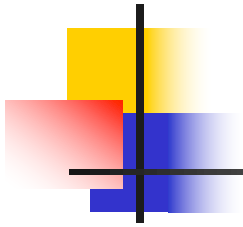
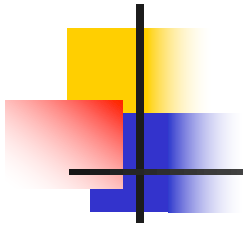


Registry

- 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.)

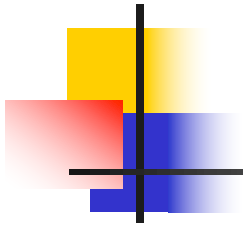
- The *registry* is a system-defined hierarchical database in which Windows applications and services store and retrieve configuration data.
- Key:

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.

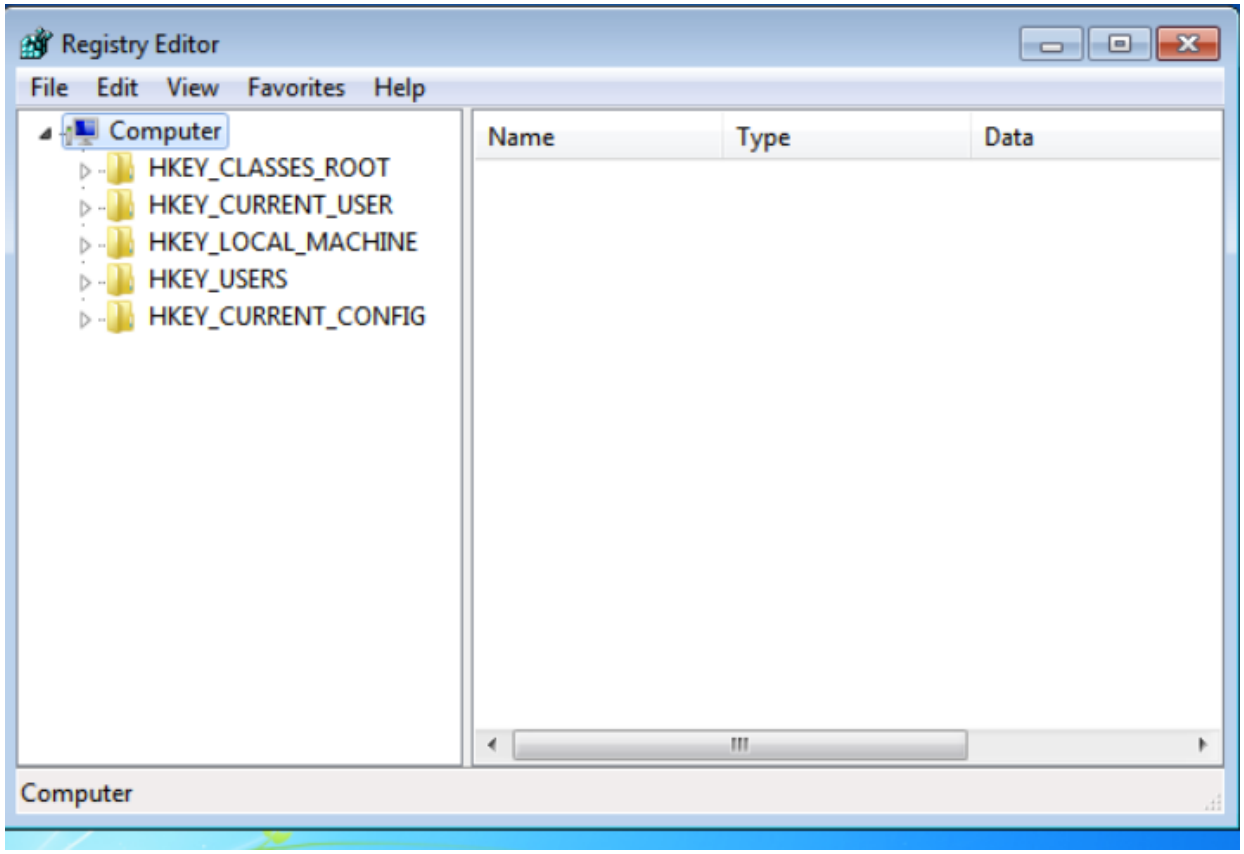
What can you possibly find from registry files?

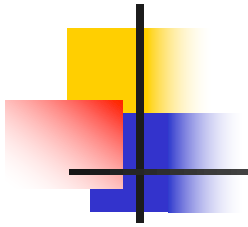


- Usernames and passwords for programs, e-mail, and Internet sites
- A history of Internet sites accessed, including date and time
- A record of Internet queries such as searches via Google, Yahoo
- Lists of recently accessed files
- A list of programs installed on the system

Registry (Cont.)

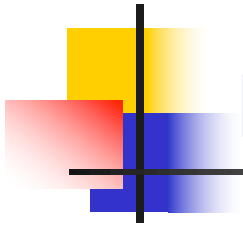
- Typically, there are five trees under My Computer:





Registry Tree

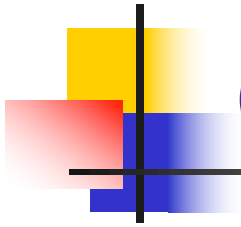
- HKEY_CLASSES_ROOT
  - contains file name extension associations and other program Identifiers.
- HKEY_CURRENT_USER
  - Defines the preferences of the current user such as environment variables, data about program groups, colors, printers, network connections, and application preferences
- HKEY_LOCAL_MACHINE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



Registry Tree (Cont.)

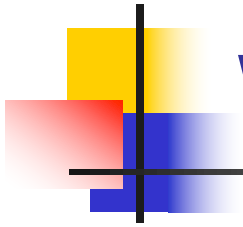
- HKEY_USERS
  - Define the default user configuration for new users on the local computer and the user configuration for the current user.
-
- HKEY_CURRENT_CONFIG
  - Contains information about the current hardware profile of the local computer system.
  - The standard hardware configuration is stored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



Glean evidence from Registry

- Make sure that you registry is backed up
- On Win95/98, registry is comprised of
  - Windows\System.dat
  - Windows\User.dat
- On WinNT/2K/2003, registry is comprised of
  - Several hive files in %systemroot%\system32\config
    - SYSTEM
    - SAM
    - SECURITY
    - SOFTWARE
  - NTUSER.dat files related to each user account

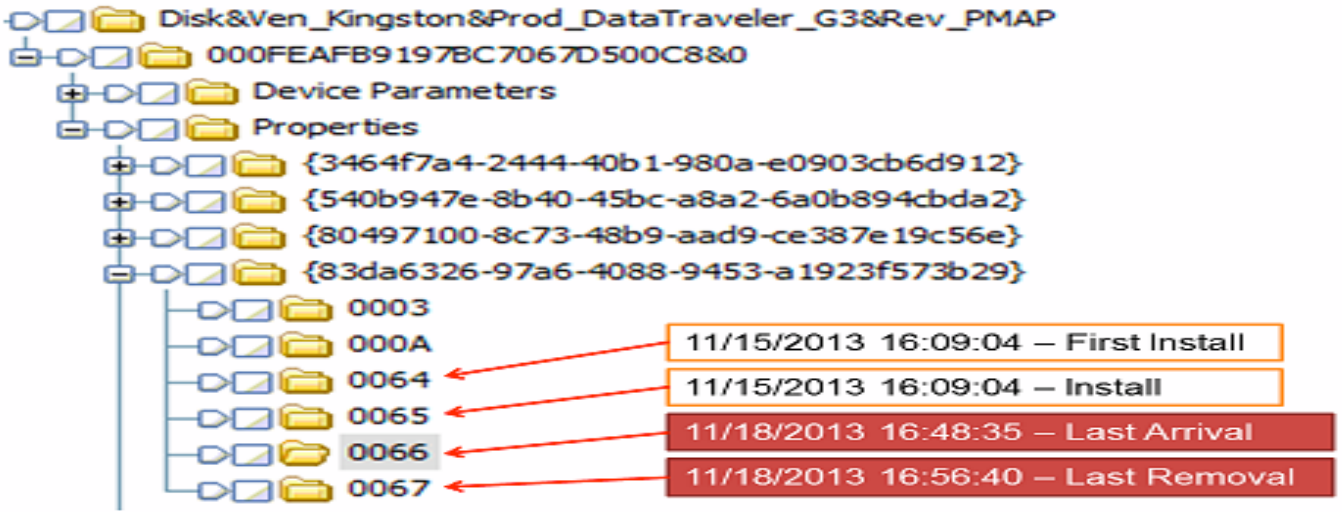


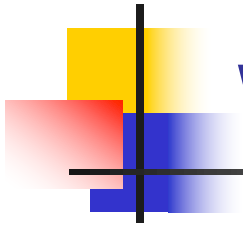
What can you find from SYSTEM?

- SYSTEM
  - Computer Name
  - Device Drivers and driver letter mappings
  - The Last Known Good Configuration
  - Setup information
  - Hardware profile
- Use of SYSTEM
  - Determine which control set is active
  - Find out timezone, Mounted devices

What can you find from SYSTEM (Con't)?

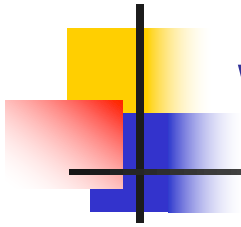
- Finding USB last insertion and removal time.
  - In USBSTOR under:
    \ControlSet00x\Enum\USBSTOR
    (x may vary, usually 1)
  - Timestamps to the registry for Device **Last Insertion (66)** Date, Device **Last Removal (67)** Date and Firmware Date.





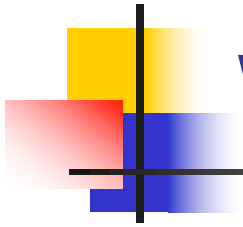
What can you find from SECURITY?

- Contains security settings such as user and group policies



What can you find from SOFTWARE?

- Contains a list of all installed programs and their settings
- Paths to application files and dirs
- Use of SOFTWARE
  - RigisteredOwner
  - RegisteredOrganization
  - ProductID
  - ProductName
  - InstallDate



What can you find from NTUSER?

- Protected storage information
  - An access-restricted area of the registry that stores confidential user information
- The recently run programs
- The recently used (open or save) files
- Recently accessed networks
- Internet Explorer usages and password
- User preference settings