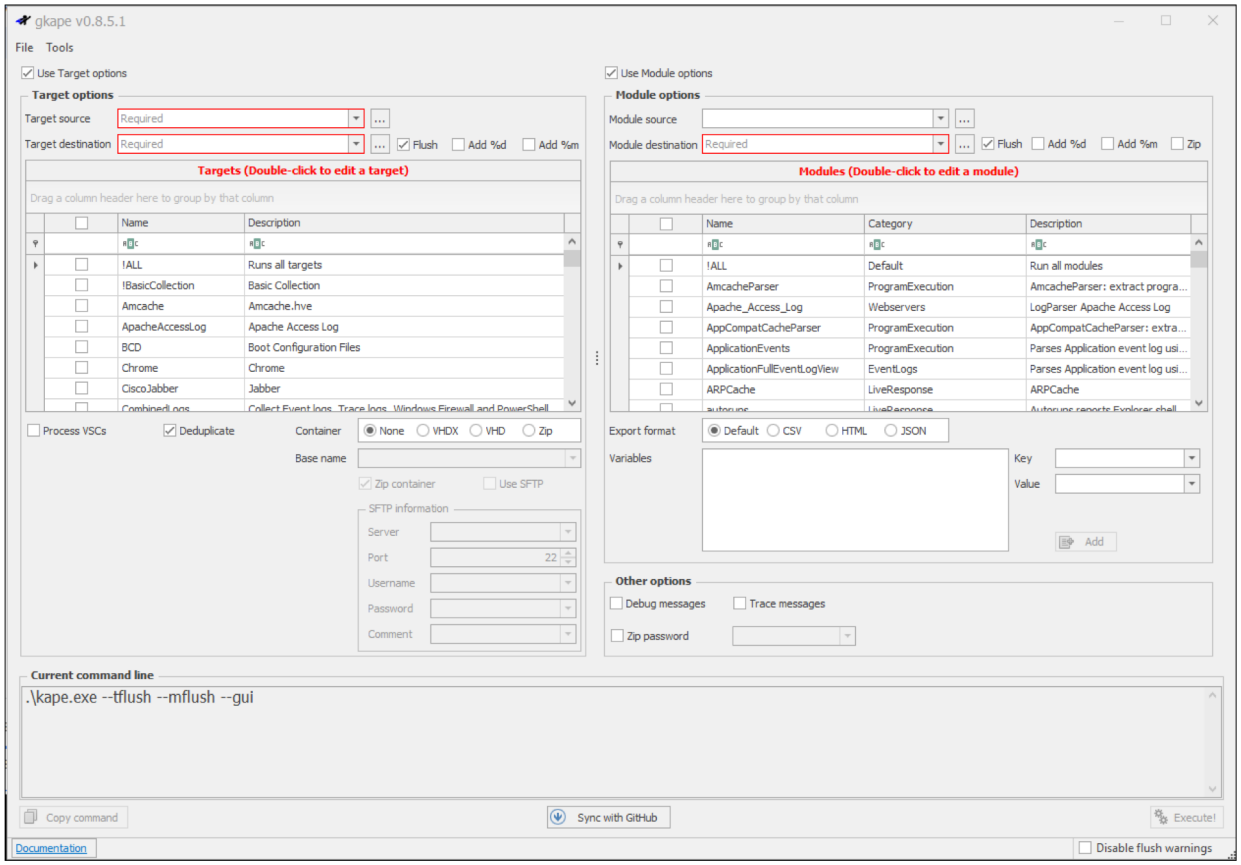
More Target cli

- Multiple Compound Targets
- Source is a file share referenced with UNC Path
- Destination is also a UNC Path
- Extract files from the VSS & dedupe them
- Send data to a

scs - SFTP server host/IP for transferring *compressed VHD(X)* container
scp - SFTP server port. Default is 22
scu - SFTP server username. Required when using --scs
scpw - SFTP server password
scc - Comment to include with transfer. Useful to include where a transfer came from. Defaults to the name of the machine where KAPE is running

```
kape --tflush --tsource C: --target RegistryHives,
LnkFilesAndJumpLists, EvidenceOfExecution  --tdest
C:\temp\tout –vss –tdd --vhdx $env:ComputerName
--scs 104.248.94.196 --scp 22 --scu kape-ssh --scpw "KAP3g0at"
```

GKAPE (GUI KAPE)



Checkout Eric Zimmerman's

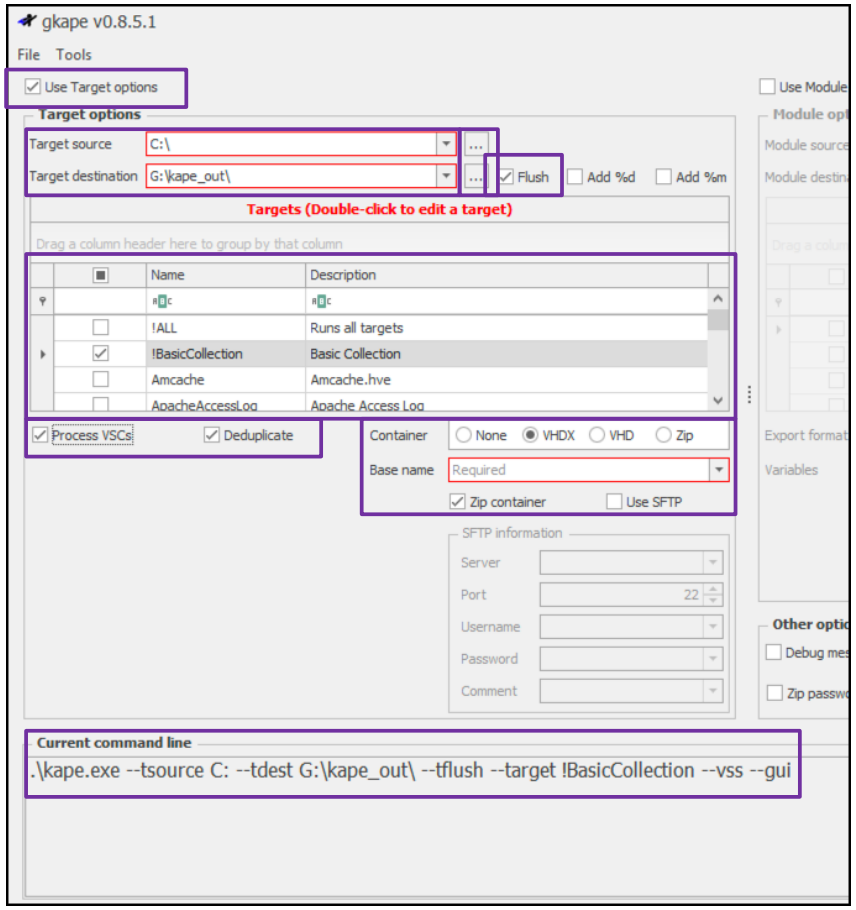
Exploring KAPE's Graphical User Interface

Link on this Workshop's GitHub Page

https://github.com/mark-hallman/DFRWS-2019-KAPE-Workshop

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

GKAPE - Targets



Hands On Lab

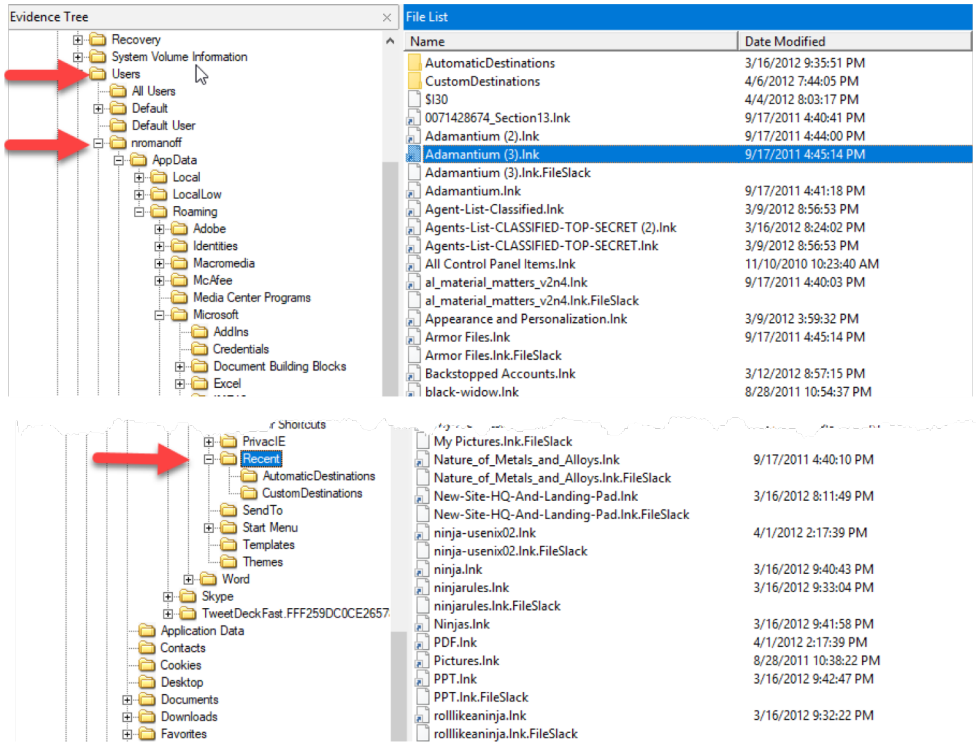
Working with Targets

Examples of Target Output

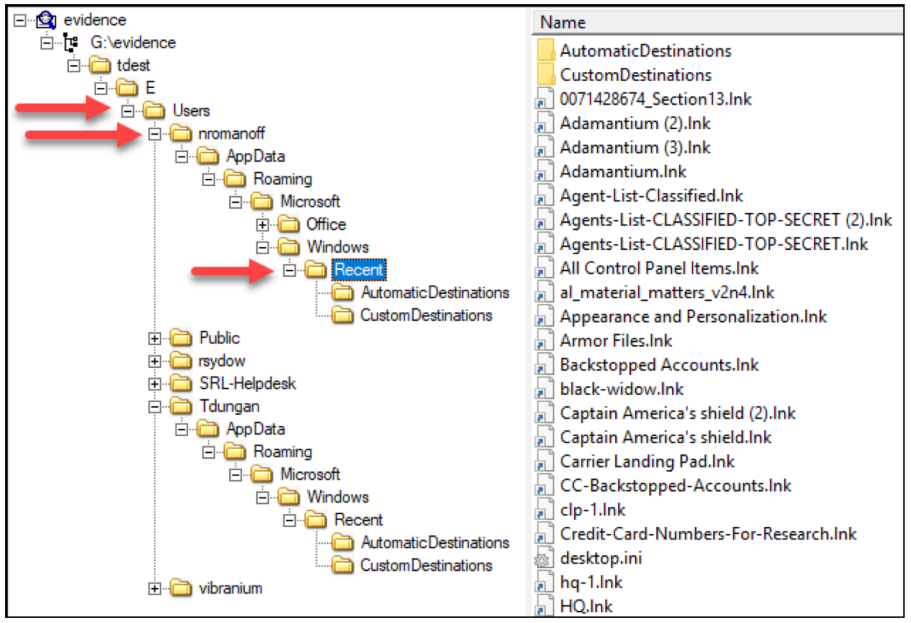
- Replicate the Folder structure
- Containers
  - VHDXs, VHDs, zip
  - zipped and unzipped
  - Volume Shadow Copies (vss)
- Log files

Replicated Folder Structure

View of Target Output in tdest



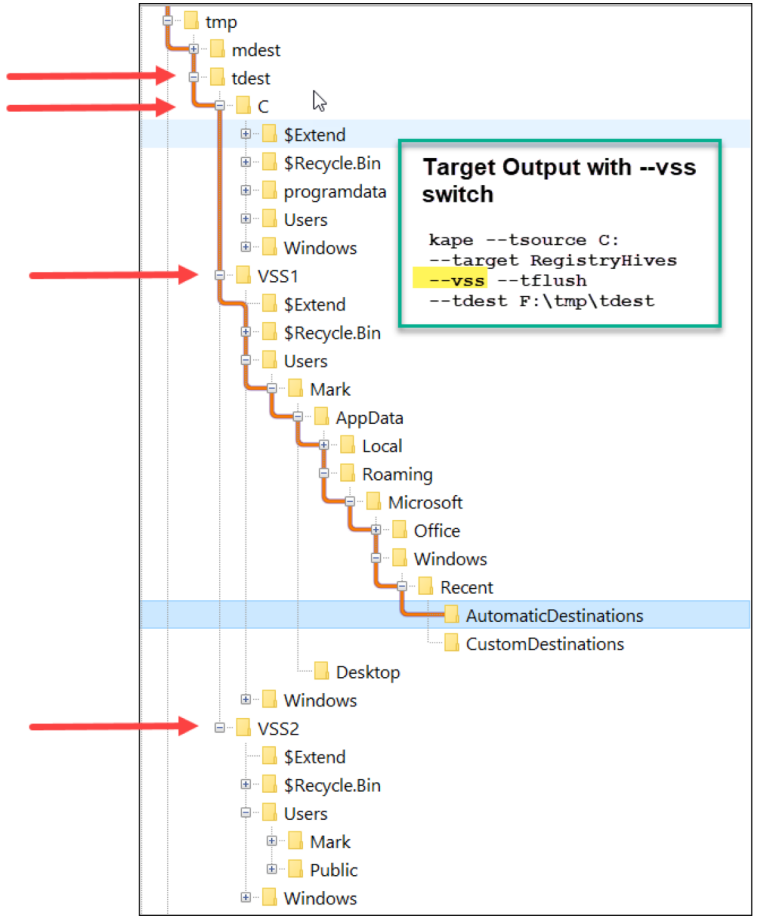
View of Source in FTK Imager



Targets ▸ SRUM.tkape

```
1  Description: System Resource Usage Monitor
2  Author: Mark Hallman
3  Version: 1
4  Id: 9858f1fc-5e22-46a0-8bfd-c821ac9b4a13
5  RecreateDirectories: true
6  Targets:
```

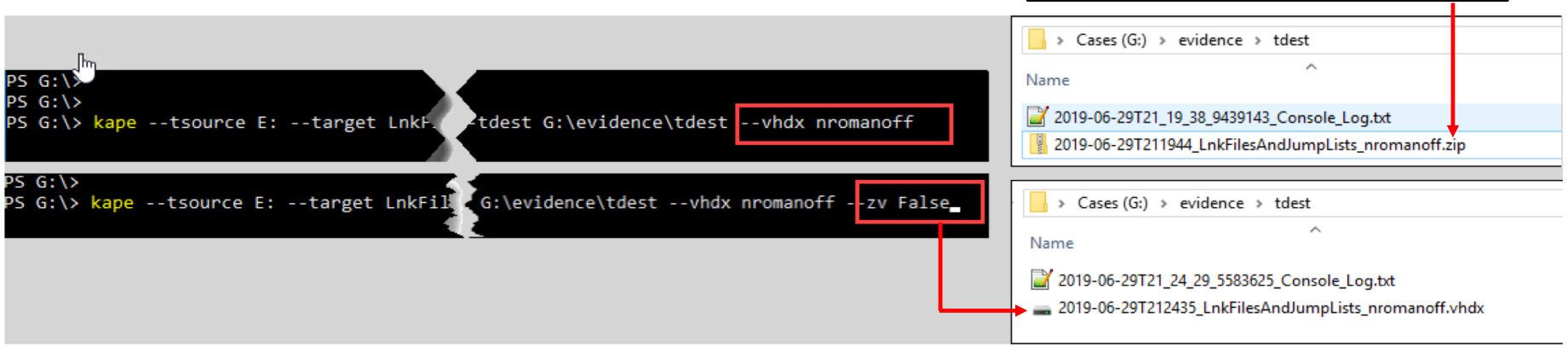
Volume Shadow Copy Output



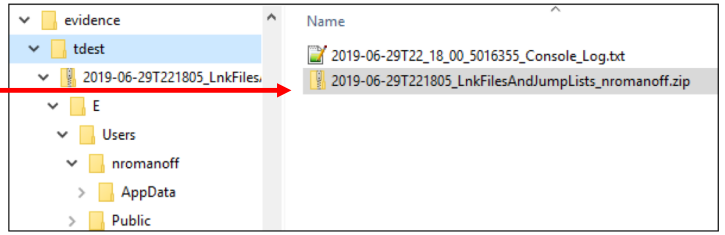
Containers for Target Output

- --vhdx - The base name of the VHDX file

Zipped VHDX is default for --vhdx



- --vhd - The base name of the VHD file
- --zip - The base name of the ZIP file

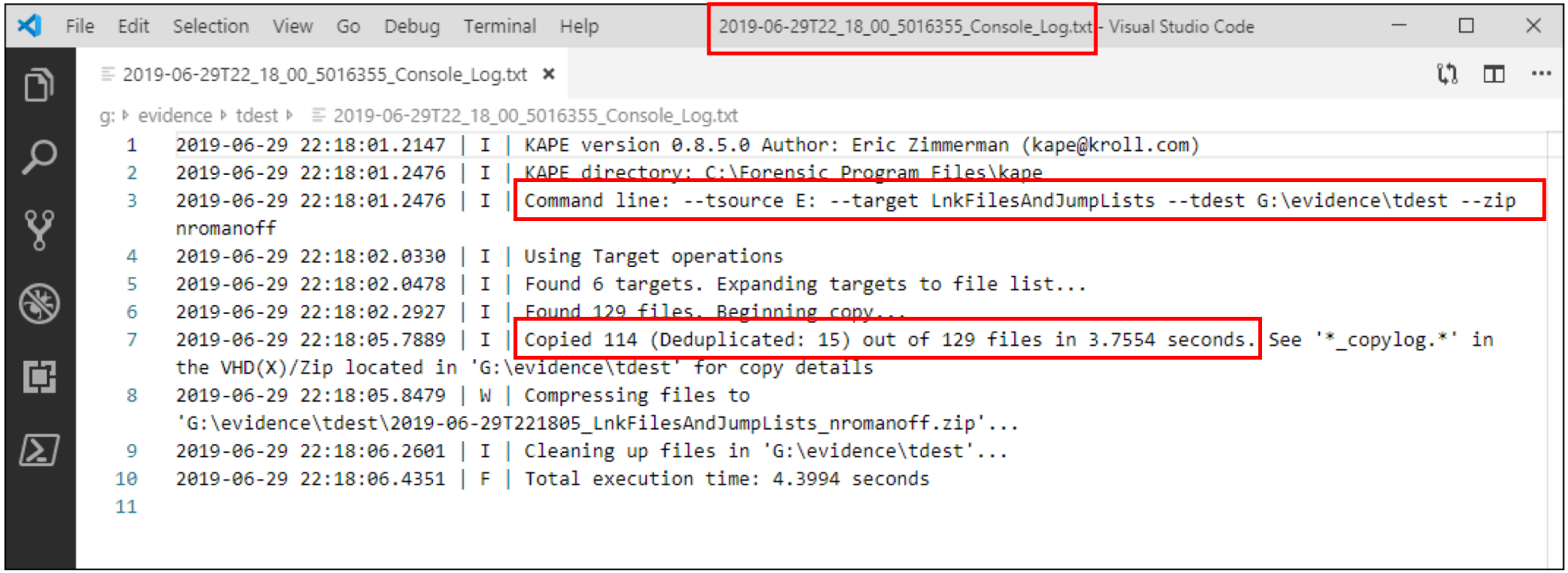


Output Logs

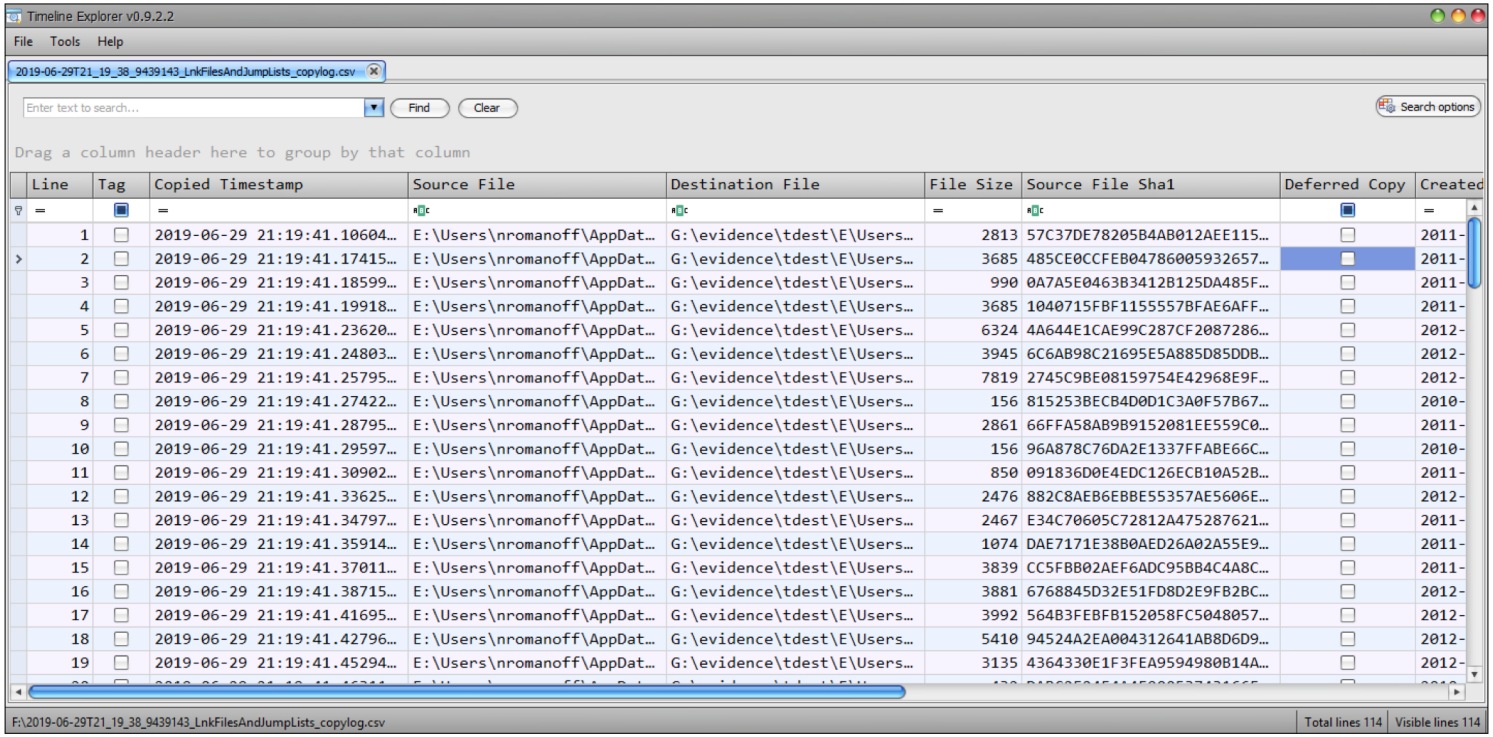
3 log files generated for targets

- %d_Console_Log.txt
- %d_target_copylog.txt
- %d_target_copylog.csv

Console_Log.txt



Copylog.csv


Timeline Explorer v0.9.2.2
File Tools Help
2019-06-29T21_19_38_9439143_LnkFilesAndJumpLists_copylog.csv
Enter text to search...
Find
Clear
Search options
Drag a column header here to group by that column
Line | Tag | Copied Timestamp | Source File | Destination File | File Size | Source File Sha1 | Deferred Copy | Created
1 2019-06-29 21:19:41.10604… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 2813 57C37DE78205B4AB012AEE115… 2011-
2 2019-06-29 21:19:41.17415… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 3685 485CE0CCFEB04786005932657… 2011-
3 2019-06-29 21:19:41.18599… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 990 0A7A5E0463B3412B125DA485F… 2011-
4 2019-06-29 21:19:41.19918… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 3685 1040715FBF1155557BFAE6AFF… 2011-
5 2019-06-29 21:19:41.23620… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 6324 4A644E1CAE99C287CF2087286… 2012-
6 2019-06-29 21:19:41.24803… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 3945 6C6AB98C21695E5A885D85DDB… 2012-
7 2019-06-29 21:19:41.25795… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 7819 2745C9BE08159754E42968E9F… 2012-
8 2019-06-29 21:19:41.27422… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 156 815253BECB4D0D1C3A0F57B67… 2010-
9 2019-06-29 21:19:41.28795… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 2861 66FFA58AB9B9152081EE559C0… 2011-
10 2019-06-29 21:19:41.29597… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 156 96A878C76DA2E1337FFABE66C… 2010-
11 2019-06-29 21:19:41.30902… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 850 091836D0E4EDC126ECB10A52B… 2011-
12 2019-06-29 21:19:41.33625… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 2476 882C8AEB6EBBE55357AE5606E… 2012-
13 2019-06-29 21:19:41.34797… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 2467 E34C70605C72812A475287621… 2011-
14 2019-06-29 21:19:41.35914… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 1074 DAE7171E38B0AED26A02A55E9… 2011-
15 2019-06-29 21:19:41.37011… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 3839 CC5FBB02AEF6ADC95BB4C4A8C… 2011-
16 2019-06-29 21:19:41.38715… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 3881 6768845D32E51FD8D2E9FB2BC… 2012-
17 2019-06-29 21:19:41.41695… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 3992 564B3FEBFB152058FC5048057… 2012-
18 2019-06-29 21:19:41.42796… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 5410 94524A2EA004312641AB8D6D9… 2012-
19 2019-06-29 21:19:41.45294… E:\Users\nromanoff\AppDat… G:\evidence\tdest\E\Users… 3135 4364330E1F3FEA9594980B14A… 2012-
F:\2019-06-29T21_19_38_9439143_LnkFilesAndJumpLists_copylog.csv
Total lines 114
Visible lines 114

Demo Timeline Explorer

Hands On Lab

Working with Targets Output

Modules
Process the collected data

Basic Module cli

Required cli switches

msource	Module source folder to process files from
module	Module configuration to use
mdest	Destination directory to copy files for processing output. RTFM for more on --tdest

```
kape --msource <target C:> --module <module-name(s)>
--mdest <module-destination>
```

```
kape --msource G:\kape_out\tdest --module LECmd,JLEcmd
--mdest G:\kape_out\mdest
```

More Module cli

- Processing data collected by the Compound Target, EvidenceOfExecution
- Requires more that one Module (at least with the currently defined modules, you could create one

```
kape --msource G:\kape_out\tdest
--module PECmd,AmcacheParser
--mflush --mdest G:\kape_out\mdest
```

```
Description: Evidence of execution related files
Author: Eric Zimmerman
Version: 1
Id: 13ba1e33-4899-4843-adf0-c7e6a20d758a
RecreateDirectories: true
Targets:
  -
    Name: Prefetch
    Category: Prefetch
    Path: C:\Windows\prefetch\*.pf
    IsDirectory: false
    Recursive: false
    Comment: ""
  -
    Name: RecentFileCache
    Category: ApplicationCompatability
    Path:
C:\Windows\AppCompat\Programs\RecentFileCache.bcf
    IsDirectory: false
    Recursive: false
    Comment: ""
  -
    Name: Amcache
    Category: ApplicationCompatability
    Path: Amcache.tkape
    IsDirectory: false
    Recursive: false
    Comment: ""
  -
    Name: Syscache
    Category: Syscache
    Path: Syscache.tkape
    IsDirectory: false
    Recursive: false
    Comment: ""
```

Module Config Vars

- Used to replace parameters in the cli
- KAPE has some Variables built in
- “mvars” can be used to provide additional vars to commands used in modules

KAPE Variable	Description
%sourceDirectory%	Full path to the dir where all filescan be found
%destinationDirectory%	Full path to the root directory where a file will be saved
%sourceFile%	
%kapeDirectory%	Contains the full path to where KAPE was launched
%fileName%	The file name being processed by a module
%computername% - cmd $env:ComputerName - PowerShell	

Modules Variables (mvars)

- --mvars allows you to pass in your own vars
- Modules must be created to accept the the mvars
- Vars are key:value pairs – not positional

Existing Module

```
Executable: EvtxECmd.exe
CommandLine: -d %sourceDirectory% --csv %destinationDirectory%
```

Cmd we want to have KAPE run

```
EvtxECmd.exe -d G:\kape_out\tdest\C --csv G:\kape_out\mdest --inc evtx_id:"4624,4625" --sd start_date: "2019-03-02 03:00:00"
```

New Module

```
Executable: EvtxECmd.exe
CommandLine: -d %sourceDirectory% --csv %destinationDirectory% --inc %evtx_id% --sd %start_date%
```

New Command using --mvars

```
kape --msource G:\kape_out\tdest\C  --module Evtxcustom --mdest G:\kape_out\mdest --mvars "evtx_id:4624,4625","start_date: 2019-02-01 03:00:00"
```

Batch Mode

- Batch mode is driven by creating a file named _kape.cli and adding one or more kape command lines in the file.
- Place the _kape.cli file in the same folder as the kape.exe.
- Remember that a module can only contain one executable, Batch Mode is one mechanism to run multiple modules
- Consistency and Repeatability. Same script used on all custodians.
- Spawns a instance of KAPE for line in the _kape.cli file.
  - Structure your batch file(s) or jobs to allow Target Completion before Module Start.
- Ending a line in the file with **"--gui"** will keep each spawned window open for review.

Batch Mode Example

1

```
cape --tsource C: --target !BasicCollection --tdest G:\tmp\tdest --tflush
--vss --tdd
```

2

_kape.cli is moved to KAPE folder

3

```
--msource G:\tmp\tdest --module AmcacheParser --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module EvtxECmd,Prefetch,PECmd      --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module RecentFileCacheParser --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module MFTECmd_$MFT,MFTECmd_$J,MFTECmd_$SDS,MFTECmd_$Boot --mdest
G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module JLECmd,LECmd --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module RBCmd --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module RECmd --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module SRUM-Dump --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module usbdeviceforensics --mdest G:\tmp\mdest --mflush --gui
--msource G:\tmp\tdest --module WxTCmd --mdest G:\tmp\mdest --mflush --gui
```


Batch Mode

```
1 --tsource c: --tdest G:\kape_out\tdest --tflush --target
  EvidenceOfExecution --vss --tdd --msource G:\kape_out\tdest --mdest
  G:\kape_out\mdest\ --module Prefetch, RecentFileCacheParser,
  AmcacheParser, RECmdSysCache
```

We know this won't work because of timing

```
1 --tsource c: --tdest G:\kape_out\tdest --tflush --target
  EvidenceOfExecution --vss --tdd
2 --msource G:\kape_out\tdest --mdest G:\kape_out\mdest\ --module Prefetch,
  RecentFileCacheParser, AmcacheParser, RECmdSysCache
3
```

SANS DFIR
DIGITAL FORENSICS & INCIDENT RESPONSE

KAPE at Scale

```
$tkape_cmd = {cmd.exe /c "c:\temp\kape\kape.exe --
tsource c: --tflush --tdest c:\temp\output\target --
target $Using:targets --vhdx $env:ComputerName --
msource c:\temp\output\target --mflush --mdest
c:\temp\output\module --zm TRUE --module
$Using:modules"}

Invoke-Command -ComputerName (Get-Content
Computers.txt) -ScriptBlock $tkape_cmd
```