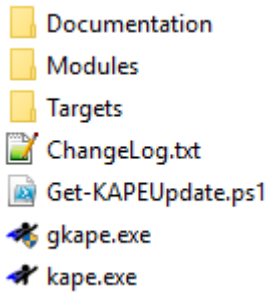
1 Introduction

Kroll Artifact Parser and Extractor (KAPE) is a triage tool that can be used to gather information from a machine under investigation. KAPE runs on Windows 64-bit systems and should be run with administrative privileges. To tamper evidence as little as possible, it is strongly recommended to run the script from a USB stick or a network share that can be mounted on the target machine. The output folder of KAPE can be specified, and it is recommended that this be on the same USB or share from which KAPE is run. The size of this output can be several Gigabytes; hence it is important to choose a partition with enough free space.

2 Preparation (on separate machine)

1. Obtain customized version of KAPE from IRIS. The download link is the following: https://ibm.box.com/s/jo7bux95vabab0xhsrhxcmmajajjvu29
2. Depending whether target machine has a physical USB port or not, either:
   a. Unzip file on USB stick.
   b. Unzip file on network share that can be mounted on target machine.
   c. The extracted folder should appear as follows:



3 Information capture (on **Windows** 64-bit target machine)

1. Mount the network share where KAPE was unzipped or connect USB stick to target machine.
2. Open windows command prompt **with administrator privileges** and navigate to the folder where “kape.exe” was extracted to.
3. In the following command. If necessary, replace the paths for “tsource”, “msource”, “tdest” and “mdest” as appropriate.
   a. “tsource” and “msource” should be the drive letter where the Windows Operating System resides (“C:” by default)
   b. “tdest” should be the path where you would like the output to be placed. Appending “\%m-%d” to the end will add hostname and timestamp. It is recommended that this folder be either a USB or network share.
   c. “mdest” is another output path for specific forensic tools run by KAPE.

```
.\kape.exe --tsource C: --tdest <full path to directory containing output files>\%m-%d --tflush --target !IRIS-FullTriage --vss --vhdx %m --msource C:\ --mdest <full path to directory containing output files>\modules\%m-%d --zm true --module !IRIS-Autoruns64-OK, !IRIS-Densityscout64-OK, !IRIS-Sigcheck64-OK
```

4. Run the command
5. A series of messages will appear, this is to be expected, and the extraction is complete when the message “Total execution time” appears in red text.

6. The data gathered by KAPE will be found in a folder that follows the format “<hostname>-YYYYMMDDThhmmss”. This folder will be found in the directory specified by the command. This data is NOT encrypted. It is recommended that this folder be added to an encrypted archive prior to sending to IBM X-Force IRIS.

Delivering files to IBM X-Force IRIS

1. It is recommended to compress and encrypt the data folder prior to delivery. The compressed, encrypted archive can then be delivered to the IRIS team via an agreed method of delivery.
2. Share complex password used to for encryption with IBM IRIS team using a different communication channel than used to share the triage output.
3. Use a method approved within your organization to securely erase the KAPE output folder.