



Lecture 6- Registry Forensics

Dr. Zunera Jalil

Email: zunera.jalil@au.edu.pk

Registry Forensics

Windows Registry holds a database of values and keys that give useful pieces of information to forensic analysts.

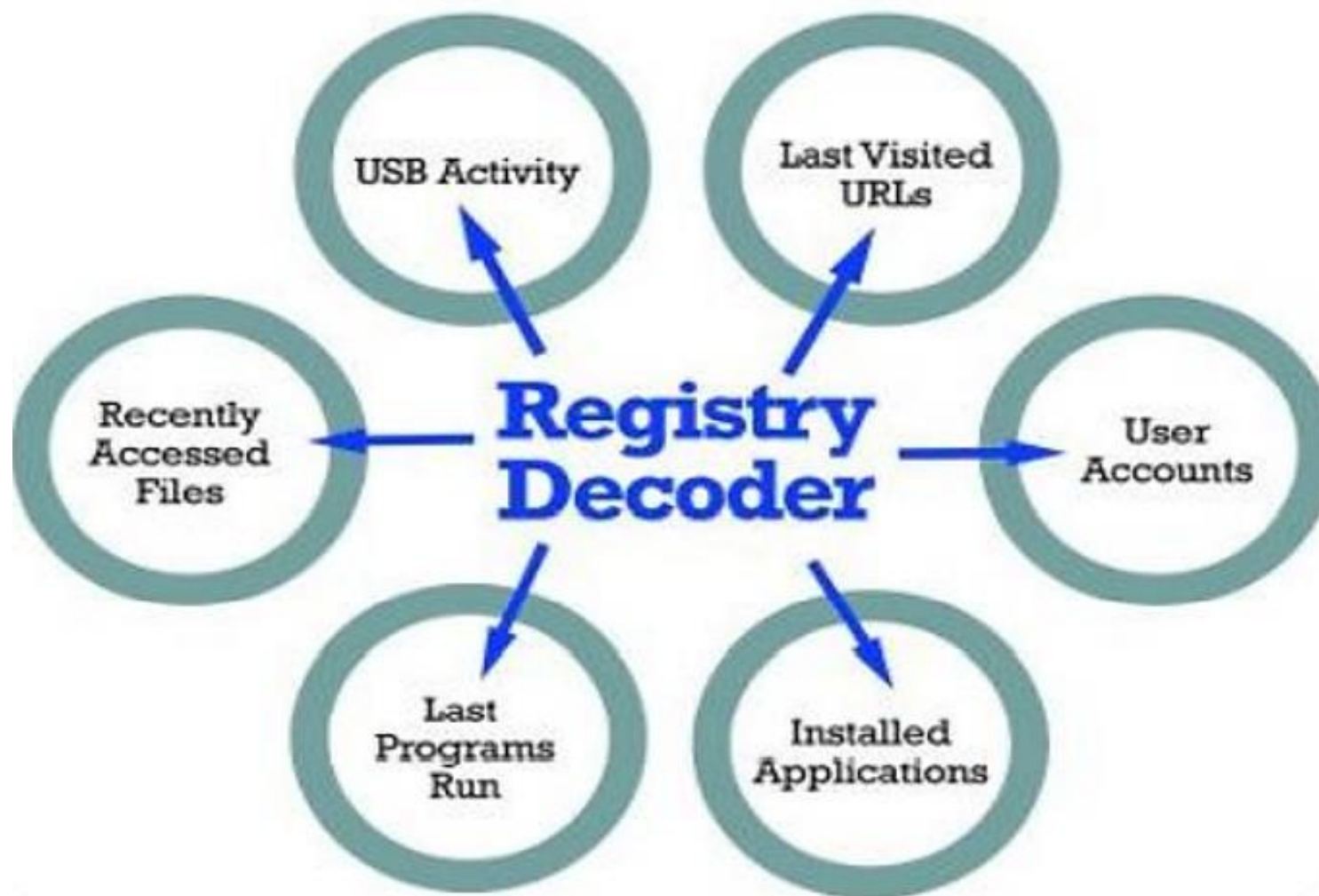
- Windows Registry keeps most of the information pertaining **policies, status** etc. in form of **keys, sub keys and values**.
- Windows registry can be worked upon by administrator through application like **'regedit'**.
- Windows can also be supplied with a command like tool like 'reg' to help users work on registry.
- Registry contains **hives** under which sub keys are present. These hives play important role in the overall functioning of the system.

Registry Forensics

- Registry keys and associated files that encompasses user activities on the system.

Registry Key	Abbr.	Associated files	Incorporates
HKEY_LOCAL_MACHINE	HKLM		System settings
HKEY_USERS	HKU	NTUSER.DAT	Settings related to all currently logged-in users
HKEY-CURRENT_USER	HKCU		Both system and application Settings with regard to all currently logged-in users
HKEY_CURRENT_CONFIG	HKCC		Registry will be created at runtime and contains hardware settings and performance details
HKLM\SYSTEM		System	File involves system settings about services and hardware
HKLM\SOFTWARE		Software	File incorporates configuration settings for all installed applications including windows
HKLM\SAM		Sam	Includes security info and user password hashes for all users on the system

**The Windows Registry contains a
wealth of forensically interesting data.**



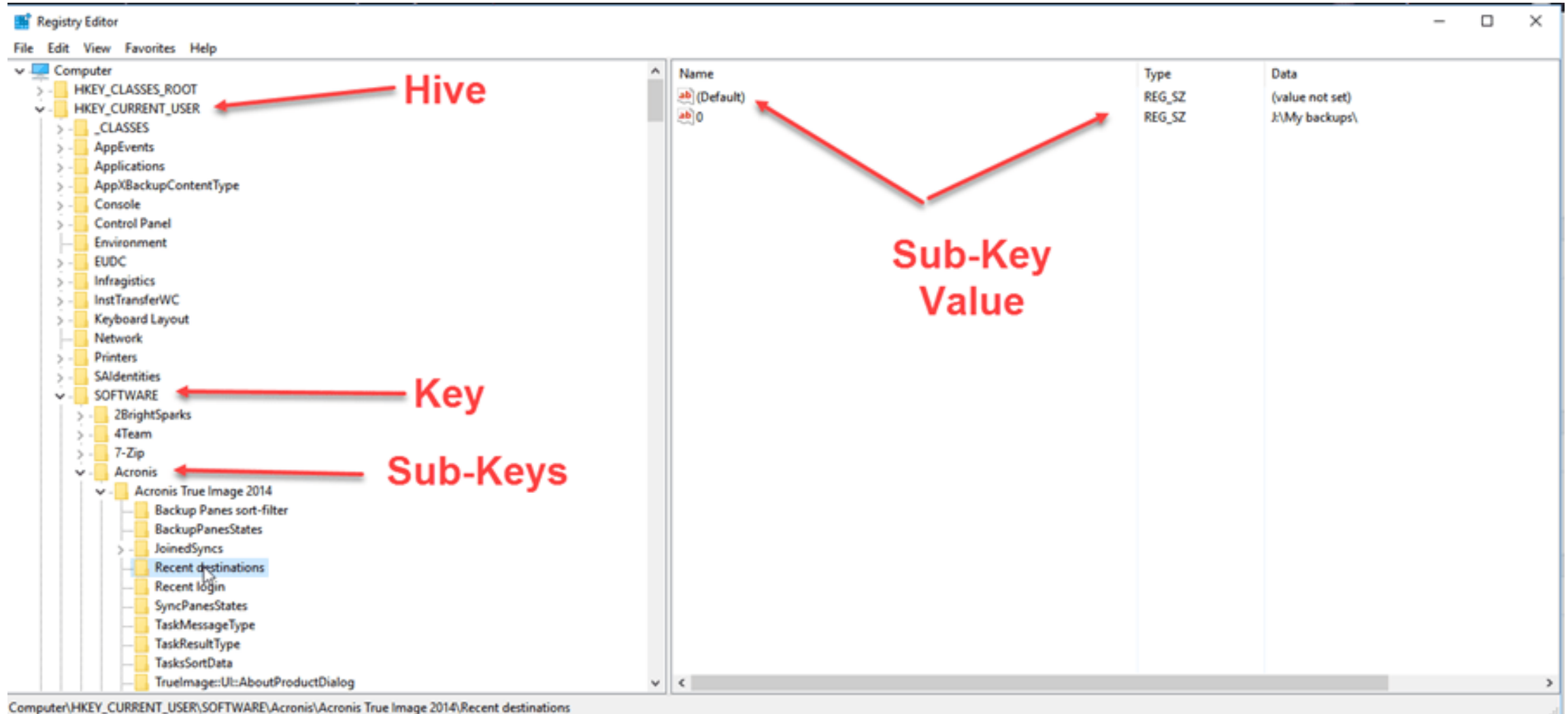
Registry Forensics

- Registry can reveal information such as time zone, shares, audit policy, wireless SSIDS, auto start locations, user login, activities, USB removable devices, trusted devices, cache, cookie and history etc.

KEY	Function
HKEY_CLASS_ROOT	A symbolic link to HKEY_LOCAL_MACHINE\SOFTWARE\Classes; provides file type and file extension information, URL protocol prefixes, and so forth
HKEY_CURRENT_USER	A symbolic link to HKEY_USERS; stores settings for the currently logged-on user
HKEY_LOCAL_MACHINE	Contains information about installed hardware and software
HKEY_USERS	Stores information for the currently logged-on user; only one key in this HKEY is linked to HKEY_CURRENT_USER
HKEY_CURRENT_CONFIG	A symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profile\xxx (with xxx representing the current hardware profile); contains hardware configuration settings

Registry Structure

6



Introduction

- Whenever you install a software program/application, a hardware or a device driver for a newly connected hardware in Windows
 - The initial configuration settings of these components are stored in registry
- A Windows component, hardware or a software, retrieves its registry entries or keys, on every startup
 - It also modifies the registry entries or keys corresponding to it, in its course of execution
 - Registry data are sorted as computer-specific data or user-specific data in order to support multiple users

Introduction

- The registry is a **hierarchical database** with critical information
- Windows registry is a **tree structure**
 - Each node in the tree is called a **key**
 - Each key can contain both **sub keys** and data entries called **values**
 - The **keys / key values** are used by **Applications**
- A key can have any number of values, and the values can be in any form

Registry Hives

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE/SAM
- HKEY_LOCAL_MACHINE/SOFTWARE
- HKEY_LOCAL_MACHINE/SECURITY
- HKEY_LOCAL_MACHINE/SYSTEM
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Registry Hives

10

- A hive is a logical group of keys, sub-keys, and values in the registry that has a set of supporting files containing backups of its data
- Most of the supporting files for the hives are in the `%SystemRoot%\System32\Config`
- Each time a new user logs on to a computer, a new hive is created
- This is called the **user profile hive**
- A **user's hive** contains specific registry information pertaining to the user's application settings, desktop, environment, network connections etc.
 - located under the HKEY_USERS key

Registry Hives

- The permanent parts of the registry are stored as a set of files called the **Hive Files**.
- Locations for these files in the hive list sub key in `HKLM\SYSTEM\CurrentControlSet\Control`.
- These files are saved in `systemroot\System32\Config` and updated with each login.

Registry Hives

12

- **This stores four of the five keys in HKEY_LOCAL_MACHINE and one key in HKEY_USERS:**
 - **SAM** Contains information stored in the key HKLM\SAM about the Security Accounts Manager (SAM) service.
 - **SECURITY** Contains the security information stored in the key HKLM\SECURITY.
 - **SOFTWARE** Contains information stored in the key HKLM\SOFTWARE about the computer's software configuration.
 - **SYSTEM** Contains information stored in the HKLM\SYSTEM about the computer's system configuration.
 - **DEFAULT** Contains the default system information that is stored in the key HKEY_USERS\DEFAULT.
- HKEY_LOCAL_MACHINE\HARDWARE is not stored as a file, because it is recreated each time the system starts.

HKEY_CLASSES_ROOT Hive

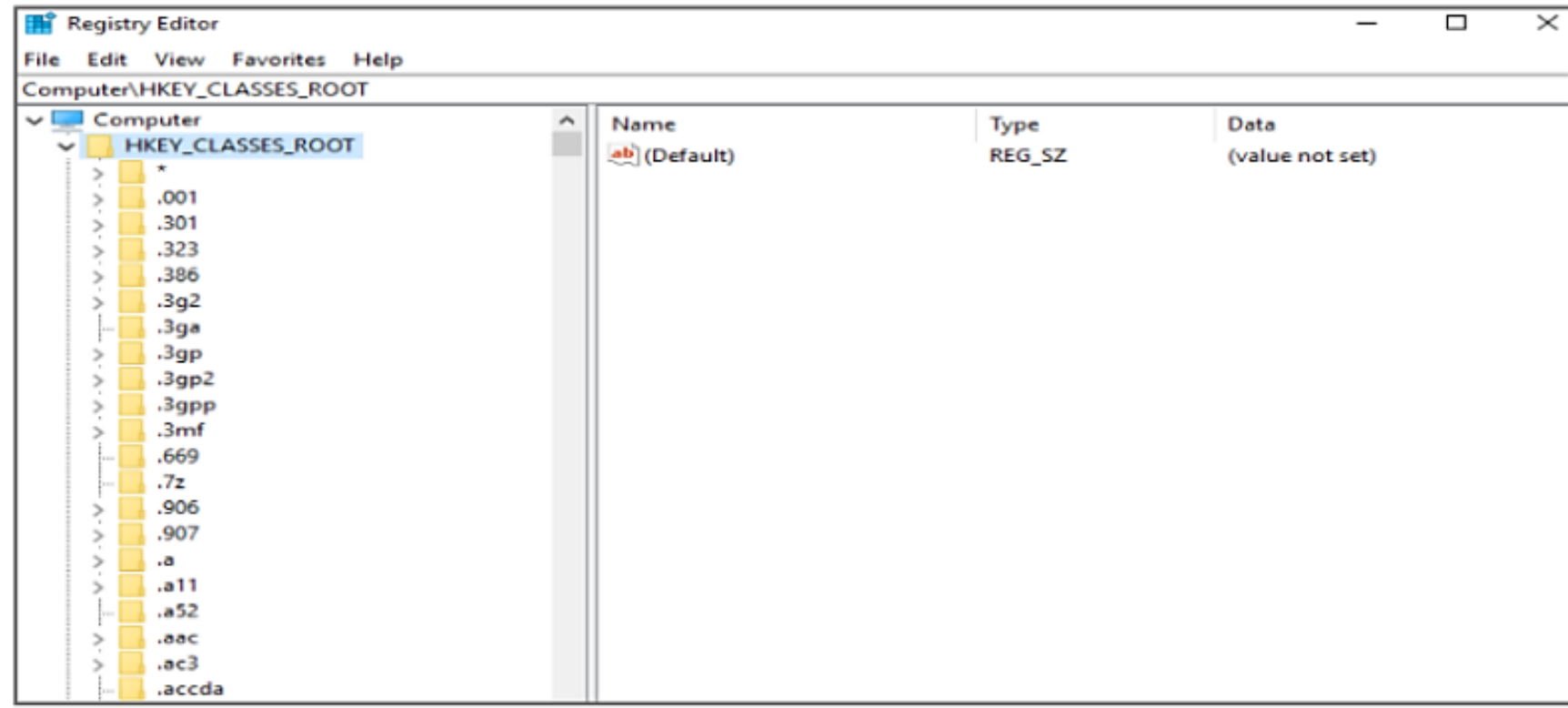
13

HKEY_CLASSES_ROOT

This is the largest of the keys in terms of the space occupied.

This is the merger of two keys with respect to per-user settings.

HKLM\Software\Classes and HKCU\software\Classes are merged together to create HKEY_CLASSES_ROOT.



HKEY_CURRENT_USER Hive

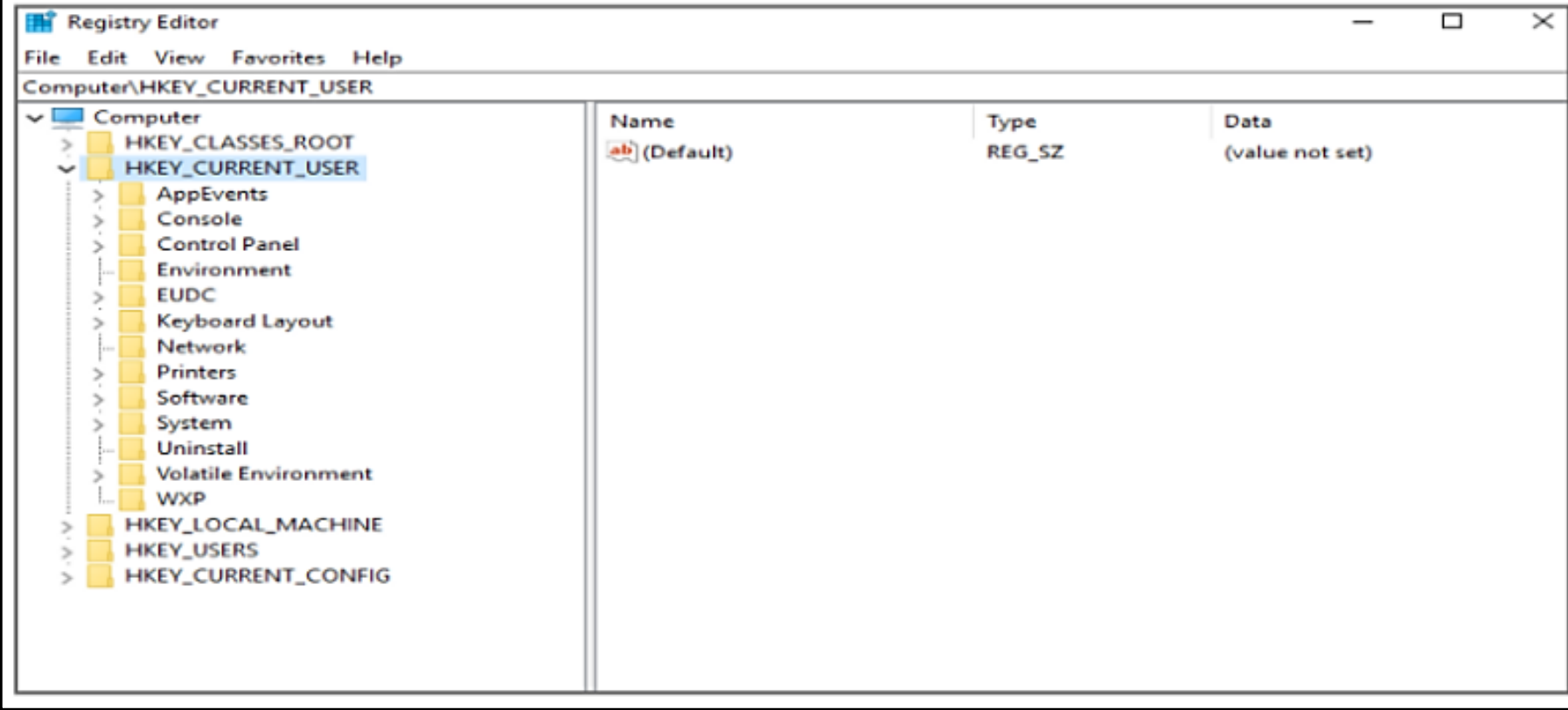
14

HKEY_CURRENT_USER

HKCU keys are current user settings that are specific to the currently logged on user.

It is derived from a link to HKCU\SID where SID is the Security Identifier of the user.

Each user gets its own user key to store unique settings.



HKEY_CURRENT_CONFIG Hive

15

HKEY_CURRENT_CONFIG	It is used to organize the current hardware config profile which is derived from link to HKLM\System\CurrentControlSet\HardwareProfiles\Current.
---------------------	---

Registry Editor

File Edit View Favorites Help

Computer\HKEY_CURRENT_CONFIG

Computer

HKEY_CLASSES_ROOT

HKEY_CURRENT_USER

HKEY_LOCAL_MACHINE

HKEY_USERS

HKEY_CURRENT_CONFIG

Software

Fonts

System

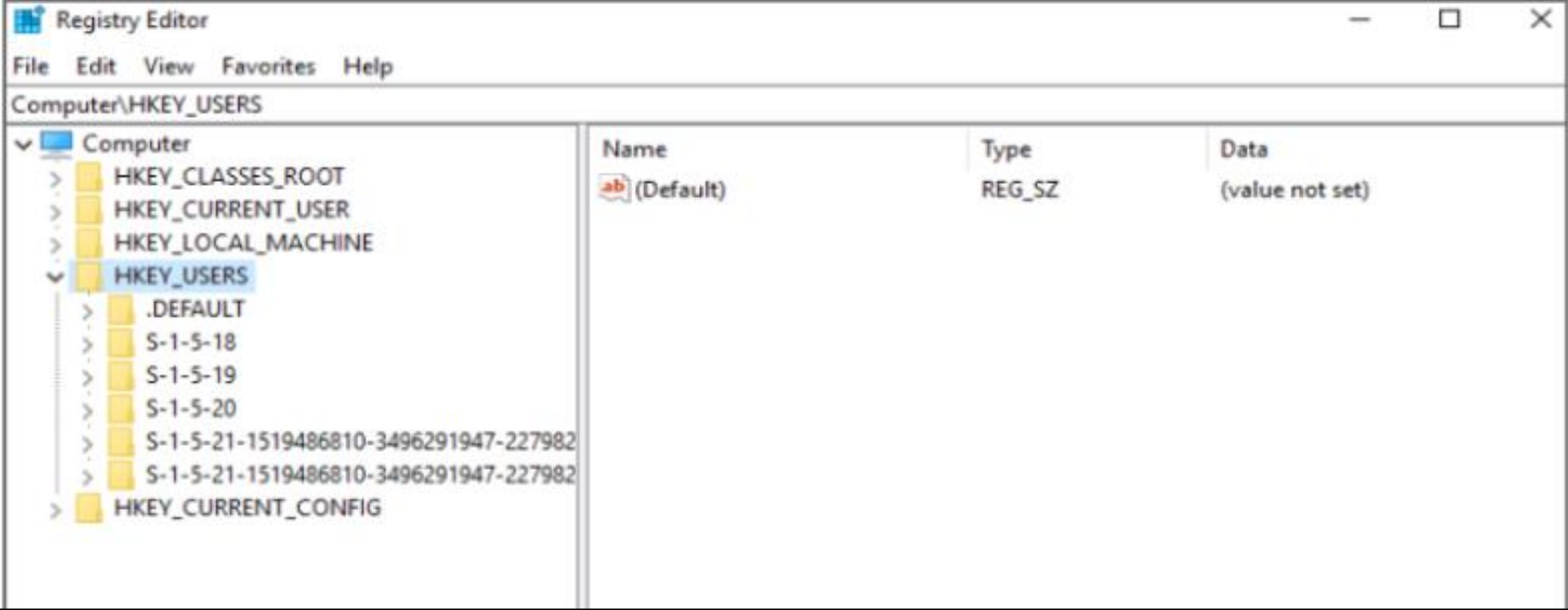
CurrentControlSet

Name	Type	Data
(Default)	REG_SZ	(value not set)

HKEY_USERS Hive

16

HKEY_USERS	HKU contains the settings that are applied to all the users. All the HKCU keys are maintained under this key.
-------------------	---



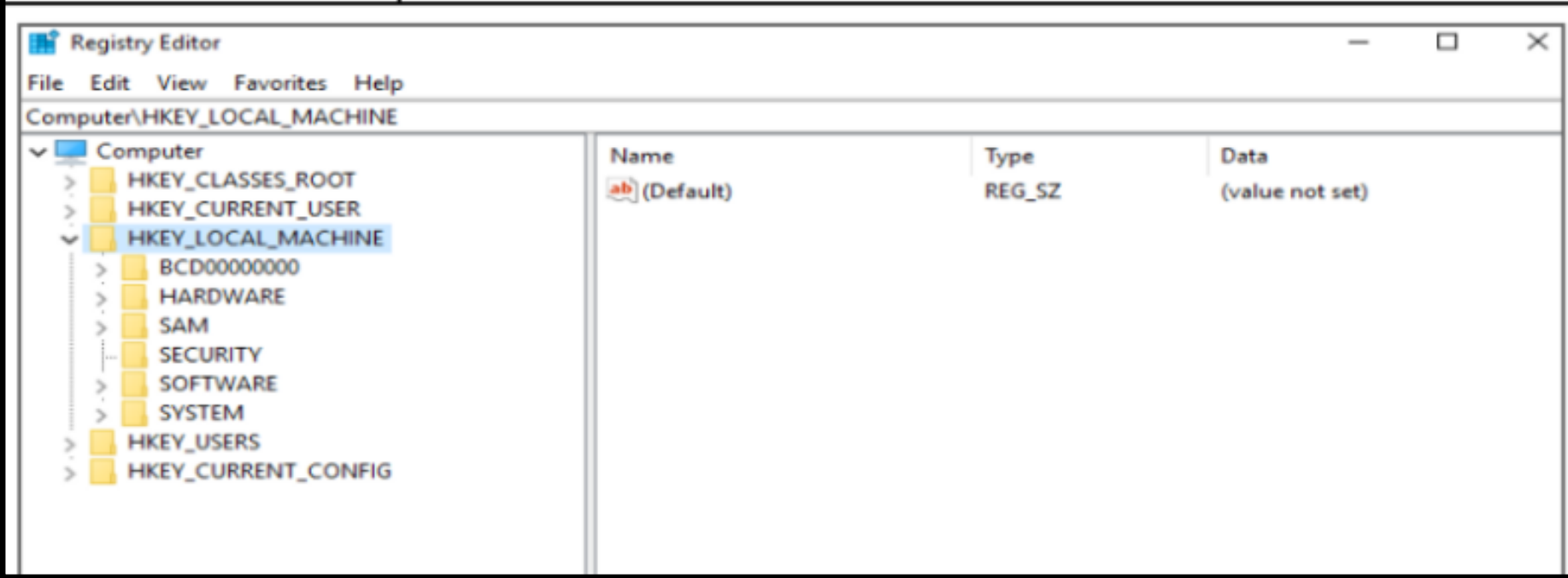
The screenshot shows the Windows Registry Editor window titled "Registry Editor". The address bar displays "Computer\HKEY_USERS". The left pane shows a tree view of the registry hives, with "HKEY_USERS" expanded. Under "HKEY_USERS", the following keys are listed: ".DEFAULT", "S-1-5-18", "S-1-5-19", "S-1-5-20", "S-1-5-21-1519486810-3496291947-227982", "S-1-5-21-1519486810-3496291947-227982", and "HKEY_CURRENT_CONFIG". The right pane shows a table with three columns: "Name", "Type", and "Data". The table contains one entry: "ab (Default)" with type "REG_SZ" and data "(value not set)".

Name	Type	Data
ab (Default)	REG_SZ	(value not set)

HKEY_LOCAL_MACHINE Hive

17

HKEY_LOCAL_MACHINE	HKLM is used to organize the current the computer settings. These settings are applied to the machine and all of the users that it contains.
---------------------------	--

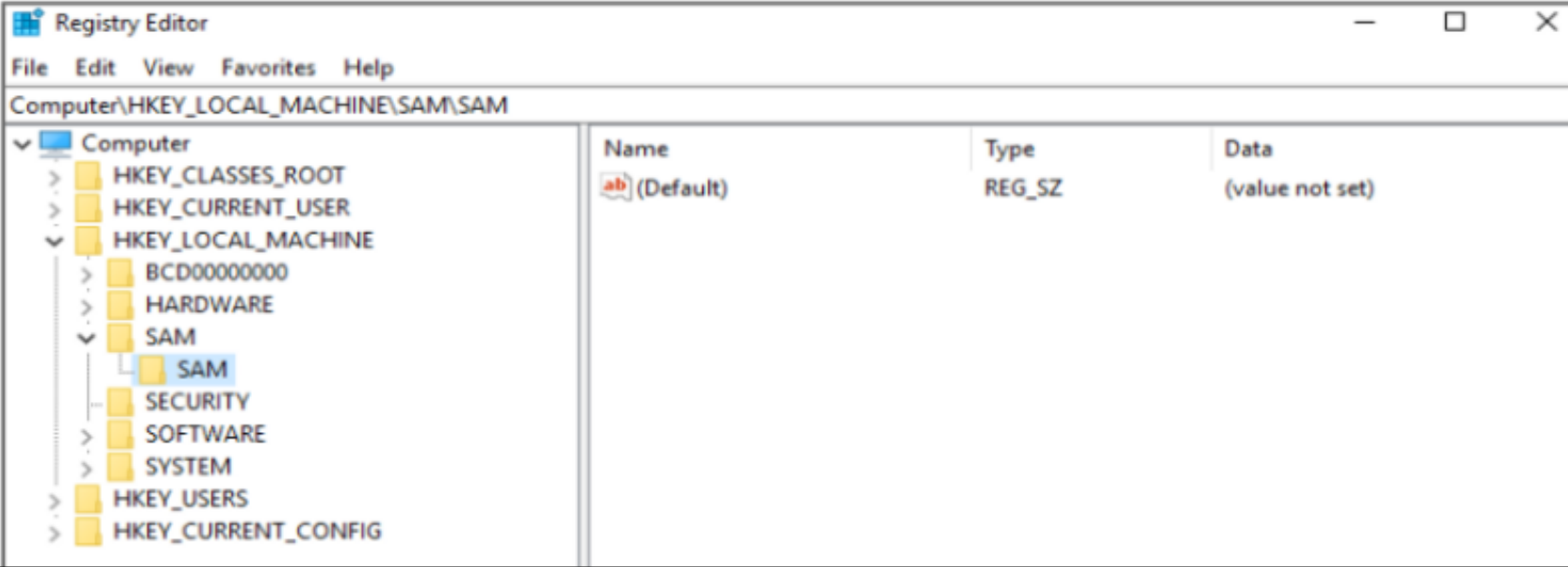


The screenshot shows the Windows Registry Editor window. The title bar reads 'Registry Editor'. The menu bar includes 'File', 'Edit', 'View', 'Favorites', and 'Help'. The address bar shows 'Computer\HKEY_LOCAL_MACHINE'. The left pane displays a tree view of the registry hives: 'Computer' (expanded), 'HKEY_CLASSES_ROOT', 'HKEY_CURRENT_USER', 'HKEY_LOCAL_MACHINE' (selected), 'BCD00000000', 'HARDWARE', 'SAM', 'SECURITY', 'SOFTWARE', 'SYSTEM', 'HKEY_USERS', and 'HKEY_CURRENT_CONFIG'. The right pane shows a table of registry values for the selected hive.

Name	Type	Data
(Default)	REG_SZ	(value not set)

1. HKEY_LOCAL_MACHINE /SAM Hive

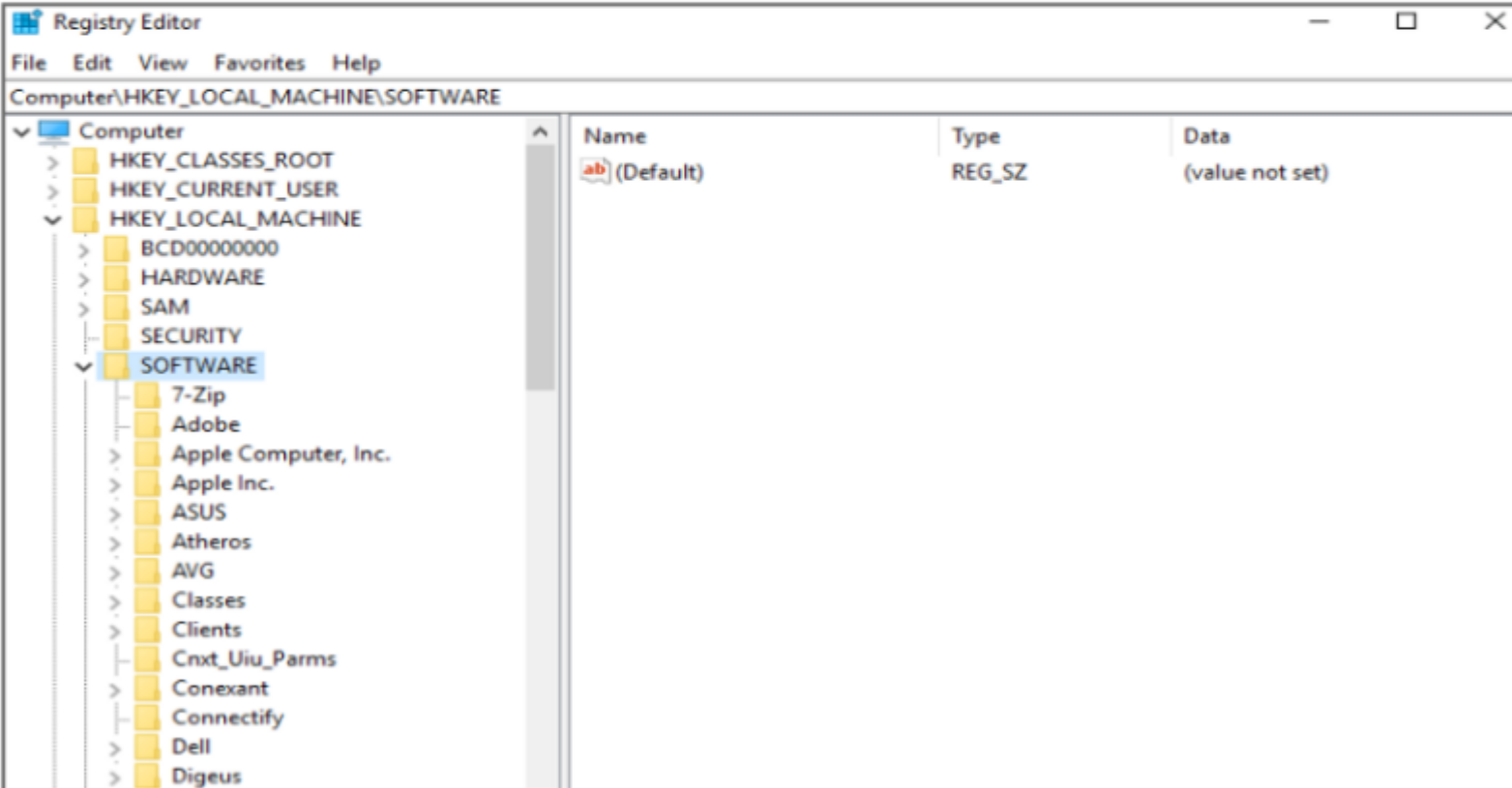
18

HKEY_LOCAL_MACHINE/ SAM	<p>SAM stands for System Account Manager. This key is used to store and organize all the system passwords. This is a system protected file. SAM key is most important for an attacker to exploit the system.</p>
	

2. HKEY_LOCAL_MACHINE/SOFTWARE Hive

19

HKEY_LOCAL_MACHINE/	Most programs that are installed in the system create keys in HKLM\Software section in the
SOFTWARE	windows registry. This key contains all the configuration settings, Executables, Path, and Uninstallation information.



Registry Editor

File Edit View Favorites Help

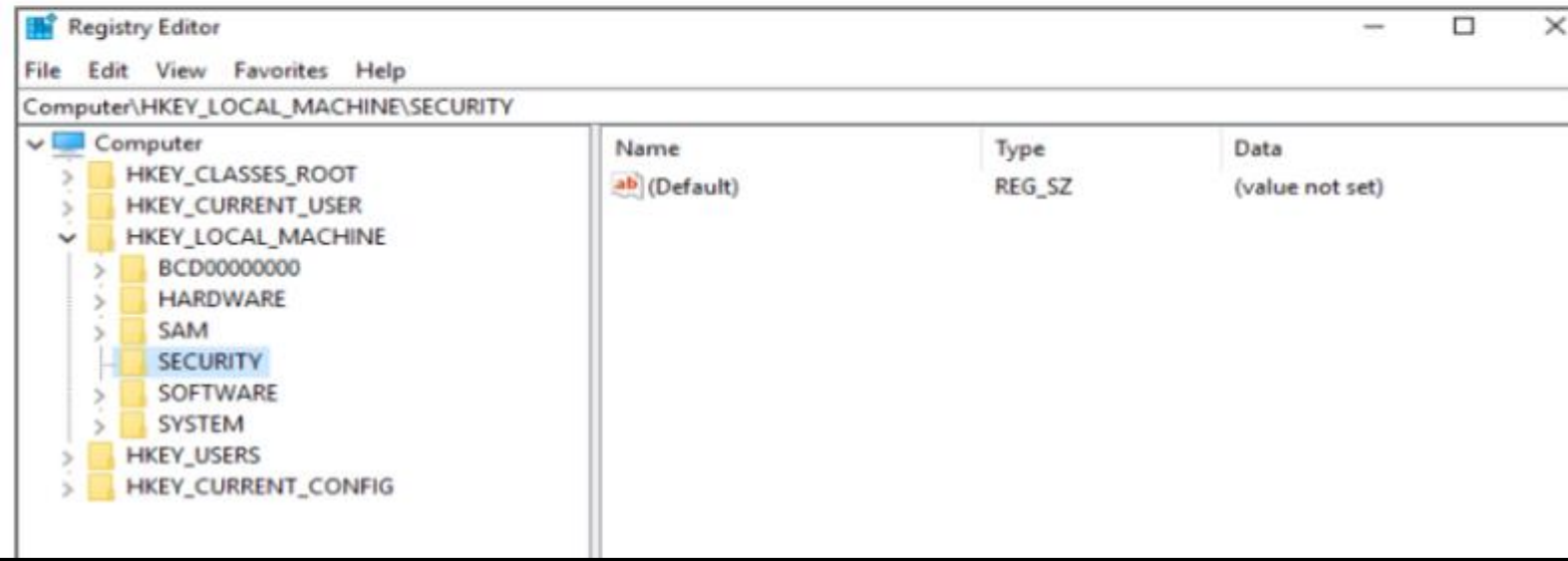
Computer\HKEY_LOCAL_MACHINE\SOFTWARE

Name	Type	Data
(Default)	REG_SZ	(value not set)

3. HKEY_LOCAL_MACHINE/SECURITY Hive

20

HKEY_LOCAL_MACHINE/ SECURITY	<p>HKLM security contains the security database of the domain into which the current user is logged on. This key is linked to the local machine and the kernel reads it to enforce the security policy applicable to the current user and all applications or operations executed by the user.</p> <p>Security key usually looks empty unless the administrative access is given.</p>
-------------------------------------	---



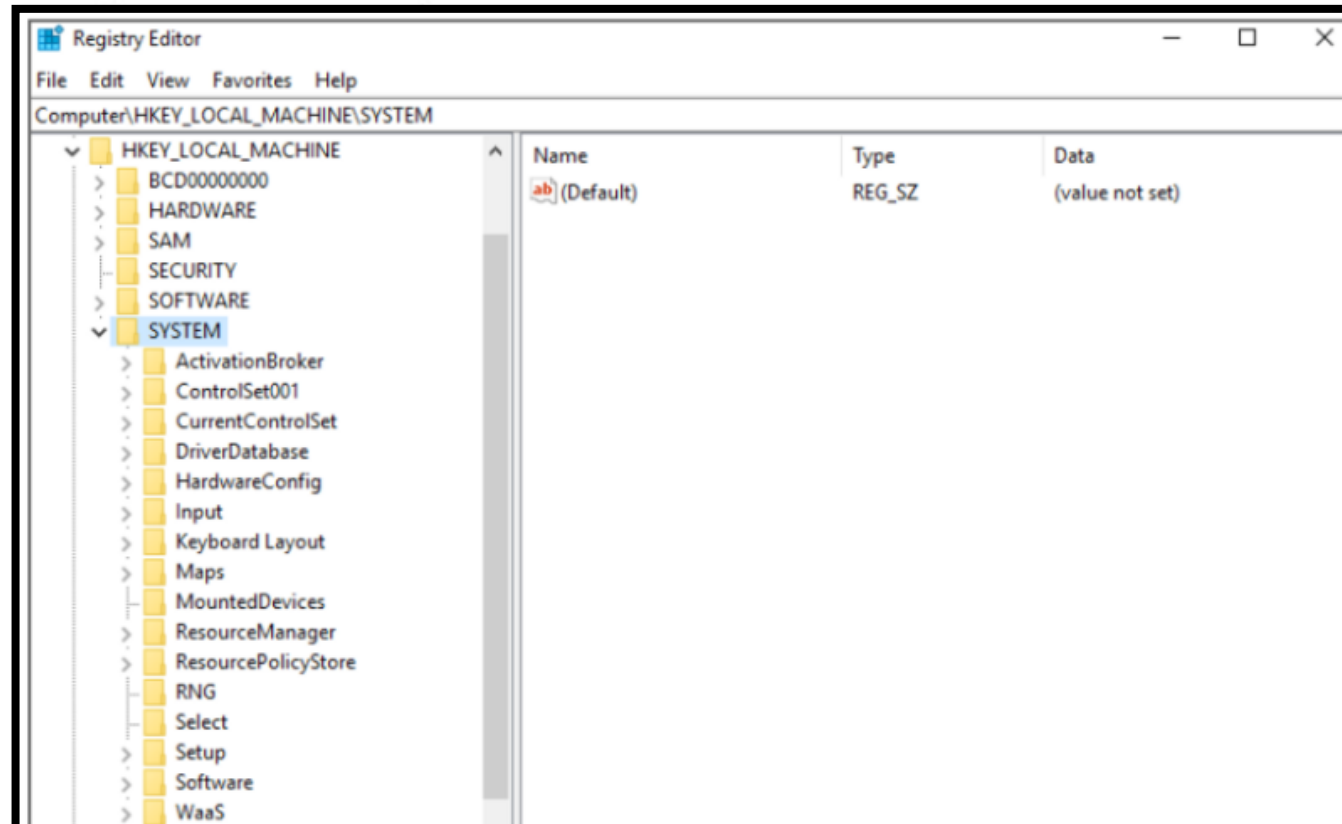
4. HKEY_LOCAL_MACHINE/SYSTEM Hive

21

HKEY_LOCAL_MACHINE/

SYSTEM

HKLM System is one of the most important registries which is located in the config folder of windows system32 directory. This key contains all the system configurations of all the users. It can only be modified if the administrative access is provided. Information such as System Default settings, External Drives, Kernel settings, and all applications that execute or perform any operation which uses HKLM Security key.



Hive and their associated files

- HKEY_CURRENT_CONFIG – System, System.alt, System.log, System.sav
- HKEY_CURRENT_USER – Ntuser.dat, Ntuser.dat.log
- HKEY_LOCAL_MACHINE\SAM – Sam, Sam.log, Sam.sav
- HKEY_LOCAL_MACHINE\Security – Security, Security.log, Security.sav
- HKEY_LOCAL_MACHINE\Software – Software, Software.log, Software.sav
- HKEY_LOCAL_MACHINE\System – System, System.alt, System.log, System.sav
- HKEY_USER\DEFAULT – Default, Default.log, Default.sav

In Windows NT and later, there are six files:

Ntuser.dat, System.dat, SAM.dat, Software.dat, Security.dat, and Default.dat.

When examining registry data from a suspect drive after you have made an acquisition and are reviewing it in a forensics tool, you need to know the location of these files.

Hive and their associated files

23

Filename and location	Purpose of file
Users\user-account\Ntuser.dat	User-protected storage area; contains the list of most recently used files and desktop configuration settings
Windows\system32\config\Default.dat	Contains the computer's system settings
Windows\system32\config\SAM.dat	Contains user account management and security settings
Windows\system32\config\Security.dat	Contains the computer's security settings
Windows\system32\config\Software.dat	Contains installed programs' settings and associated usernames and passwords
Windows\system32\config\System.dat	Contains additional computer system settings
Windows\system32\config\systemprofile	Contains additional NTUSER information

Volatile Hives

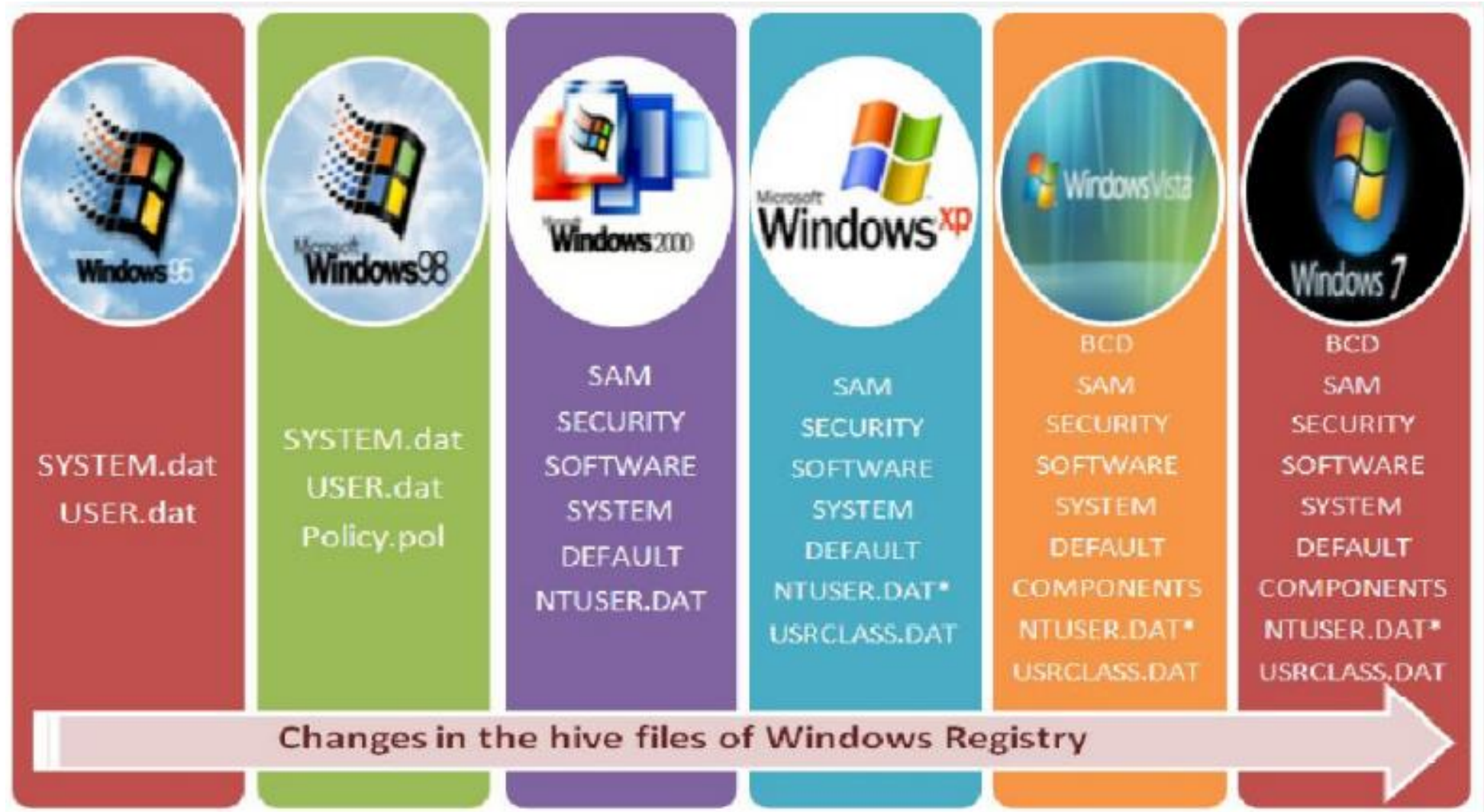
Some of these hives are volatile –

created when the system starts or user logs in

- HKEY_LOCAL_MACHINE\System\CurrentControlSet
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE\Hardware

Changes in Hive Files

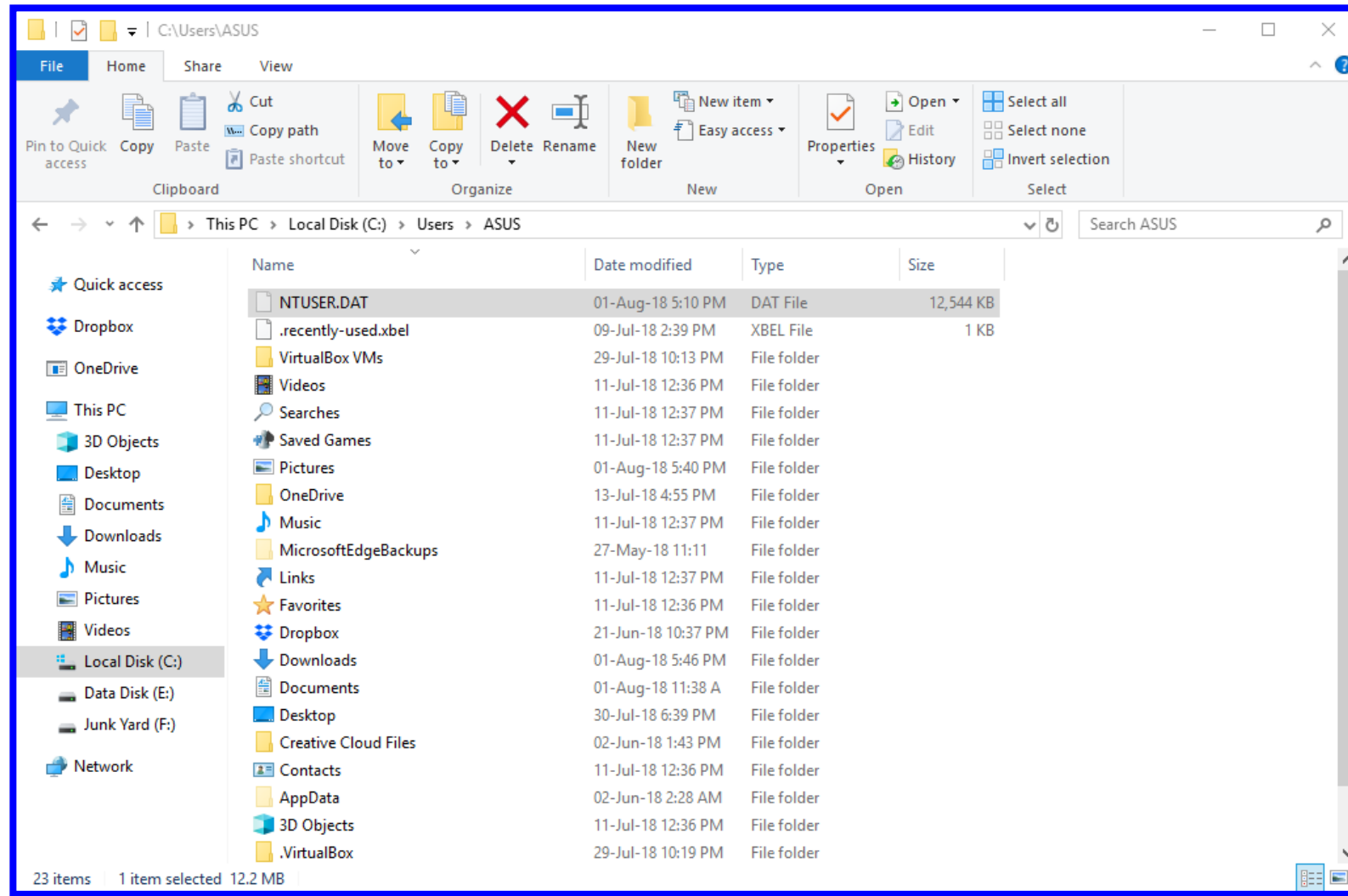
25



Path for Registry Files

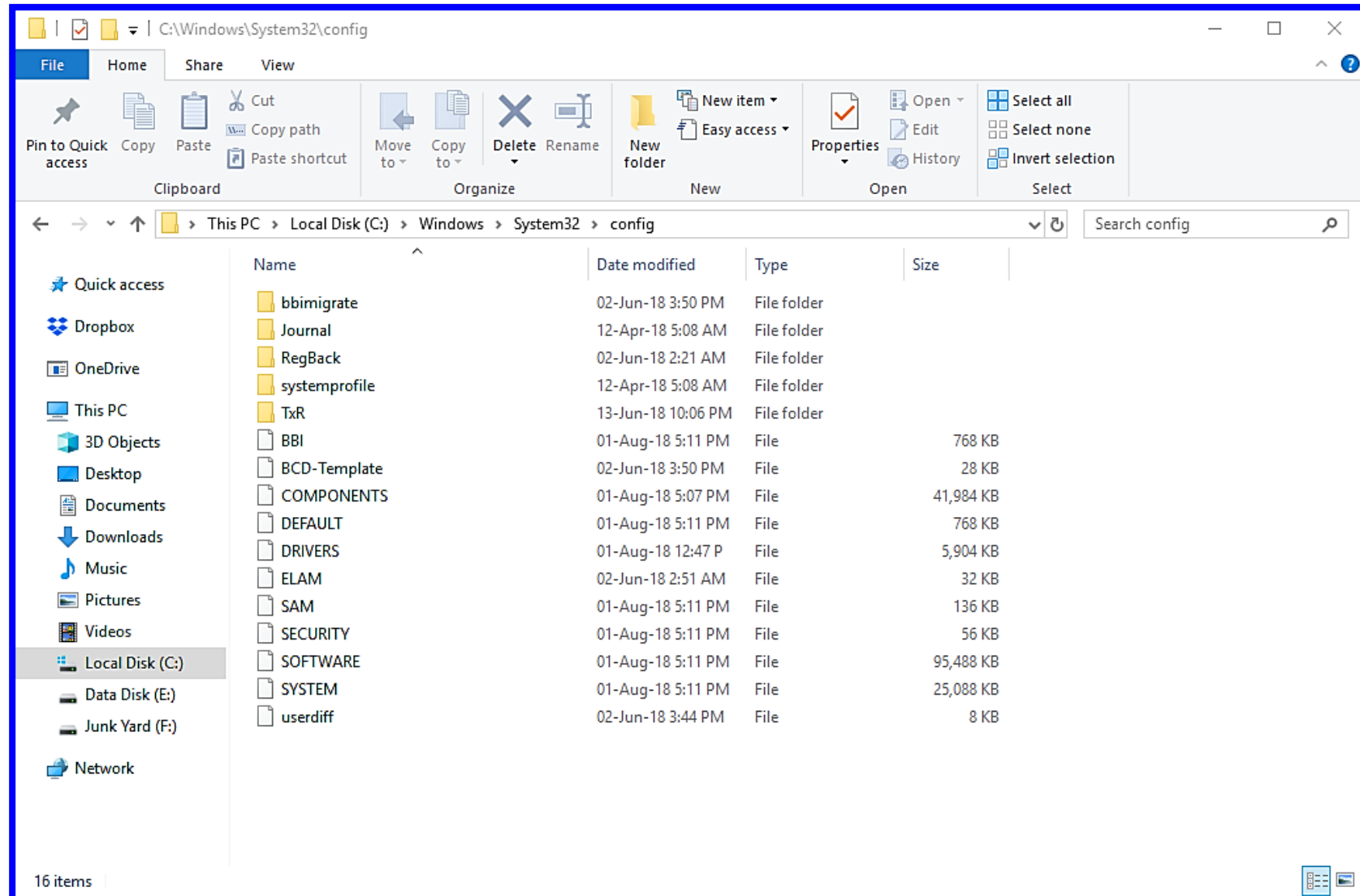
26

Path for HKEY_CURRENT_USER file NTUSER.DAT



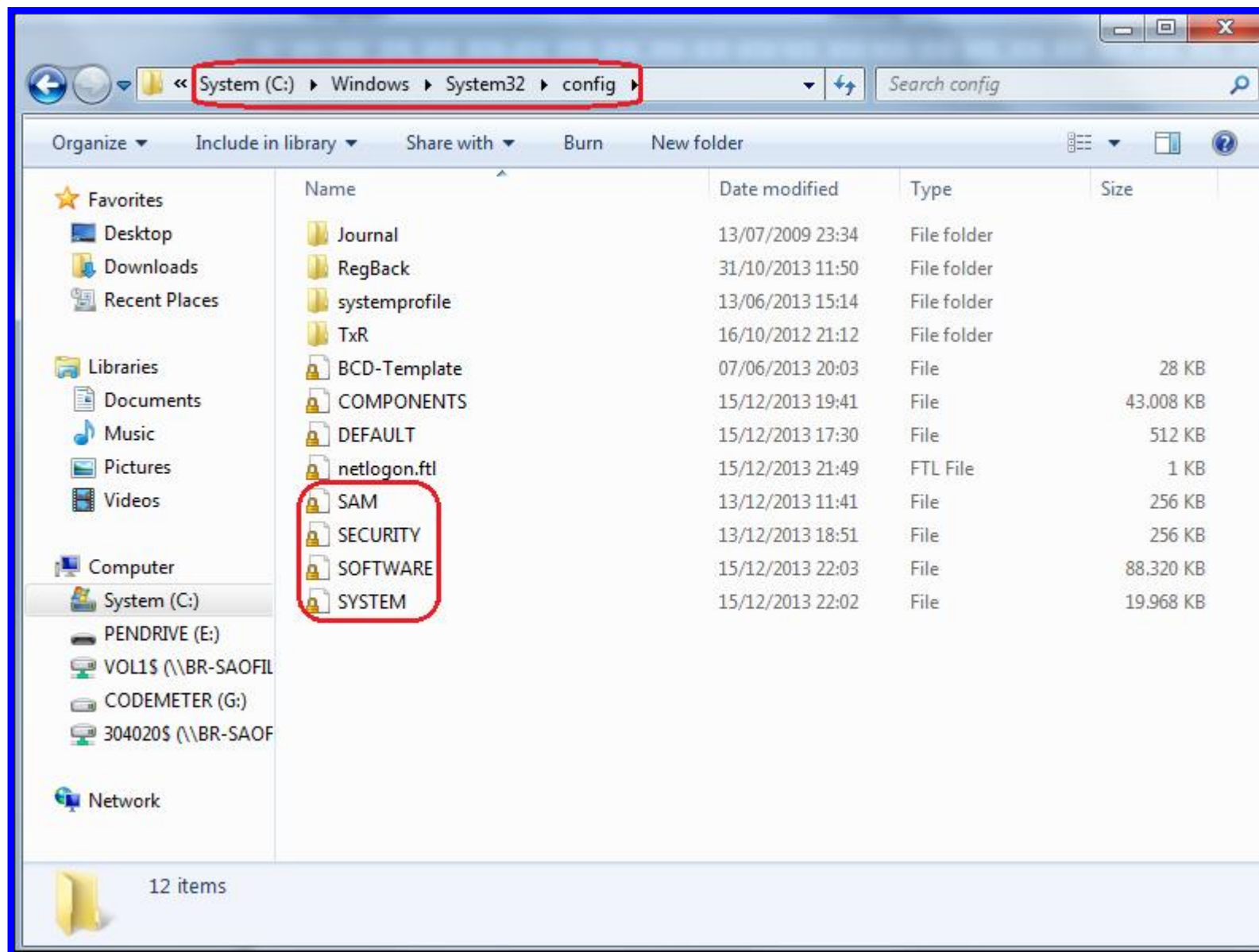
Path for Registry Files

Path for HKEY_LOCAL_MACHINE files SAM, SYSTEM, SOFTWARE, SECURITY



Path for Registry Files

28



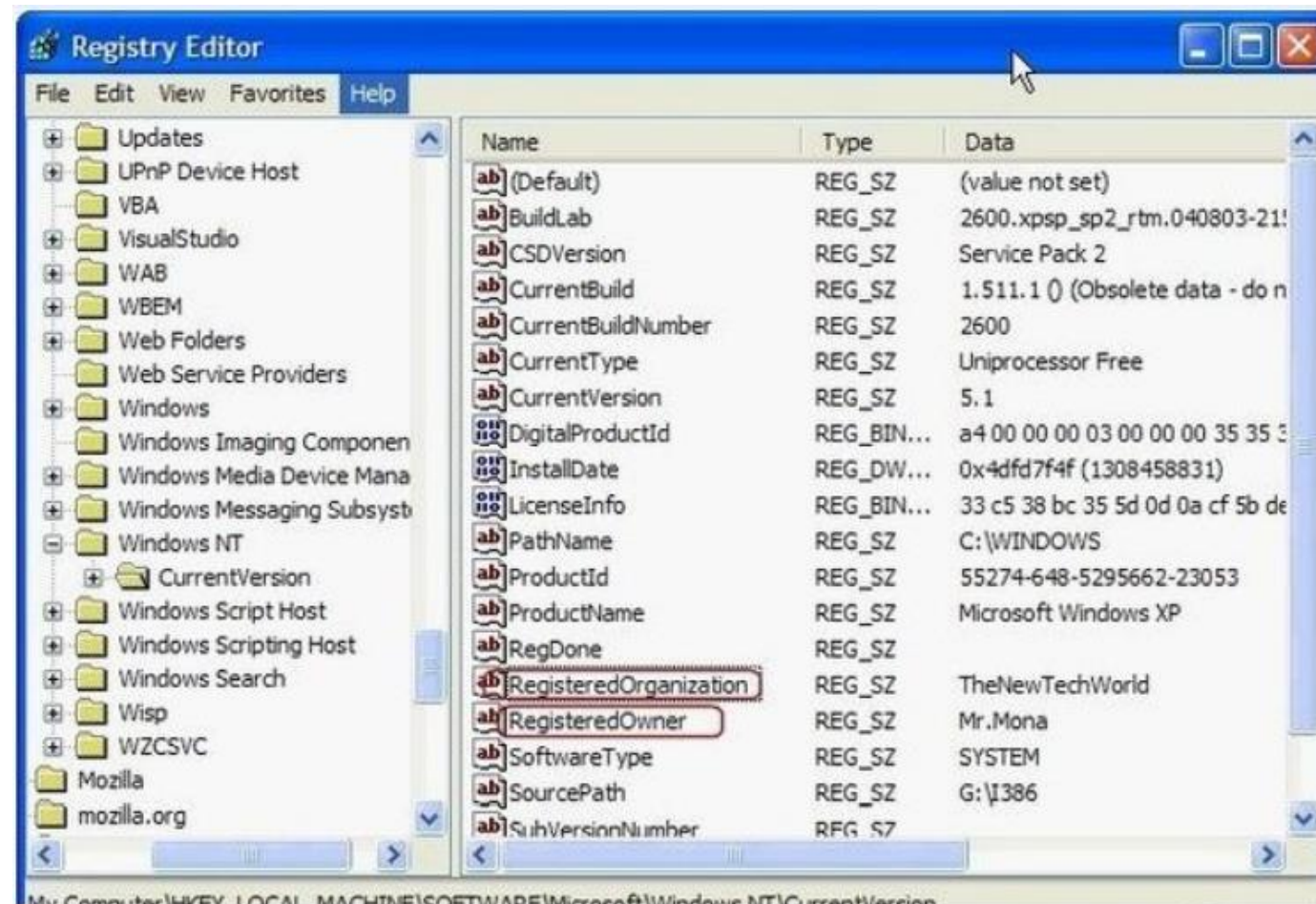
Forensically Interesting artefacts

29

- Configuration settings
- Application settings
 - Download directories
 - Recently accessed files (images, movies, etc.)
 - AutoStart locations
 - Applications that start w/ little or NO user interaction
- Tracking info
 - Attached USB devices (thumb drives, Ext HD, digital cameras)
 - User activity MRUs
 - Viewed documents or images
 - Applications installed or launched (UserAssist keys)

Info of Interest in Registry

- Basic information of system can be acquired.
- Computer Name, Time of Last Shutdown, Product Name, build etc., Time zone settings, **Wireless SSIDS, USB Device connected, user, MRU**



Info of Interest in Registry

31

System Information	Key
Computer Name	SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName
Time of last shutdown	SYSTEM\ControlSet00x\Control\Windows
Product name ,build, version etc.	SOFTWARE\Microsoft\Windows NT\CurrentVersion
Time zone settings	SYSTEM\CurrentControlSet\Control\TimeZoneInformation
User created shares	SYSTEM\CurrentControlSet\Services\lanmanserver\Shares
Audit policy	\SECURITY\Policy\PolAdtEv
Wireless SSIDs	SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID}
USB devices connected	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\USBSTOR
last time	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses
Mounted Devices	HKEY_LOCAL_MACHINE\System\MountedDevices
User	SAM\SAM\Domains\Account\Users\{RID}

Info of Interest in Registry

32

most recently used	<code>\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs</code>
most recently used	<code>\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU</code>
Search Assistant MRU Lists	<code>Software\Microsoft\Search Assistant\ACMrU</code>
Internet downloads directory	<code>Computer\HKEY_CURRENT_USER\Software\Microsof</code>
Restore points	<code>HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore</code>

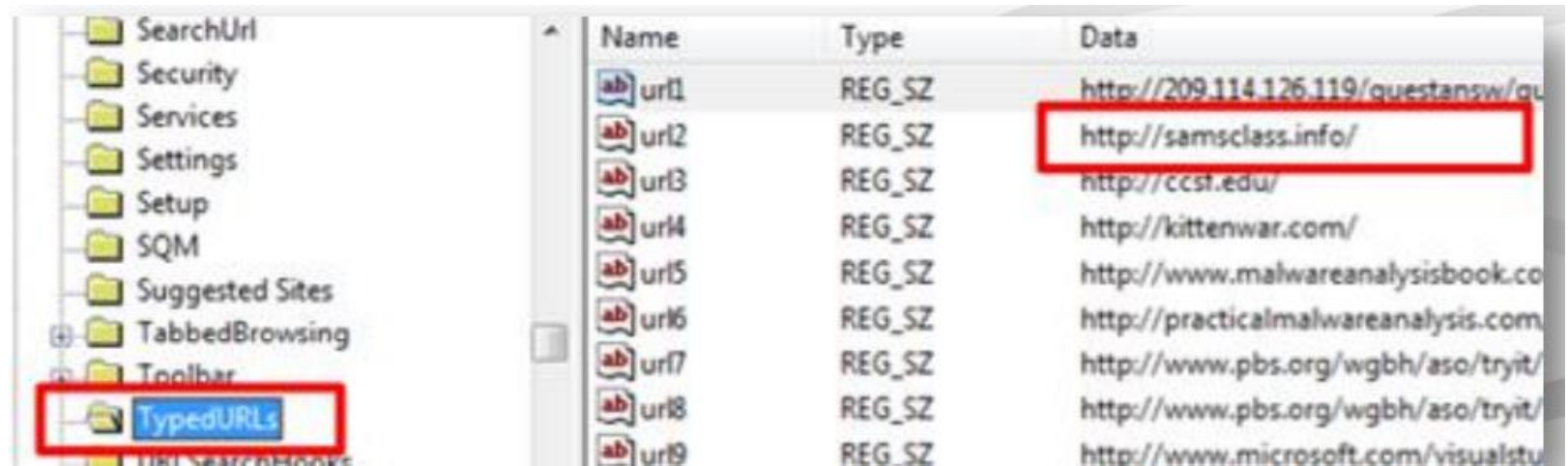
Artifacts of Interest

33

- **Computer name** is the name that the user gives to its computer.
 - is made once in the lifetime usage of the system
 - can be used to trace various activities on network and internet carried by the user.
- **Time of last shutdown** is the time at which the system was completely shut down.
 - can lead us to know the status of the user and time stamps of various files
 - can co-relate to give an idea of the mental status of the suspect.
- Sometime user themselves create **shared folders and applications** for others to use over local network or internet (remote desktops).
 - This information can be traced out to find and analyse what kind of things or information the user was trying to share and thus stamps of the shared files/folders can also be analyzed

Artifacts of Interest

- **Audit policy information** can be very useful as it can let us know about what types of information/events an investigator should look for in the event log.
 - Service set identifications (SSIDs) maintained by Windows can be useful in situations where unauthorized access is need to be investigated and IP addresses needs to be traced
- **USB devices** connected to computer are also registered via PnP (plug and play) manager.



Artifacts of Interest

35

- Many applications maintain **MRU lists**
 - a list of recently used files or opened/created files.
 - search assistant MRU lists are also maintained by search applications.
- **MRU lists of connected systems** etc. are also maintained.
 - This information can of genuine help to understand victim's state of mind or condition just before the crime.
- **System restore points** can be studied to understand **how and when the user created back-ups**.
 - Restore points can be used to understand long back status of the user work.

WINDOWS Password Storage

36

- User and passwords in a window system are stored in either of two places:
 1. SAM (Security Account Manager)
 2. AD (Activity directory) SAM
- 1. **Security Account Manager (SAM)** is a **database file** in Windows XP, Windows Vista and Windows 7 that stores users' passwords. It can be used to authenticate local and remote users.
- 2. **Active Directory** is used to authenticate remote users. SAM uses cryptographic measures to prevent forbidden users to gain access to the system.
- The user passwords are stored in a hashed format in a registry hive. This file can be found in **%SystemRoot%/system32/config/SAM**

FIND it now?

Forensically interesting spots in Windows Registry

Forensic Value	Registry Key Path
Time Zone Information	SYSTEM\ControlSet00#\Control\TimeZoneInformation
Windows Product Info.	SOFTWARE\Microsoft\Windows NT\CurrentVersion
Windows Computer Name	SYSTEM\ControlSet00#\Control\ComputerName\ComputerName
Windows Services	SYSTEM\ControlSet00#\Service
Windows DHCP Config	SYSTEM\ControlSet00#\Services\Tcpip\Parameters\Interfaces\\.\DhcpIPAddress
Legal Notice & Text	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
NTFS Last Accessed	SYSTEM\ControlSet\Control\FileSystem
Autoruns	Highly recommended to use AutoRuns tool which is from the Microsoft's SysInternals Suite.
Installed Applications	HKLM\SOFTWARE\Microsoft\Windows\C.V.\App\Paths
	HKLM\SOFTWARE\Microsoft\Windows\C.V.\Uninstall
Windows Firewall	SYSTEM\ControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\EnableFirewall
	SYSTEM\ControlSet\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile\EnableFirewall
	SYSTEM\ControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\EnableFirewall
Remote Desktop	SYSTEM\ControlSet\Control\TerminalServer\fdenyTSConnections
Network History	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Nla\Cache
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
Network Types (Wired is 0x06 , Broadband is 0x17 , Wireless is 0x47)	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
Shutdown Details	HKLM\SYSTEM\ControlSet001\Control\Windows
ApplInit_DLLs	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\Applinit_DLLs
	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadApplinit_DLLs
Windows Recycle Bin	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{GUID}\NukeOnDelete
Last User Logged In	SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser
User Sessions	SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\SessionData\<#>\LastLoggedOnSamUser

Forensically interesting spots in Windows Registry

Forensic Value	Registry Key Path
Local Users	SAM\Domains\Users
UserPasswordHint	SAM\SAM\Domains\Account\Users\\<32\bit>hexvalue\UserPasswordHint
Graphic Login Tile	SAM\Domains\Account\Users\\<32\bit>hexvalue\UserTile
UAL Setting	SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
User Assist Key	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
Last Registry Subkey that was viewed by the user	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit>LastKey
Hidden Files Settings	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
Hiding File Extensions	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
Start Menu Run MRUs	HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
RecentDocs MRUs	HKEY_USERS\{SID}\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
Remote Desktop MRU	HKEY_USERS\{SID}\Software\Microsoft\Terminal\Server\Client\Servers HKEY_USERS\{SID}\Software\Microsoft\Terminal\Server\Client\Default
IE TypedURLs	NTUSER.DAT\Software\Microsoft\Internet Explorer
IE Browser Settings	NTUSER.DAT\Software\Microsoft\Internet Explorer\Main
MUICache	NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\MUICache

Quiz 2 [5 minutes] CLO No. 1

Western Digital 26400

Drive Parameters: 13328 cyl • 15 heads • 63 spt • 6448.6 MB



What will be the capacity of this drive?

Quiz 3

8th April (After Eid Holidays)

EC Council Modules 1, 2 3 and 4

EC-Council



Digital Forensics Essentials

PROFESSIONAL SERIES

EC-COUNCIL OFFICIAL CURRICULA

References

- <https://www.hackers-arise.com/post/2016/10/21/Digital-Forensics-Part-5-Analyzing-the-Windows-Registry-for-Evidence>
- <https://www.sciencedirect.com/book/9780128032916/windows-registry-forensics>
- https://books.google.com.pk/books?id=x4hIH4JEBIsC&printsec=copyright&redir_esc=y#v=onepage&q&f=false

ANY QUESTIONS