

# KAPE

## Task 2 Introduction to KAPE

From amongst kape.exe and gkape.exe, which binary is used to run GUI version of KAPE?

gkape.exe

## Task 3 Target Options

What is the file extension for KAPE Targets?

.tkape

What type of Target will we use if we want to collect multiple artifacts with a single command?

Compound targets

## Task 4 Module Options

What is the file extension of the Modules files?

mkape

What is the name of the directory where binary files are stored, which may not be present on a typical system, but are required for a particular KAPE Module?

bin

## Task 5 KAPE GUI

In the second to last screenshot above, what target have we selected for collection?

KapeTriage

In the second to last screenshot above, what module have we selected for processing?

!EZParser

What option has to be checked to append date and time information to triage folder name?

%d

What option needs to be checked to add machine information to the triage folder name?

%m

## Task 6 KAPE CLI

```
C:\Users\THM-4n6\Desktop\KAPE>kape.exe -h
KAPE version 1.1.0.1 Author: Eric Zimmerman (kape@kroll.com)

    tsource      Target source drive to copy files from (C, D:, or F:\ for example)
    target       Target configuration to use
    tdest        Destination directory to copy files to. If --vhdx, --vhd or --zip is set, files will end up
    tlist        List available Targets. Use . for Targets directory or name of subdirectory under Targets.
    tdetail      Dump target file details
    tflush       Delete all files in 'tdest' prior to collection
    tvars        Provide a list of key:value pairs to be used for variable replacement in Targets. Ex: --tvar
    --start-time Multiple pairs should be connected by a
```

```
    debug        Show debug information during processing
    trace        Show trace information during processing

    gui          If true, KAPE will not close the window it executes in when run from gkape. Default is FALSE
    ul           When using _kape.cli, when true, KAPE will execute entries in _kape.cli one at a time vs. in parallel. Default
    cu           When using _kape.cli, if true, KAPE will delete _kape.cli and both Target/Module directories upon exiting. Defa

    sftpc        Path to config file defining SFTP server parameters, including port, users, etc. See documentation for examples
    sftp         When true, show passwords in KAPE switches for connection when using --sftpc. Default is TRUE

    rlc          If true, local copy of transferred files will NOT be deleted after upload. Default is FALSE
    guids        KAPE will generate 10 GUIDs and exit. Useful when creating new Targets/Modules. Default is FALSE
    sync         If true, KAPE will download the latest Targets and Modules from specified URL prior to running. Default is http

    ifw          If false, KAPE will warn if a process related to FTK is found, then exit. Set to true to ignore this warning an

Variables: %d = Timestamp (yyyyMMddTHH:mm:ss)
           %s = System drive letter
           %m = Machine name
```

Run the command `kape.exe` in an elevated shell. Take a look at the different switches and variables. What variable adds the collection timestamp to the target destination?

%d

What variable adds the machine information to the target destination?\

%m

Which switch can be used to show debug information during processing?

debug

Which switch is used to list all targets available?

tlist

Which flag, when used with batch mode, will delete the `_kape.cli`, targets and modules files after the execution is complete?

cu

## Task 7 Hands-on Challenge

I saved the target destination as target and module destination as output in the task 5 kape gui , we are going to use them

**Two USB Mass Storage devices were attached to this Virtual Machine. One had a Serial Number 0123456789ABCDE. What is the Serial Number of the other USB Device?**

Use the EZviewer to view the output file , open the file

C:/Users/THM-4n6/Desktop/Output/Registry/20251019050016/20251019050016\_DeviceClasses\_C\_Windows\_System32\_config\_SYSTEM.csv

#####	ROOT\Cor	{53f5630d}	Multiple	STORAGE	Volume	{e251921f-4da2-11ec-a783-001a7dda7110}	
#####	ROOT\Cor	{53f5630d}	Multiple	STORAGE	Volume	{f529a9d6-4d9e-11ec-a782-001a7dda7110}	
#####	ROOT\Cor	{6ac27878}	Multiple	SWD	WPDBUSENUM	{e251921f-4da2-11ec-a783-001a7dda7110}	
#####	ROOT\Cor	{6ac27878}	Multiple	SWD	WPDBUSENUM	{f529a9d6-4d9e-11ec-a782-001a7dda7110}	
#####	ROOT\Cor	{a5dcbf10}	Multiple	USB	VID_0930&PID_6545	1C6F654E59A3B0C179D366AE	
#####	ROOT\Cor	{a5dcbf10}	Multiple	USB	VID_0E0F&PID_0003	6&30c5d09c&0&5	
#####	ROOT\Cor	{a5dcbf10}	Multiple	USB	VID_0E0F&PID_0008		650268328
#####	ROOT\Cor	{a5dcbf10}	Multiple	USB	VID_2537&PID_1068	0123456789ABCDE	

1C6F654E59A3B0C179D366AE

**7zip, Google Chrome and Mozilla Firefox were installed from a Network drive location on the Virtual Machine. What was the drive letter and path of the directory from where these software were installed?**

Check the file

C:/Users/THM-4n6/Desktop/Output/FileFolderAccess/20251019095902\_AutomaticDestinations.csv

35	C:\Users\THM-4n6\Desktop\Tarj	#####	#####	f01b4d95c	Windows	4	36	22	D	#####	#####	樟品6	02:0b:fc:71c:\Program Files\Amazon\Ec2ConfigServi	1
36	C:\Users\THM-4n6\Desktop\Tarj	#####	#####	f01b4d95c	Windows	4	36	23	A	#####	#####	新盛源,并	00:1a:7d:cE\KAPE	1
37	C:\Users\THM-4n6\Desktop\Tarj	#####	#####	f01b4d95c	Windows	4	36	24		7	#####		Z:\setups	1
38	C:\Users\THM-4n6\Desktop\Tarj	#####	#####	f01b4d95c	Windows	4	36	25		6	#####	新盛源,并	00:1a:7d:c\knownfolder\{1898981D-9985-4558-841C-	3

Z:\Setups

**What is the execution date and time of CHROMESETUP.EXE in MM/DD/YYYY HH:MM?**

Use the file

C:/Users/THM-4n6/Desktop/Output/Registry/20251019050016/20251019050016\_RecentApps\_C\_Users\_THM-4n6\_NTUSER.DAT.csv

Microsoft.Windows.Explorer	Multiple	::{52205FC	11/24/2021 15:24
OperaSoftware.OperaWebBrowser.1637811529	Multiple	C:\Users\	11/25/2021 4:10
Z:\setups\OperaSetup.exe	Multiple		11/25/2021 3:33
Z:\setups\ChromeSetup.exe	Multiple		11/25/2021 3:33
{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\NOTEPAD.EXE	Multiple	C:\Windo	11/25/2021 3:42

11/25/2021 03:33

What search query was run on the system?

Open the file  
C:/Users/THM-4n6/Desktop/Output/Registry/20251019050016/20251019050016\_WordWheelQuery\_\_C\_Users\_THM-4n6\_NTUSER.DAT.csv in EZviewer

	A	B	C	D	
1	SearchTerm	BatchKeyPath	MruPosition	BatchValueName	KeyName
2	setup	ROOT\SOFTWARE\Microsoft\Win		0	2 WordWheelQuery
3	ush	ROOT\SOFTWARE\Microsoft\Win		1	1 WordWheelQuery
4	RunWallpaperSetup.cmd	ROOT\SOFTWARE\Microsoft\Win		2	0 WordWheelQuery
5					

RunWallpaperSetup.cmd

When was the network named Network 3 First connected to?

Use the file  
C:/Users/THM-4n6/Desktop/Output/Registry/20251019050016/20251019050016\_KnownNetworks\_\_C\_Windows\_System32\_config\_SOFTWARE.csv

FirstNetwork	BatchKeyPath	NetworkName	BatchValueName	Type	FirstConnectLOCAL	LastConnectedLOCAL
Network	ROOT\Microsoft	Network	Multiple	Wired	11/24/2021 19:12	11/24/2021 19:12
Network 2	ROOT\Microsoft	Network	Multiple	Wired	11/24/2021 19:18	11/24/2021 23:33
Network 2	ROOT\Microsoft	Network	Multiple	Wired	11/25/2021 22:13	11/25/2021 22:13
Network 3	ROOT\Microsoft	Network	Multiple	Wired	11/30/2021 15:44	10/19/2025 8:29

11/30/2021 15:44

KAPE was copied from a removable drive. Can you find out what was the drive letter of the drive where KAPE was copied from?

Check the file  
C:/Users/THM-4n6/Desktop/Output/FileFolderAccess/20251019095902\_AutomaticDestinations.csv

\\tsclient\D\Get-Zimmerman\	1	FALSE
c:\fc:7\C:\Program Files\Amazon\Ec2	1	FALSE
a:7d\c:E:\KAPE	1	FALSE
Z:\setups	1	FALSE
3:7d\knownfolder\19999B1D-9995	3	FALSE

E