INVESTIGATING WINDOWS REGISTRY ------PART 3

7.WINDOWS REGISTRY

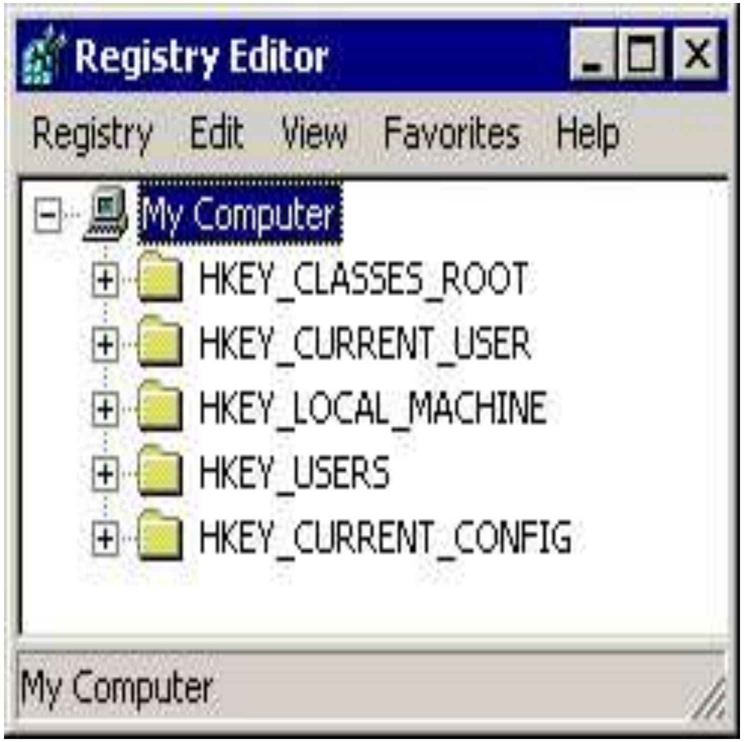
- A central hierarchical database to store information necessary to configure the system for one or more users, applications and hardware devices.
- Replaces AUTOEXEC.BAT, CONFIG.SYS and INI files
- The Registry can reveal the software installed in the past, the security configuration of the machine, DLL trojans and startup programs.

PURPOSE OF USING REGISTRY

- to view what software has been installed
- To track unauthorized software such as steganography tools, **L0phtcrack,** and **sniffer programs.**
- for identifying software and applications that were installed on a system and then manually deleted.

WINDOWS REGISTRY

There are five root keys:



My Computer
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

My Computer

(HKCR)
(HKCU)
(HKLM)
(HKU)
(HKCC)

REGISTERY TOOLS

- **Registry Reader**: Access Data
- **Encase**
- Windows
  - **Regedit**
  - **Regedt32**
- Freeware tools
  - Never work on the original
  - Make a copy

REGISTER ROOT KEYS ARE MADE FROM MAJOR FILES:

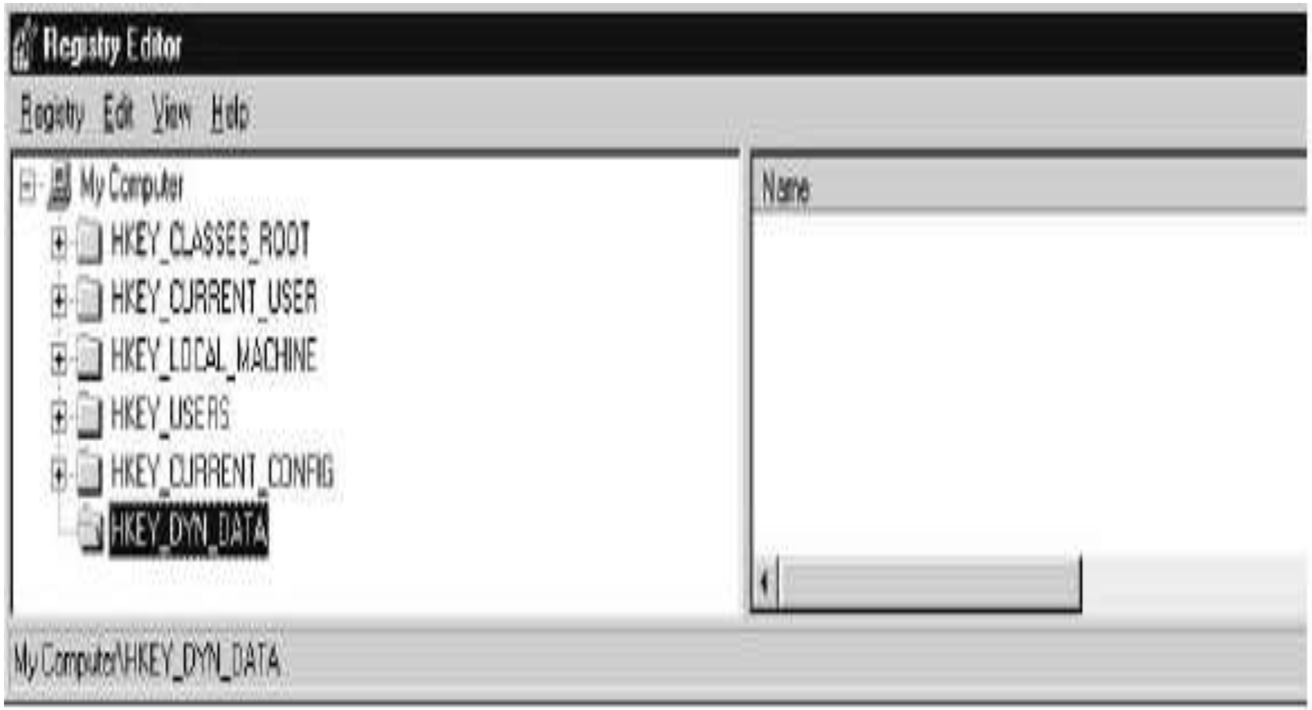
- SAM
- SECURITY
- SOFTWARE
- SYSTEM

The default location for these files

\WINNT\System32\Config directory.

REGISTRY ON LIVE SYSTEM

- To review the contents , use the Registry Editor **(Regedit)**



REGISTRY OFFLINE

- **Meaning**

Investigating the Registry from a forensic duplicate without booting from the native operating system

PROCESS

1. Copy the Registry hive(root) files from their **default location** to your forensic workstation ***(%system32%\System32\Config)***
2. Run Regedit
3. Import these files by selecting Registry
4. Import Registry File

8.WEB BROWSER FILES

Purpose

- To track the recently viewed web pages

WEB BROWSER

NETSCAPE , INTERNET EXPLORER maintains a cache that contains recently viewed web pages.

- **Netscape History Files**
- **Netscape.hst**(history file) path \Program Files\Netscape\Users\<*username*> *directory*
- **Netscape's fat.db** file maintains an even longer history of browsing activity

- **Internet Explorer History Files**
- **index.dat** file holds the viewer history
- The actual HTML and files are stored in the Internet Explorer cache files

Netscape's fat.db and netscape.hst files and Internet Explorer's index.dat file are **binary files**

TOOLS USED
Internet Explorer History Viewer
Pasco, a free forensic utility(allows the examination of Internet Explorer cache files)
EnCase

WEB BROWSER FILES

DIAL UP NETWORKING

- determine the browsing activities of a user
- By reviewing DUN settings on system.
- **Dial -on-demand** allows Windows to initiate a connection automatically whenever an app requires the use of the Internet.
- A list of IP addresses are maintained by **autodial** feature.
- Command ***rasautou –s***

  To view autodial database.