**Picking up where the KAPE crew-aid left off, the Kape Triage collections will collect most of the files needed for a DFIR Investigation. This module pulls evidence from File System files, Registry Hives, Event Logs, Scheduled Tasks, Evidence of Execution, SRUM data, SUM data, Web Browser data (IE/Edge, Chrome, Mozilla history), LNK Files, Jump Lists, 3rd party remote access software logs, 3rd party antivirus software logs, Windows 10 Timeline database, and $I Recycle Bin data files. The KAPE product will produce an Export Format of “csv” files. Example CSV Name will resemble “20231201052349\_EvtxECmd\_Output.csv”. This particular output is for Event Logs.**

**The Goal is to prove via multiple evidence points that something either did or did not happen. Listed below are the most common locations a Hunter will be interested in but not an exhaustive list.**

**User Behavior**

* UserAssist: Applications opened
* RecentDocs: Files and folders opened
* Shellbags: Locations browsed by the user
* Open / Save MRU: Files that were opened
* Last-Visited MRU: Applications used to open files
* LNK Files Shortcut Files, Recent Items
* Jump Lists AutomaticDestinations Used to allow users to quickly access items. Data stored

here will have a unique file prepended with the AppID of the associatied application and embedded with LNK files in each stream.

* Prefetch Last time an application was executed on a system.
* Office Recent Files MS Office programs will track Recent used MS Files

**System Profiling Information/ Execution**

Using FTK Imager to create a disk image, and obtain the following if not already known, or if you have the NTUSER.DAT of the user in question, you can use the “Registry Explorer” Zimmerman tool.

* **Computername:**

Registry: HKLM\System\CurrentControlSet\Control\Computername\

* **Windows Version:**   
  Registry: HKLM\Software\Microsoft\Windows NT\Currentversion\
* **Timezone:**  
  Registry: HKLM\System\CurrentControlSet\Control\TimeZoneInformation\
* **Network Information:**   
  Registry: HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{interface-name}

**Network History:**

Registry:HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

Registry: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed

Registry: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache

* **Shutdown time:**   
  Registry: HKLM\System\ControlSet001\Control\Windows\ShutdownTime
* **Defender settings:**  
  Registry: HKLM\Software\Microsoft\Windows Defender\
* **USB Usage:**

Registry: HKLM\SYSTEM\CurrentContorlSet\Enum\USB

Registry: HKLM\SYSTEM\CurrentContorlSet\Enum\USBSTOR

* **Drive Letter & Volume Name:**

Registry: HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices

Registry: HKLM\SYSTEM\MountedDevices

* **Windows Explorer Address/Search Bars:**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

NTUSER.DAT \Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

* **OpenSaveMRU**: this key tracks files that have been opened or saved within a Windows shell dialog box.

Registry:NTUSER.DAT \Software\Microsoft\Windows\CurrentVersion\Explorer\ComDIg32\OpenSaveMRU

NTUSER.DAT \Software\Microsoft\Windows\CurrentVersion\Explorer\ComDIg32\OpenSacePIDIMRU

* **Background Activity Moderator (BAM)**

Registry*: HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}*

* **Background Activity Moderator (BAM)**Registry*: HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings*
* **Application Compatibility Cache ("AppCompatCache") / Shimcache**  
  Registry: *SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache*
* **AmCache**  
  Registry: *C:\Windows\AppCompat\Programs\Amcache.hve*
* **Prefetch**  
  Path: *C:\Windows\Prefetch\\*.pf*
* **Shortcut (LNK) Files**Path:*C:\users\<username>\AppData\Roaming\Microsoft\Windows\Recent*Path*: C:\users\<username>\AppData\Roaming\Microsoft\Office\Recent*
* **Persistence Mechanisms/Auto-Run Keys**Registry*:   
  HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run  
  HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce  
  HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run  
  HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce*
* **Startup Folder**Paths:  
  *C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup  
  C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp*
* What is the name of the suspicious script in the StartUp folder?
* **Windows Services**

Registry: *HKLM\SYSTEM\CurrentControlSet\Services*

* **Scheduled Tasks**

Registry:

*HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks  
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree*  
Path:  
*C:\Windows\System32\Tasks*