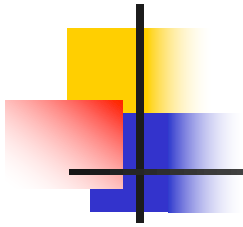
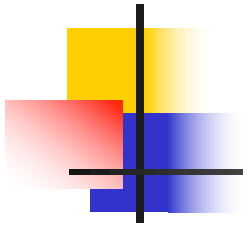


Registry

- Central hierarchical, configuration database
- Operating system relies on it
- Contains information about
  - Hardware including plug and play devices
  - Users information, preferences
    - Support multiple users
  - Application information
  - Network information



Registry (Cont.)

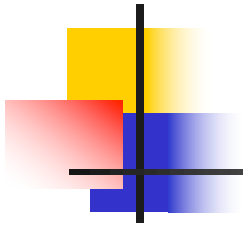
- The *registry* is a system-defined hierarchical database in which Windows applications and services store and retrieve configuration data.
- Key:

The registry database is structured in a tree format where each tree node is called a **Key**.

The Key can contain **Subkeys** and zero or more settings (**values**).

The registry database may vary with Microsoft Windows versions.

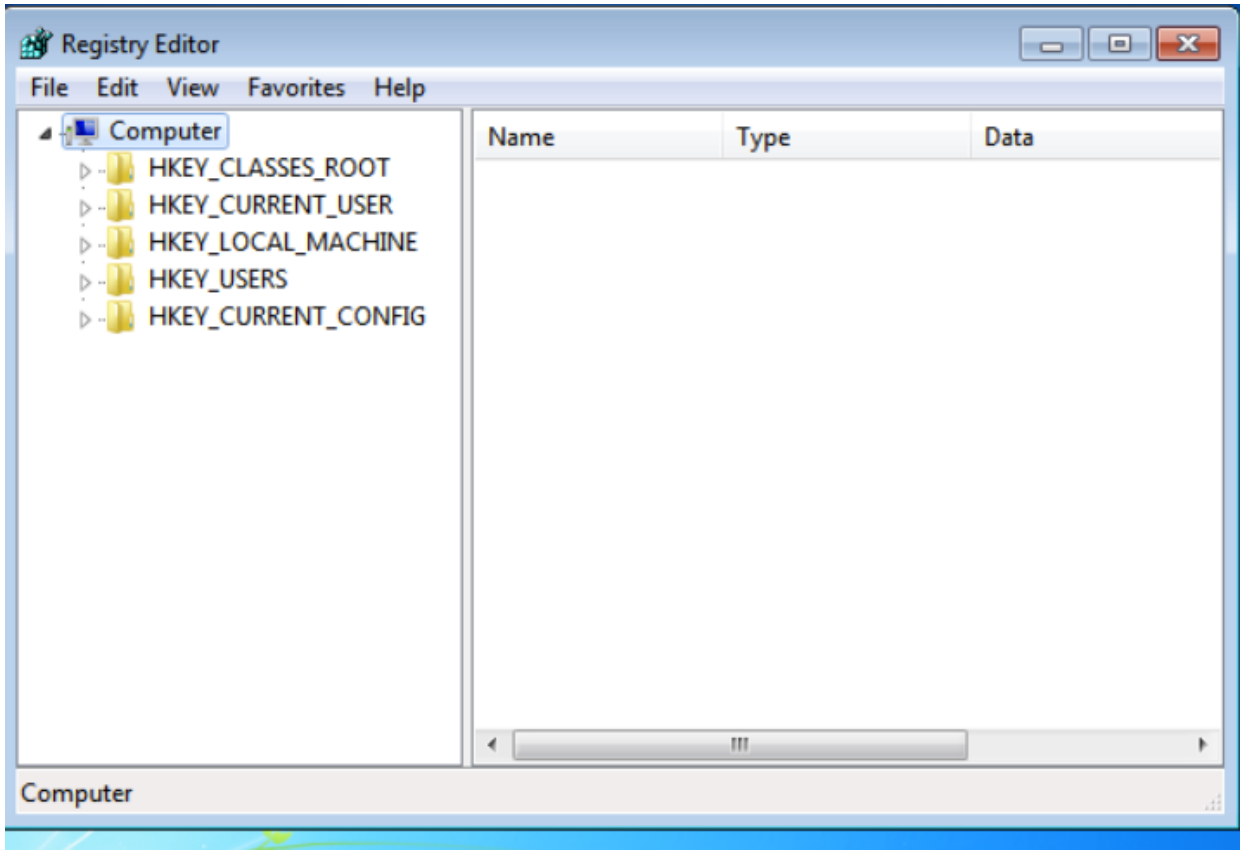
What can you possibly find from registry files?

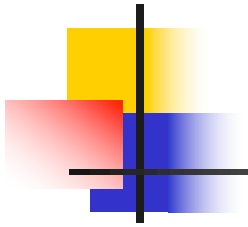


- Usernames and passwords for programs, e-mail, and Internet sites
- A history of Internet sites accessed, including date and time
- A record of Internet queries such as searches via Google, Yahoo
- Lists of recently accessed files
- A list of programs installed on the system

Registry (Cont.)

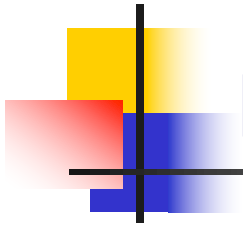
- Typically, there are five trees under My Computer:





Registry Tree

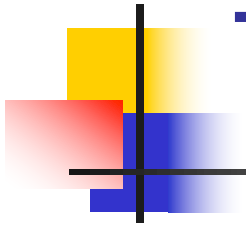
- HKEY_CLASSES_ROOT
  - contains file name extension associations and other program Identifiers.
- HKEY_CURRENT_USER
  - Defines the preferences of the current user such as environment variables, data about program groups, colors, printers, network connections, and application preferences
- HKEY_LOCAL_MACHINE
  - Define the physical state of the computer, including data about the bus type, system memory, and installed hardware and software



Registry Tree (Cont.)

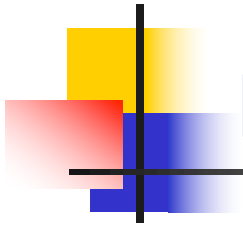
- HKEY_USERS
  - Define the default user configuration for new users on the local computer and the user configuration for the current user.
-
- HKEY_CURRENT_CONFIG
  - Contains information about the current hardware profile of the local computer system.
  - The standard hardware configuration is stored under the **Software** and **System** keys of **HKEY_LOCAL_MACHINE**

The data is divided into computer-specific and user-specific values before storing into the registry database. For example, when an application is installed, it stores computer-specific data in HKEY_LOCAL_MACHINE key. If the application records user data, it should be stored in HKEY_CURRENT_USER Key.



Tools to view/edit registry:

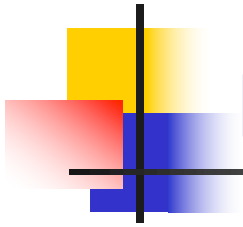
- To Read/Edit registry, use regedt32/regedit
  - Provided by Microsoft Windows.
- Reg view (read only)
- RegRipper
- Registry Recon
- Registry Explorer
- AccessData Registry Viewer
- Encase



Registry Hives

- Registry editor only shows the hierarchical structure of the registry as a single tree. However, registry files are not stored in a single file on the hard drive.

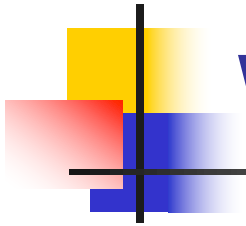
- Windows stores registry in separate binary files called hives.
- For each hive, additional supporting files are also created that contain backup copy of the respective hives to restore the hives during failed system boot.



Registry Hives (Contd.)

Registry hives and their supporting files on disk.

Registry hive	Supporting 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_USERS\.DEFAULT	Default, Default.log, Default.sav

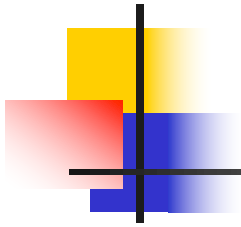


Where to find the supporting files

- Most supporting files for **HKEY_LOCAL_MACHINE** hive such as SAM, Security, Software, System are stored in C:\WINDOWS\System32\config\

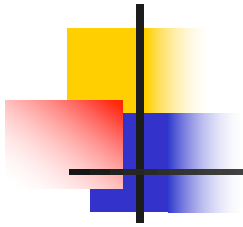
- The supporting files for **HKEY_CURRENT_USER** hive such as NTUSER.DAT are stored in C:\Users\USER_NAME. Every user profile has an Ntuser.dat file that contains personal files and preference settings specific to the user. For example, desktop preferences, default document folder etc.

- Registry files are a great source of system and user information. Therefore, very critical for forensic investigation.



Registry values

- Contains three parts
  - Name
  - Type
  - Data
- Subkey contains at least one value, its default value
  - (default) REG_SZ (value not set)



Registry Value type

- REG_BINARY
  - raw binary data
  - Must contain even numbers of bytes
  - For example, 01 BD 42 56 34 00
- REG_DWORD
  - 32-bit, double-word value
  - For example, 0x01ACDE01
- REG_SZ
  - String values
  - The most common and simplest type