

# CS 798: Digital Forensics and Incident Response

## Lecture 10 - Evidence in Operating Systems

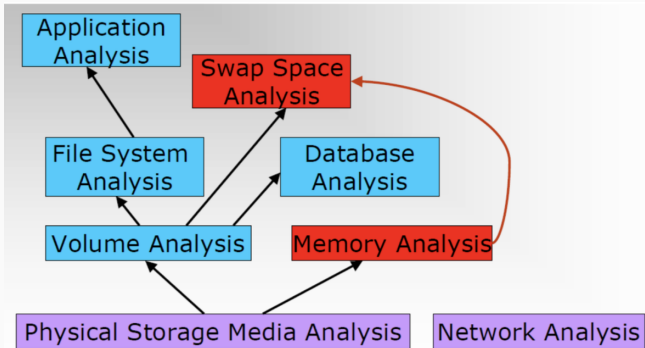
---

Diogo Barradas

Winter 2025

University of Waterloo

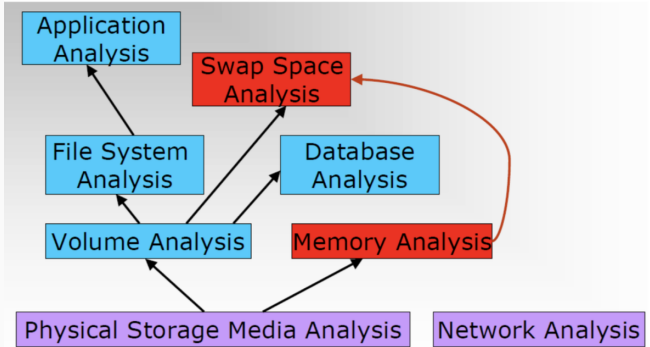
# We talked about file systems...



Source: „File System Forensic Analysis“, Brian Carrier

- Studied the kind of evidence that can be found on file systems
- Learned multiple techniques to retrieve that evidence
- Seen how to recover deleted files with and w/o metadata

# Evidence in operating systems



Source: „File System Forensic Analysis“, Brian Carrier

- Why is the operating system relevant in forensics?
- What kind of evidentiary artifacts may be useful?
- Where to locate those artifacts?

1. Investigation of OS artifacts

2. Case study: Windows

Windows Registry

Windows Event log

3. What about Linux?

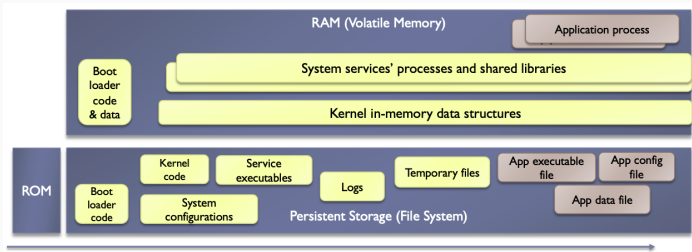


# Investigation of OS artifacts

---

# What do we mean by OS artifacts?

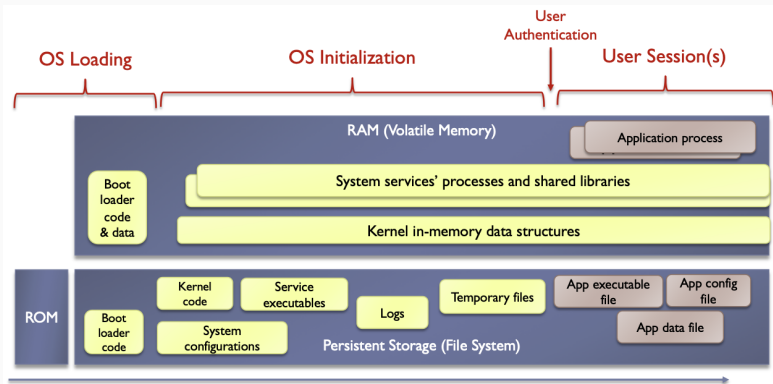
- Evidentiary data pertaining to data / code maintained / executed by the OS
  - We broadly include: firmware, bootloader, kernel, system libraries, and system services
  - Data structures: in-memory (e.g., process list) and persistent (e.g., config files)
- Can serve as containers for data / code specific to applications



(Sketchy) system state evolution over time

# Generation of OS artifacts over time

- Rough depiction of stages during the normal operation of a computer system



# Artifacts result from the OS's supervision activities

- Manages all **interactions** with the environment
  - Access to the network, controlling the time, plugged storage devices, scanning available networks, etc.
- Manages **execution** and state of services & applications
  - Programs executed at bootstrap, when the user logs in, or by the user itself
- Manages **authentication** and access controls
  - Validates user credentials, grants/denies access to resources, keeps logs

## OS artifacts can help track past / present user activity

- Ultimately, in a forensic examination, we're investigating the actions of a user (real / bot)
- Almost every event or action is the result of a user either doing something (or not doing something)
- Many events introduce changes to the system state that are supervised by the OS
- OS forensics helps us understand how system changes correlate to events resulting from the actions of users

## Examples of typical user activities to investigate

1. File download
2. Program execution
3. File opening / creation
4. Deleted files
5. Physical device location
6. USB or drive storage
7. Account usage
8. Network usage

# Where to look? Depends on the operating system

- **Linux**

- Configuration files
  - `/etc/passwd`
  - `/etc/sudoers`
  - `/etc/inittab`
  - `/var/spool/cron/*`
- Log files
  - `/var/log/boot.log`
  - `/var/log/auth.log`
  - ...

- **Windows**

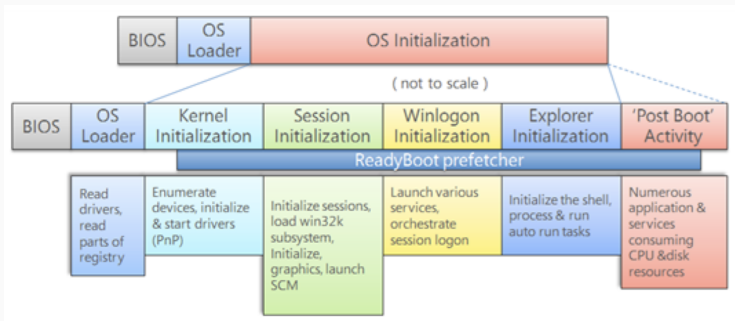
- Dedicated data structures
  - Windows Registry
- System logging service
  - Windows Event log
- Special files

## Case study: Windows

---



# Windows boot sequence



# Case study: Windows

---

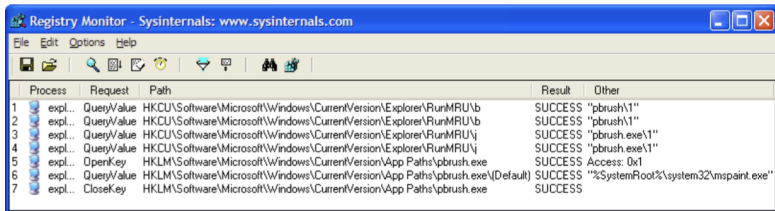
## Windows Registry

# Forensics relevance of the Windows Registry

- The Registry is the heart and soul of Windows OSes and a wealth of information can be recovered:
  - System configuration
  - Devices on the system
  - User names
  - Personal settings, browser preferences, etc.
  - Web browsing activity
  - Files opened
  - Programs executed
  - Applications' settings

# Registry access activity

- Virtually everything done in Windows refers to or is recorded into the Registry
  - RegMon can be used to display registry activity in real time
- Registry access barely remains idle: the registry is referenced in one way or another with every action taken by the user

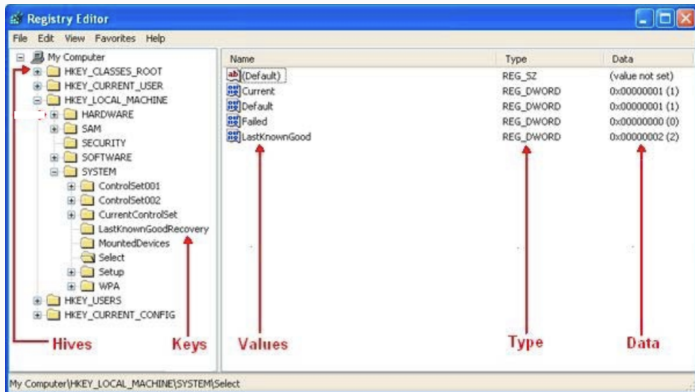


The screenshot shows the 'Registry Monitor' window from Sysinternals. The title bar reads 'Registry Monitor - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Edit', 'Options', and 'Help'. The toolbar contains icons for file operations, search, and monitoring. The main area displays a table of registry activity.

	Process	Request	Path	Result	Other
1	expl...	QueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\b	SUCCESS	"pbrush\1"
2	expl...	QueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\b	SUCCESS	"pbrush\1"
3	expl...	QueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\j	SUCCESS	"pbrush.exe\1"
4	expl...	QueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\j	SUCCESS	"pbrush.exe\1"
5	expl...	OpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\pbrush.exe	SUCCESS	Access: 0x1
6	expl...	QueryValue	HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\pbrush.exe\Default	SUCCESS	"%SystemRoot%\system32\mspaint.exe"
7	expl...	CloseKey	HKLM\Software\Microsoft\Windows\CurrentVersion\App Paths\pbrush.exe	SUCCESS	

# Structure of the Windows Registry

- The Registry can be seen as a unified file system
  - The Registry's specific structure is divided into key and value
- Main root keys (**hives**) represent the root directory, sub-keys represent the sub folders, and values represent the files



# Root key functions

- **HKEY\_LOCAL\_MACHINE (HKLM)**
  - Contains system-wide hardware settings and configuration information (e.g., list of drives mounted on the system)
- **HKEY\_USERS (HKU)**
  - Contains the root of all user profiles that exist on the system
- **HKEY\_CLASSES\_ROOT (HKCR)**
  - Ensures a program opens when executed in Windows Explorer
- **HKEY\_CURRENT\_USER (HKCU)**
  - Contains the profile of the user who is currently logged in
- **HKEY\_CURRENT\_CONFIG (HCU)**
  - HW profile used by the computer during start up

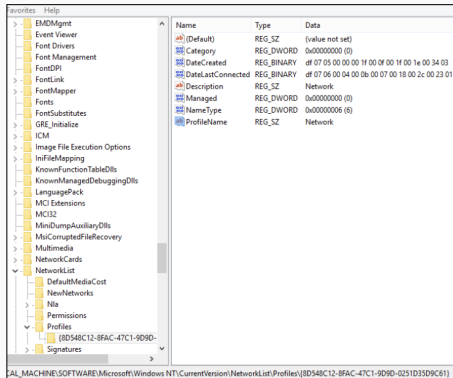
'HKEY' is an abbreviation for Handle to a Key

# HKEY\_LOCAL\_MACHINE (HKLM)

- Settings that are used by the system during start-up
  - It is independent from the user login
- Contains five subkeys:
  - **System**
    - System configuration, e.g., computer name, time zone
  - **Software**
    - Installed applications and OS services
  - **SAM (Security Account Manager)**
    - Stores user and group security information
  - **Security**
    - The security policy of the current user
  - **Hardware**
    - Information about the hardware devices

# Network history

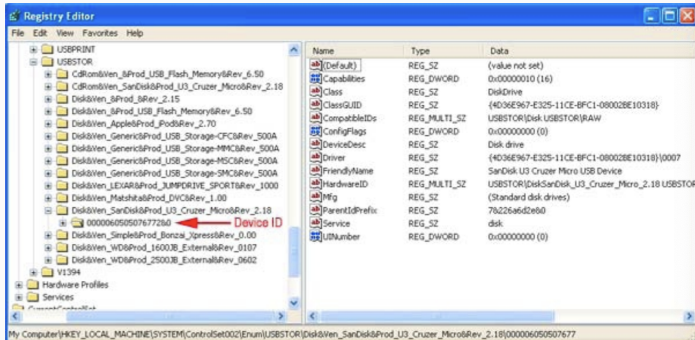
- Identify networks the computer has been connected to
  - Wireless or wired
  - Domain/intranet name
  - SSID
  - Gateway MAC Address
- Location:
  - HKLM\Software\Microsoft\WindowsNT\CurrentVersion\NetworkList
- Also tell the last time the network was connected to





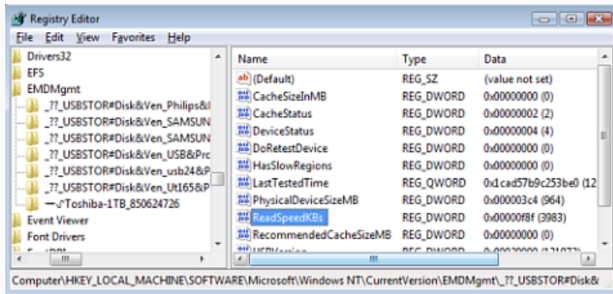
# USB devices

- Anytime a device is connected to the Universal Serial Bus (USB), drivers are queried and the device's information is stored into the Registry (i.e., thumb drives)
  - HKLM\System\CurrentControlSet\Services\USBSTOR



# Volume serial number

- Serial number of the USB volume
  - HKLM\Software\Microsoft\WindowsNT\CurrentVersion\EMDMgmt

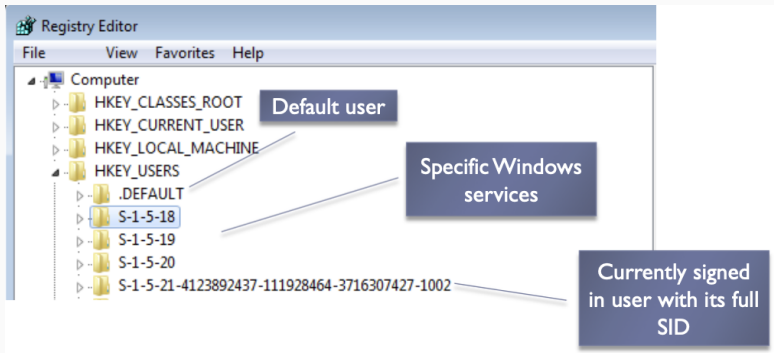


`\\_??_USBSTOR#Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15#0C90195032E36889&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}GEEKSQUAD_1414378827`

- Drive letter and volume name
  - HKLM\System\MountedDevices

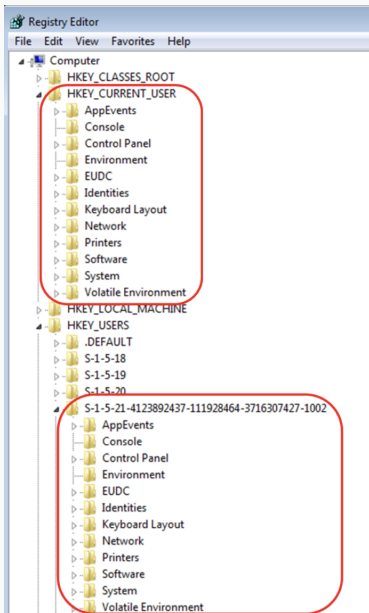
# HKEY\_USERS (HKU)

- Contains user-specific configuration information for all currently active users on the computer



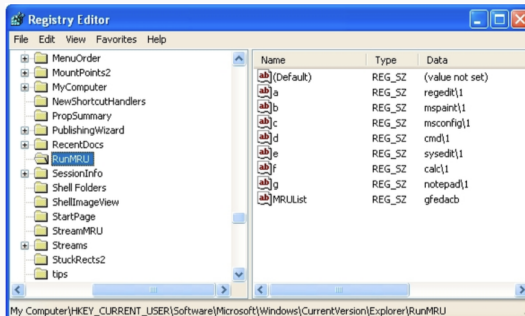
# HKEY\_CURRENT\_USER (HKCU)

- HKCU is a pointer to the current user under the HKU



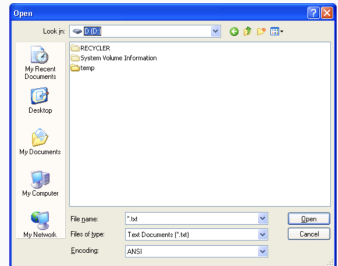
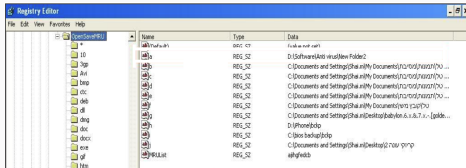
# MRU lists

- MRU (most recently used) lists contain entries about specific actions done by the user
- MRU lists are located throughout different Registry keys
  - e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
- When a user types a command into the 'Run' box via the Start menu, the entry is added to this Registry key



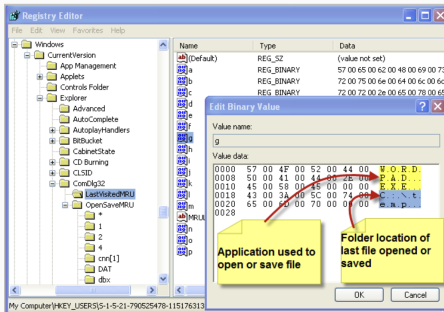
# OpenSave MRU

- OpenSave MRU: tracks files that were opened / saved within a Windows shell dialog box
  - e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDMRU



# Last Visited MRU

- Tracks the specific executable used by an application to open the files documented in the OpenSaveMRU key
- Location:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
- e.g., wordpad.exe was last run to open file in folder c:\temp



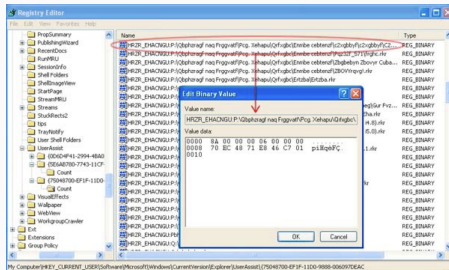
# MRU lists are widely used also by applications

XP Search Files	Software\Microsoft\Search Assistant\ACMRu\5603
Internet Search Assistant	Software\Microsoft\Search Assistant\ACMRu\5001
Printers, Computers and People	Software\Microsoft\Search Assistant\ACMRu\5647
Pictures, music, and videos	Software\Microsoft\Search Assistant\ACMRu\5604
XP Start Menu - Recent	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
R. Desktop - Connect	Software\Microsoft\Terminal Server Client\Default [MRUnumber]
Run dialog box	Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
Regedit - Last accessed key	Software\Microsoft\Windows\CurrentVersion\Applets\Regedit
Regedit - Favorites	Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites
MSPaint - Recent Files	Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
Mapped Network Drives -	Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU
Computer searched via Windows Explorer	Software\Microsoft\Windows\CurrentVersion\Explorer\FindComputerMRU
WordPad - Recent Files	Software\Microsoft\Windows\CurrentVersion\Applets\Wordpad\Recent File List
Common Dialog - Open	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
Common Dialog - Save As	Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
WMP XP - Recent Files	Software\Microsoft\MediaPlayer\Player\RecentFileList
WMP XP - Recent URLs	Software\Microsoft\MediaPlayer\Player\RecentURLList
OE6 Stationery list 1 - New Mail	Identities\{C19958F2-22F3-4C6A-9AE0-12049CE0706F}\Software\Microsoft\Outlook Express\5.0\Recent Stationery List *the CLSID varies, just an example given
OE 6 Stationery list 2 - New Mail	Identities\{C19958F2-22F3-4C6A-9AE0-12049CE0706F}\Software\Microsoft\Outlook Express\5.0\Recent Stationery Wide List *the CLSID varies
PowerPoint - Recent Files	Software\Microsoft\Office\10.0\PowerPoint\Recent File List
Access - Filename MRU	Software\Microsoft\Office\10.0\Common\Open Find\Microsoft Access\Settings\File New Database\File Name MRU
FrontPage - Recent lists	Software\Microsoft\FrontPage\Explorer\FrontPage Explorer\Recent File List
Excel - Recent Files	Software\Microsoft\Office\10.0\Excel\Recent Files
Word - Recent Files	Software\Microsoft\Office\10.0\Word\Data



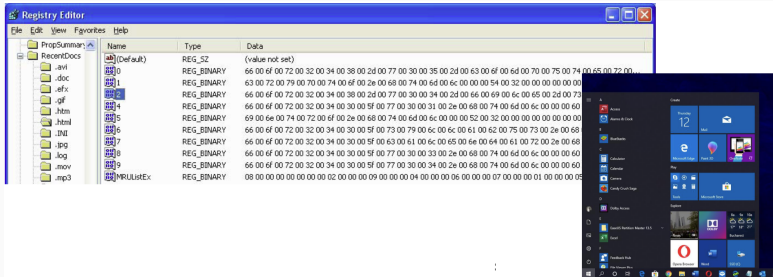
# UserAssist

- The UserAssist key contains information about the exe files and links that you open frequently
  - Indicates last accessed system objects
  - e.g., Control Panel applets, shortcut files, programs, etc.
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist



## Recent files

- A registry key tracks the last files and folders opened and is used to populate data in “Recent” menus of the Start menu
- Location:
  - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



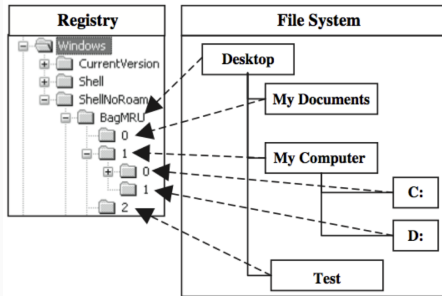
# MS Office recent files

- MS Office programs track their own Recent Files list to make it easier for users to remember the last files they were editing
- Location:
  - HKCU\Software\Microsoft\Office\VERSION

PowerPoint - Recent Files	Software\Microsoft\Office\10.0\PowerPoint\Recent File List
Access - Filename MRU	Software\Microsoft\Office\10.0\Common\Open Find\Microsoft Access\Settings\File New Database\File Name MRU
FrontPage - Recent lists	Software\Microsoft\FrontPage\Explorer\FrontPage Explorer\Recent File List
Excel - Recent Files	Software\Microsoft\Office\10.0\Excel\Recent Files
Word - Recent Files	Software\Microsoft\Office\10.0\Word\Data

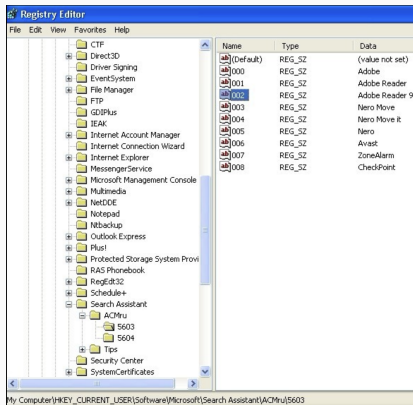
# Shell Bags

- Track user window viewing preferences to Windows Explorer
  - Store info about which folders were most recently browsed
- Location:
  - `HKU\Software\Microsoft\Windows\Shell\Bags`



# Search Assistant

- Search assistant remembers a user's search terms for filenames, computers, or words on a file
- Location:
  - HKCU\Software\Microsoft\SearchAssistant\ACMru\#\#\#\#
- Search:
  - 5001: the Internet
  - 5603: doc names
  - 5604: Words in a file
  - 5647: Printers, computers, and people



# More Registry artifacts

- **System information**

- Computer name, OS version, last shutdown time

- **Time zone information**

- important for establishing a timeline of activity on the system

- **Shares**

- Remotely shared resources, e.g., disk volumes (can be hidden)

- **Audit policy**

- Indicates types of events recorded in the Event Log

- **Mounted devices**

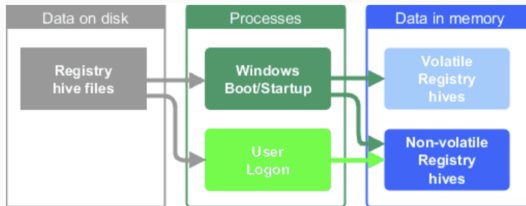
- Information about devices and volumes mounted on NTFS

- **Users**

- account creation time, names, last login time, last failed login attempt, account expiration, etc.

# How the registry is assembled

- The registry is commonly described as a hierarchical database, but note two important facts:
  - The registry database is only ever complete when loaded into your computer's memory
  - The registry is the sum of two parts, the data and the processes that create it and provide access to it



# Forensic analysis of the registry

- Browse the registry using some registry viewer tool
  - e.g., regedit
- Copy the entire memory-resident registry
  - e.g., Regripper
- Create forensic copies of the registry's files
  - e.g., FTK Imager
- Analyze the dumps using specific decoders
  - e.g., yarp



# Case study: Windows

---

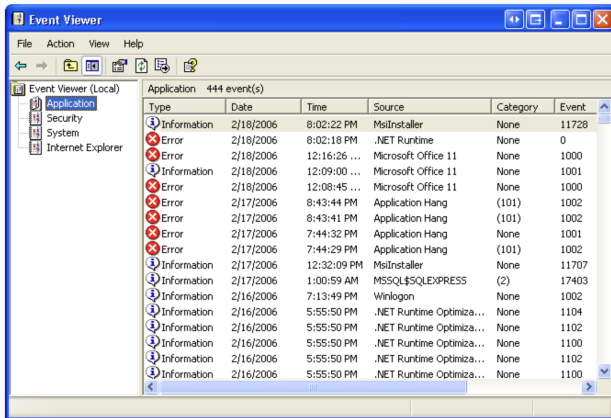
## Windows Event log

# Windows Event log

- Whenever an event, such as a user logging on or off, occurs, the operating system **logs the event**
- An **event** can be any occurrence that the OS or a program wants to keep track of or alert the user about
- Windows has a centralized log service to allow apps and OS to report events that have taken place
  - Application (example: Database message)
  - System (example: driver failure)
  - Security (example: Logon attempt, file access)

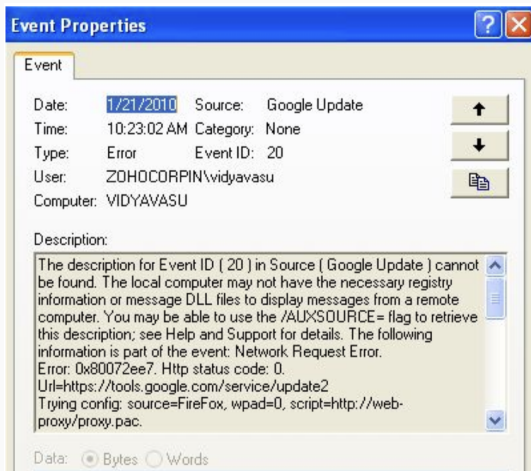
# Structure of the Event log

- The Event Log can be seen using a specific system tool



# Event format

- Events have a specific format and meaning



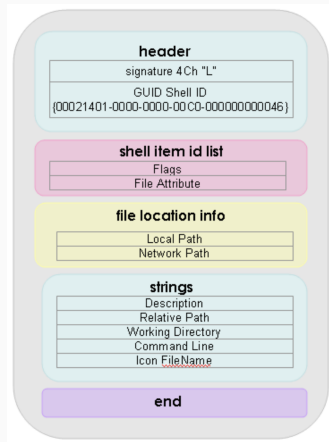
# Last login, last password change, success login

- The last login time will be stored in the registry key
  - SAM\Domains\Account\Users
  - Local accounts of the system and equivalent security identifiers
  - Saves the last time a user's password has been changed
- Successful or failed logons:
  - %systemroot%\System32\winevt\logs\Security.evtx
  - Event ID - 528/4624 - Successful Logon
  - Event ID - 529/4625 - Failed Logon
  - Event ID - 540/4624 - Successful Network Logon

- Analyze logs for suspicious services running at boot time
  - Review services started or stopped around the time of a suspected compromise
- Examples of relevant IDs:
  - 7034 - Service crashed unexpectedly
  - 7035 - Service sent a Start / Stop control
  - 7036 - Service started or stopped
  - 7040 - Start type changed (Boot | On Request | Disabled)
- Numerous malware and worms in the wild utilize Services
  - Services started on boot for malware persistence
  - Services can crash due to attacks like process injection

# Shortcut (LNK) files

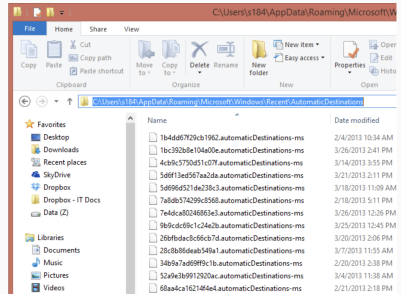
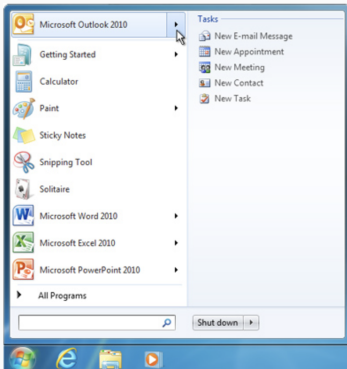
- Shortcut files (.lnk) automatically created by Windows
  - Recent Items
  - Opening local and remote data files and documents will generate a shortcut file
- Location:
  - C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent



Found to deliver malware (see McAfee analysis)

# Windows jump lists

- Windows task bar (or **jump list**) allows users to easily access / execute recent items / tasks
- Location:
  - `C:\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations`





# Prefetch files

- Windows creates a prefetch file when an application is run from a particular location for the very first time; used to speed up the loading of applications
- Location:
  - C:\Windows\Prefetch\exename-hash.pf
  - Includes last time of exec , # of times run, device and file handles used by the program

Application Name	CALC.EXE	1. Hash of the original path of the application
Application Run Count	22	2. Application name
Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	04/24/2014 09:29:16 AM	3. The number of times the application was run
2nd Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	03/31/2014 10:20:52 AM	4. Timestamps for the last 8 times the application was run
3rd Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	03/05/2014 09:47:30 AM	
4th Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	03/03/2014 03:15:12 PM	
5th Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	02/25/2014 01:48:58 PM	
6th Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	02/21/2014 02:48:26 PM	
7th Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	02/20/2014 04:57:18 PM	
8th Last Run Date/Time - (UTC-5:00) (MM/dd/yyyy)	02/19/2014 08:51:49 AM	
Source	PhysicalDrive0 - Partition 4 (Microsoft NTFS, 675.99 GB) OS [C:] (All Files and Folders) - [ROOT]\Windows\Prefetch\CALC.EXE-0FEBF3A8.pf	
Located At	File offset 0	

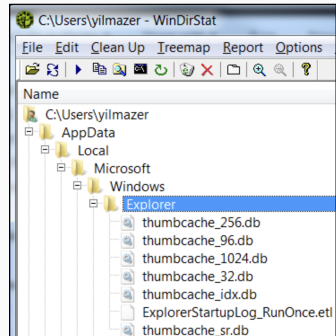
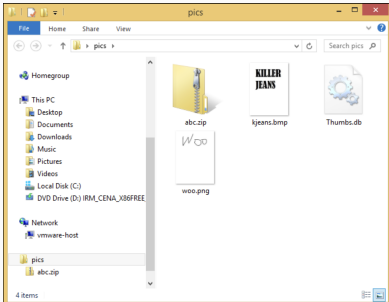
# Autorun locations

- Registry keys that launch programs or apps during boot
  - C:\Windows\Prefetch\exename-hash.pf
  - e.g., in a system intrusion, autorun locations could reveal the installation of a trojan backdoor
- List of common autorun locations:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce  
HKLM\Software\Microsoft\Windows\CurrentVersion\Run  
HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Run  
HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce  
(ProfilePath)\StartMenu\Programs\Startup
```

# Thumbnails

- On Win XP: hidden file `thumbs.db` in directory where pictures exist; stores thumbnail even if pictures deleted
  - Include: thumbnail, last modification time, original filename
- Since Win7: data sits under single directory
  - `C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer`



# Recycle Bin

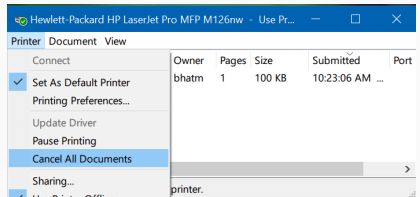
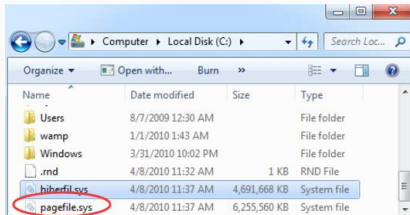
- The Recycle Bin allows user to retrieve and restore files that have been deleted
- The user's deleted file is placed within the file under a subdirectory named with the user's security ID, e.g.,
  - C:\RECYCLER\S-1-5-21-1454471165-630328440-725345543-1003

Operating System	Common File System Structure	Location of Deleted Files
Windows 95/98/ME	FAT32	C:\Recycled\INFO2
Windows NT/2K/XP	NTFS	C:\Recycler\INFO2
Windows Vista	NTFS	C:\\$Recycle.Bin\
Windows 7	NTFS	C:\\$Recycle.Bin\



# More interesting files

- Installed programs
- Printer files
  - Contain information about printing jobs
- `pagefile.sys` and `hiberfil.sys`
  - The swap file and the file for storing RAM contents upon hibernation



# What about Linux?

---

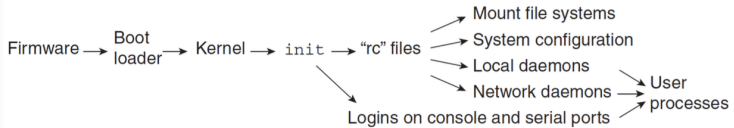
# What's different about Linux?

- No registry
  - Have to gather system info from **scattered sources**
- Different file system
  - No file creation dates (until EXT4)
  - **Different metadata** updated when files deleted
- Files/data are **mostly plain text**
  - Good for string searching and interpreting data



# Linux boot sequence

- At a high-level, Unix systems have same boot sequence



System	Boot Loader Configuration	Kernel File Name	Kernel Configuration
Solaris	/etc/bootrc (x86 platform) firmware (SPARC platform)	/kernel/genunix	/etc/system
Linux	/boot/grub/grub.conf /boot/lilo.conf	/boot/vmlinuz	/etc/sysctl.conf
FreeBSD	/boot.config /boot/loader.conf /boot/loader.rc	/kernel /kernel/kernel	/boot/device.hints



# Basic system profiling

- Linux distro name/version number:
  - `/etc/*-release`
- Installation date:
  - Look at dates on `/etc/ssh/ssh_host*_key` files
- Computer name:
  - `/etc/hostname` (also log entries under `/var/log`)
- IP address(es):
  - `/etc/hosts` (static assignments)
  - `/var/lib/dhclient`, `/var/log/*` (DHCP)
- `/etc/localtime` stores default time zone data

# User accounts

- Basic user data in `/etc/passwd`
  - UID 0 account has admin privs
- Password hashes in `/etc/shadow`
  - (brute force with “John the Ripper”)
- Group memberships in `/etc/group`
- Login history: `/var/log/wtmp`
  - Shows user, source, time, and duration of login
  - Need to use Linux `last` command to view
- Other logs that may contain useful data:
  - `/var/log/auth.log`
  - `/var/log/secure`
  - `/var/log/audit/audit.log`

- `/home/<user>` is a common convention
- Home directory for admin user is `/root`
- “Hidden” files/dirs have names starting w/ “.”
  - Contain app-specific configuration information
  - Sometimes executed at login
  - Possible back-door or persistence mechanism

# Command history

- `\$HOME/.bash_history`
- Unfortunately not time-stamped by default
- Can be modified/removed by user
- Sudo history in:
  - `/var/log/auth.log`
  - `/var/log/sudo.log`

# Persistence mechanisms

- Service start-up scripts
  - `/etc/inittab`, `/etc/init.d`, `/etc/rc.d` (traditional)
  - `/etc/init.conf`, `/etc/init` (upstart)
- Scheduled tasks (“cron jobs”)
  - `/etc/cron*`
  - `/var/spool/cron/*`

# Takeaways

- Windows and Linux are the most popular operating systems on desktop and server platforms
- Due to its central role in setting up and supervising the system, Windows maintains valuable data structures for forensic investigators: the Registry, and the Event Log
- By analyzing artifacts from such sources, we can gather a wealth of info about user activities on the computer

- **Textbook:**
  - Luttgens – Chapters 12.2-12.6
- **Other resources:**
  - Deeper into Windows Registry
  - Windows forensic and security
  - The evolution of Windows
- **Acknowledgements:**
  - Slides adapted from Nuno Santos's Forensics Cyber-Security course at Técnico Lisbon