# 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

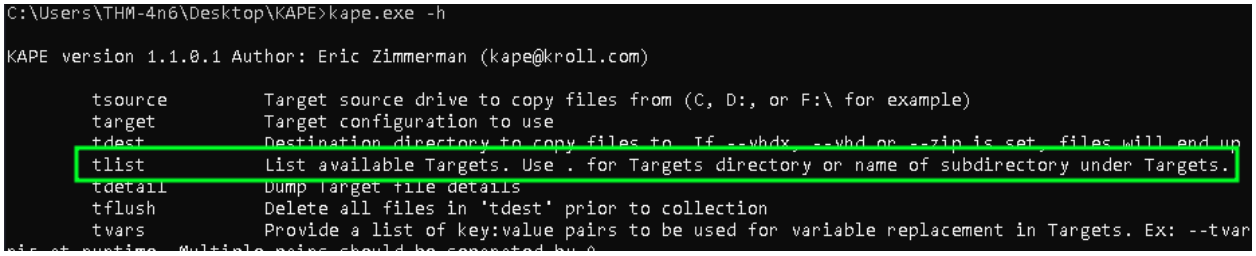
**What option has to be checked to append date and time information to triage folder name?**

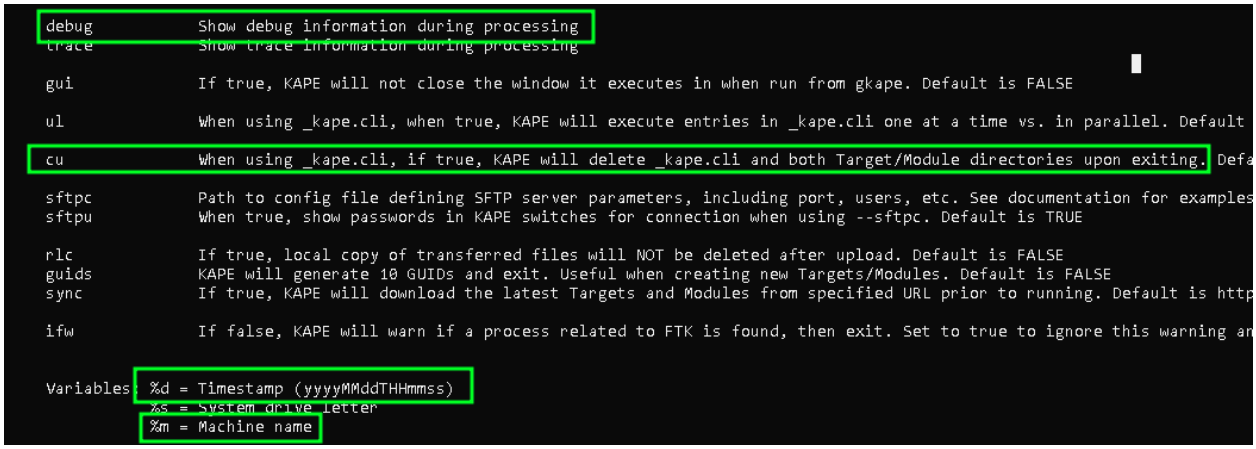
%d

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

%m

# Task 6 KAPE CLI




**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 | {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\Tar | ######## | ######## | ######## | f01b4d95c | Windows | 4 | 36 | 22 | D | ######## | ######## | 桴嗝6 | 02:0b:fc:7f | C:\Program Files\Amazon\Ec2ConfigServi | 1 |
| 36 | C:\Users\THM-4n6\Desktop\Tar | ######## | ######## | ######## | f01b4d95c | Windows | 4 | 36 | 23 | A | ######## | ######## | 敷歲瀨ㄏ | 00:1a:7d:c | E:\KAPE | 1 |
| 37 | C:\Users\THM-4n6\Desktop\Tar | ######## | ######## | ######## | f01b4d95c | Windows | 4 | 36 | 24 | 7 | | ######## | | | Z:\setups | 1 |
| 38 | C:\Users\THM-4n6\Desktop\Tar | ######## | ######## | ######## | f01b4d95c | Windows | 4 | 36 | 25 | 6 | ######## | ######## | 敷歲瀨ㄏ | 00:1a:7d:c | knownfolder:{18989B1D-99B5-455B-841C- | 3 |

Z:\Setups

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

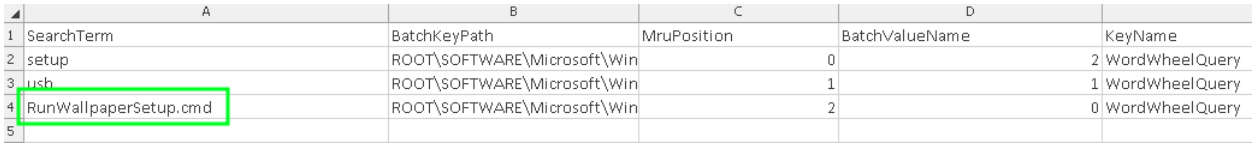
Use the file C:/Users/THM-4n6/Desktop/Output/Registry/20251019050016/20251019050016_RecentApps__C_Users_THM-4n6_NTUSER.DAT.csv

| | | | | |
|---|---|---|---|---|
| \ | Microsoft.Windows.Explorer | Multiple | ::{52205FD | 11/24/2021 15:24 |
| \ | OperaSoftware.OperaWebBrowser.1637811529 | Multiple | C:\Users\T | 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

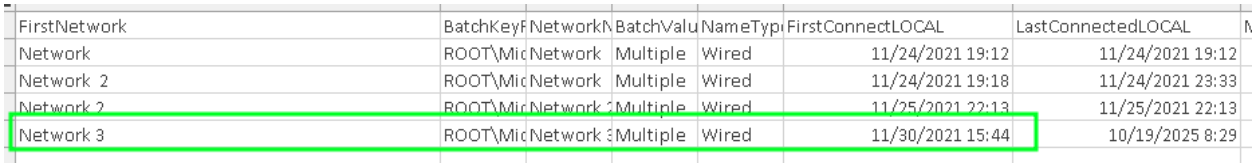


| | A | B | C | D | |
|---|---|---|---|---|---|
| 1 | SearchTerm | BatchKeyPath | MruPosition | BatchValueName | KeyName |
| 2 | setup | ROOT\SOFTWARE\Microsoft\Win | 0 | 2 | WordWheelQuery |
| 3 | ush | ROOT\SOFTWARE\Microsoft\Win | 1 | 1 | WordWheelQuery |
| 4 | RunWallpaperSetup.cmd | ROOT\SOFTWARE\Microsoft\Win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

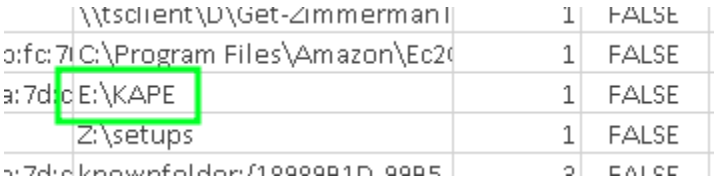


| FirstNetwork | BatchKeyF | NetworkN | BatchValu | NameTyp | FirstConnectLOCAL | LastConnectedLOCAL | N |
|---|---|---|---|---|---|---|---|
| Network | ROOT\Mic | Network | Multiple | Wired | 11/24/2021 19:12 | 11/24/2021 19:12 | |
| Network 2 | ROOT\Mic | Network | Multiple | Wired | 11/24/2021 19:18 | 11/24/2021 23:33 | |
| Network 2 | ROOT\Mic | Network 2 | Multiple | Wired | 11/25/2021 22:13 | 11/25/2021 22:13 | |
| Network 3 | ROOT\Mic | Network 3 | 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 |
| o:fc:7 | C:\Program Files\Amazon\Ec2 | 1 | FALSE |
| a:7d:c | E:\KAPE | 1 | FALSE |
| | Z:\setups | 1 | FALSE |
| a:7d:c | knownfolder:{18989B1D-99B5 | 2 | FALSE |

E