



# WINDOW FORENSICS

Prepared By :

**Muhammad Zohaib**  
**Soc Analyst L1**

## REGISTRY HIVES

Registry hive	Supporting files
<b>HKEY_CURRENT_CONFIG</b>	System, System.alt, System.log, System.sav
<b>HKEY_CURRENT_USER</b>	Ntuser.dat, Ntuser.dat.log
<b>HKEY_LOCAL_MACHINE \ SAM</b>	Sam, Sam.log, Sam.sav
<b>HKEY_LOCAL_MACHINE \ Security</b>	Security, Security.log, Security.sav
<b>HKEY_LOCAL_MACHINE \ Software</b>	Software, Software.log, Software.sav
<b>HKEY_LOCAL_MACHINE \ System</b>	System, System.alt, System.log, System.sav
<b>HKEY_USERS \ .DEFAULT</b>	Default, Default.log, Default.sav

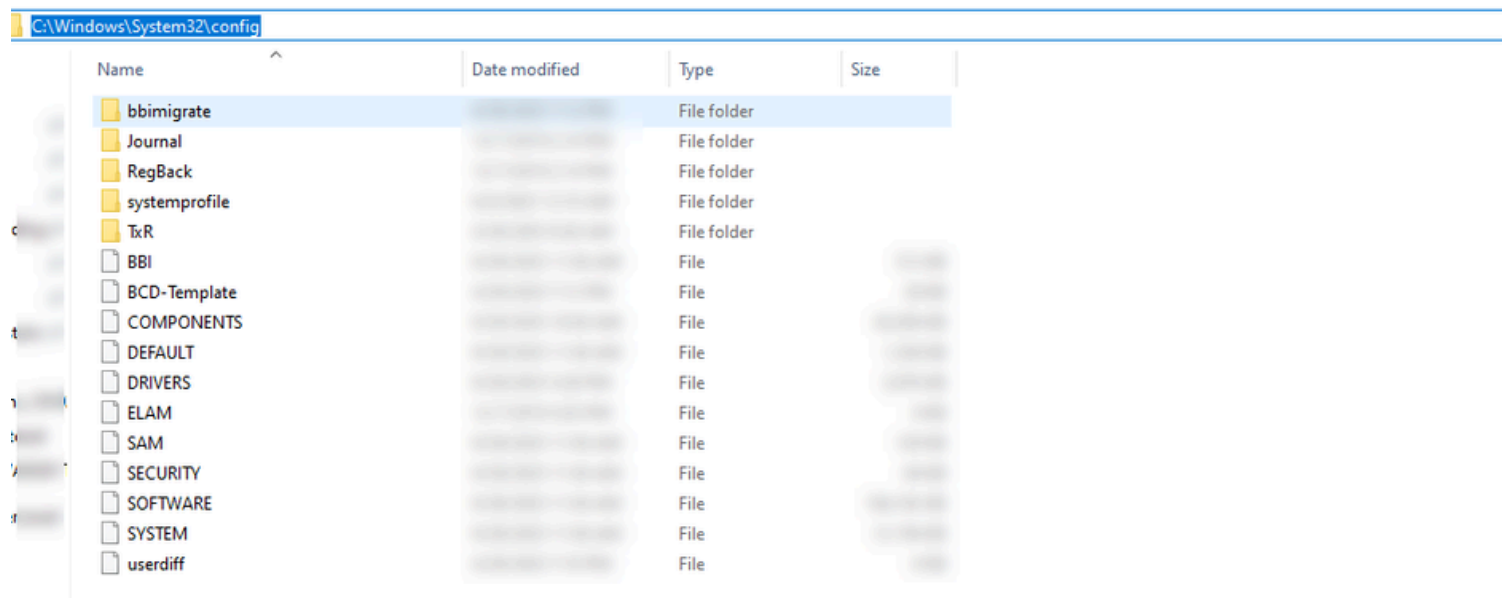
Extension	Description
<b>none</b>	A complete copy of the hive data.
<b>.alt</b>	A backup copy of the critical HKEY_LOCAL_MACHINE \ System hive. Only the System key has an .alt file.
<b>.log</b>	A transaction log of changes to the keys and value entries in the hive.
<b>.sav</b>	A backup copy of a hive. Windows Server 2003 and Windows XP/2000: Copies of the hive files as they looked at the end of the text-mode stage in Setup. Setup has two stages: text mode and graphics mode. The hive is copied to a .sav file after the text-mode stage of setup to protect it from errors that might occur if the graphics-mode stage of setup fails. If setup fails during the graphics-mode stage, only the graphics-mode stage is repeated when the computer is restarted; the .sav file is used to restore the hive data.

Folder/predefined key	Description
<b>HKEY_CURRENT_USER</b>	Contains the root of the configuration information for the user who is currently logged on. The user's folders, screen colors, and Control Panel settings are stored here. This information is associated with the user's profile. This key is sometimes abbreviated as HKCU.
<b>HKEY_USERS</b>	Contains all the actively loaded user profiles on the computer. HKEY_CURRENT_USER is a subkey of HKEY_USERS. HKEY_USERS is sometimes abbreviated as HKU.
<b>HKEY_LOCAL_MACHINE</b>	Contains configuration information particular to the computer (for any user). This key is sometimes abbreviated as HKLM.
<b>HKEY_CLASSES_ROOT</b>	<p>HKCR (HKEY_CLASSES_ROOT) controls which program opens which file type.</p> <p>It merges info from:</p> <p><b>HKLM \ Software \ Classes</b> → default (all users).</p> <p><b>HKCU \ Software \ Classes</b> → user-specific (overrides default).</p> <p><b>To change for one user</b> → edit HKCU.</p> <p><b>To change for all users</b> → edit HKLM.</p> <p><b>Writing to HKCR</b> → system decides whether it goes to HKCU or HKLM.</p>
<b>HKEY_CURRENT_CONFIG</b>	Contains information about the hardware profile that is used by the local computer at system startup.

## ACCESSING REGISTRY HIVES OFFLINE

If you are accessing a **live** system, you will be able to access the registry using regedit.exe, and you will be greeted with all of the standard root keys we learned about in the previous task. However, if you only have **access** to a **disk image**, you must know where the **registry hives** are **located** on the disk. The majority of these hives are located in the **C:\Windows\System32\Config** directory and are:

- **DEFAULT** (mounted on HKEY\_USERS \ DEFAULT)
- **SAM** (mounted on HKEY\_LOCAL\_MACHINE \ SAM)
- **SECURITY** (mounted on HKEY\_LOCAL\_MACHINE \ Security)
- **SOFTWARE** (mounted on HKEY\_LOCAL\_MACHINE \ Software)
- **SYSTEM** (mounted on HKEY\_LOCAL\_MACHINE \ System)



Name	Date modified	Type	Size
bbimigrate		File folder	
Journal		File folder	
RegBack		File folder	
systemprofile		File folder	
TxR		File folder	
BBI		File	
BCD-Template		File	
COMPONENTS		File	
DEFAULT		File	
DRIVERS		File	
ELAM		File	
SAM		File	
SECURITY		File	
SOFTWARE		File	
SYSTEM		File	
userdiff		File	

**NTUSER.DAT** (mounted on HKEY\_CURRENT\_USER when a user logs in)

**USRCLASS.DAT** (mounted on HKEY\_CURRENT\_USER \ Software \ CLASSES)

---

## DATA ACQUISITION TOOL

---

### KAPE:

KAPE is a live data acquisition and analysis tool which can be used to acquire registry data. It is primarily a command-line tool but also comes with a GUI. The below screenshot shows what the KAPE GUI looks like. We have already selected all the settings to extract the registry data using KAPE in this screenshot. We will learn more about collecting forensic artifacts using KAPE in a dedicated KAPE room. ( FTK image and Autopsy Also )

---

## EXPLORING WINDOWS REGISTRY TOOL

---

### Registry Viewer:

As we can see in the screenshot below, AccessData's Registry Viewer has a similar user interface to the Windows Registry Editor. There are a couple of limitations, though. It only loads one hive at a time, and it can't take the transaction logs into account.

### Zimmerman's Registry Explorer:

Eric Zimmerman has developed a handful of tools that are very useful for performing Digital Forensics and Incident Response. One of them is the Registry Explorer. It looks like the below screenshot. It can load multiple hives simultaneously and add data from transaction logs into the hive to make a more 'cleaner' hive with more up-to-date data. It also has a handy 'Bookmarks' option containing forensically important registry keys often sought by forensics investigators. Investigators can go straight to the interesting registry keys and values with the bookmarks menu item.

### RegRipper:

RegRipper is a utility that takes a registry hive as input and outputs a report that extracts data from some of the forensically important keys and values in that hive. The output report is in a text file and shows all the results in sequential order.

---

## SYSTEM INFORMATION AND SYSTEM ACCOUNTS

---

Now that we have learned **how to read registry data**, let's find out where to look in the registry to **perform our forensic analysis**.

When we start performing **forensic analysis**, the **first step** is to find out about the system information. This **task** will cover gathering information related to a **machine's System** and Account information.

---

## OS VERSION:

If we only have triage data to perform forensics, we can determine the **OS version** from which this data was pulled through the registry. **To find the OS version**, we can use the following registry key:

- **SOFTWARE\Microsoft\Windows NT\CurrentVersion**
- 

## CURRENT CONTROL SET:

The hives containing the machine's configuration data used for controlling system startup are called Control Sets. Commonly, we will see **two Control Sets**, ControlSet001 and ControlSet002, in the SYSTEM hive on a machine. In most cases (but not always), ControlSet001 will point to the Control Set that the machine booted with, and ControlSet002 will be the **last known good configuration**. Their locations will be:

- **SYSTEM\ControlSet001**
- **SYSTEM\ControlSet002**
- **SYSTEM\Select\Current**

Similarly, the last known good configuration can be found using the following registry value:

- **SYSTEM\Select\LastKnownGood**
- 

## COMPUTER NAME:

It is crucial to establish the Computer Name while performing forensic analysis to ensure that we are working on the machine we are supposed to work on. We can find the Computer Name from the following location:

- **SYSTEM\CURRENTCONTROLSET\CONTROL\COMPUTERNAME\COMPUTERNAME**
- 

## TIME ZONE INFORMATION:

For accuracy, it is important to establish what time zone the computer is located in. This will help us understand the chronology of the events as they happened. For finding the Time Zone Information, we can look at the following location:

- **SYSTEM\CurrentControlSet\Control\TimeZoneInformation**
- 

## NETWORK INTERFACES AND PAST NETWORKS:

The following registry key will give a list of network interfaces on the machine we are investigating:

- **SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces**

The past networks a given machine was connected to can be found in the following locations:

- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged**
- **SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed**

---

### Autostart Programs (Autoruns):

The following registry keys include information about programs or commands that run when a user logs on.

- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run**
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\Run**

The following registry key contains information about services:

- **SYSTEM\CurrentControlSet\Services**
- 

### SAM hive and user information:

The SAM hive contains user account information, login information, and group information. This information is mainly located in the following location:

- **SAM\Domains\Account\Users**
- 

The information contained here includes the **relative identifier (RID)** of the **user**, **number of times** the **user logged in**, **last login time**, **last failed login**, **last password change**, **password expiry**, password policy and password hint, and any groups that the user is a part of.

---

---

## USAGE OR KNOWLEDGE OF FILES/FOLDERS

---

### Recent Files:

Windows maintains a list of recently opened files for each user. As we might have seen when using Windows Explorer, it shows us a list of recently used files. This information is stored in the NTUSER hive and can be found on the following location:

- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**



---

### Office Recent Files:

Similar to the Recent Docs maintained by Windows Explorer, Microsoft Office also maintains a list of recently opened documents. This list is also located in the NTUSER hive. It can be found in the following location:

- **NTUSER.DAT\Software\Microsoft\Office\VERSION**

The version number for each Microsoft Office release is different. An example registry key will look like this:

- **NTUSER.DAT\Software\Microsoft\Office\15.0\Word**

Starting from **Office 365**, Microsoft now ties the location to the user's live ID . In such a scenario, the recent files can be found at the following location.

- **NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID\_####\FileMRU**

In such a scenario, the recent files can be found at the following location. This location also saves the complete path of the most recently used files.

---

### ShellBags:

When any user opens a folder, it opens in a specific layout. Users can change this layout according to their preferences. These layouts can be different for different folders. This information about the **Windows 'shell'** is stored and can identify the Most Recently Used files and folders. Since this setting is different for each user, it is located in the user hives. We can find this **information on the following locations:**

- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags**
- **USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU**
- **NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU**
- **NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags**
- 

Registry Explorer **doesn't** give us much information about **ShellBags**. However, another tool from **Eric Zimmerman's tools** called the **ShellBag Explorer** shows us the information in an easy-to-use format.

---



---

### **Open/Save and LastVisited Dialog MRUs:**

When we open or save a file, a dialog box appears asking us where to save or open that file from. It might be noticed that once we open/save a file at a specific location, Windows remembers that location. This implies that we can find out recently used files if we get our hands on this information. We can do so by examining the following registry keys

- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU**
  - **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU**
- 

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

Another way to identify a user's recent activity is by looking at the paths typed in the Windows Explorer address bar or searches performed using the following registry keys, respectively.

- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths**
  - **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery**
- 

---

## **EVIDENCE OF EXECUTION**

---

### **UserAssist :**

Windows keeps track of applications launched by the user using Windows Explorer for statistical purposes in the User Assist registry keys. These keys contain information about the programs launched, the time of their launch, and the number of times they were executed. However, programs that were run using the command line can't be found in the User Assist keys. The User Assist key is present in the NTUSER hive, mapped to each user's GUID. We can find it at the following location:

- **NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count**
- 

---

### **ShimCache:**

is a mechanism used to keep track of application compatibility with the OS and tracks all applications launched on the machine. Its main purpose in Windows is to ensure backward compatibility of applications. It is also called Application Compatibility Cache (AppCompatCache). It is located in the following location in the SYSTEM hive:

- **SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache**

ShimCache stores file name, file size, and last modified time of the executables.

---

### **AmCache:**

The AmCache hive is an artifact related to ShimCache. This performs a similar function to ShimCache, and stores additional data related to program executions. This data includes execution path, installation, execution and deletion times, and SHA1 hashes of the executed programs. This hive is located in the file system at:

- **C:\Windows\appcompat\Programs\Amcache.hve**

Information about the last executed programs can be found at the following location in the hive:

- **Amcache.hve\Root\File\{Volume GUID}\**
- 

### **BAM/DAM:**

Background Activity Monitor or BAM keeps a tab on the activity of background applications. Similar Desktop Activity Moderator or DAM is a part of Microsoft Windows that optimizes the power consumption of the device. Both of these are a part of the Modern Standby system in Microsoft Windows.

In the Windows registry, the following locations contain information related to BAM and DAM. This location contains information about last run programs, their full paths, and last execution time

- **SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}**
  - **SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}**
- 

---

## EXTERNAL DEVICES/USB DEVICE FORENSICS

---

### Device identification:

The following locations keep track of USB keys plugged into a system. These locations store the vendor id, product id, and version of the USB device plugged in and can be used to identify unique devices. These locations also store the time the devices were plugged into the system.

- **SYSTEM\CurrentControlSet\Enum\USBSTOR**
  - **SYSTEM\CurrentControlSet\Enum\USB**
- 

### First/Last Times:

Similarly, the following registry key tracks the first time the device was connected, the last time it was connected and the last time the device was removed from the system.

- **SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven\_Prod\_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####**
- 

### USB device Volume Name:

The device name of the connected drive can be found at the following location:

- **SOFTWARE\Microsoft\Windows Portable Devices\Devices**
-