TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#5: Windows Forensics & File Recovery

Spring 2022

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn

Nội dung trình bày

- Registry Windows
- Recovery Files and Partitions

Windows Forensics

Các loại thông tin trên máy tính

- Volatile Information
- Non-Volatile Information

Volatile Information

- **Volatile information** can be easily modified or lost when the system is shut down or rebooted
- It helps to determine **a logical timeline of the security incident** and the users who would be responsible
- **Volatile data** resides in registers, cache, and RAM

Volatile information includes:

- System time
- Logged-on user(s)
- Open files
- Network information
- Network connections
- Process information
- Process-to-port mapping
- Process memory
- Network status
- Clipboard contents
- Service/driver information
- Command history
- Mapped drives
- Shares

Non-Volatile Information

- Non-volatile data remains **unchanged** when a system is shut down or loses power.
  - Example: Emails, word processing documents, spreadsheets and various "deleted" files
- Such data usually reside in **hard drives**, it also exists in swap files, slack space and unallocated drive space
- Other non-volatile data sources include CD-ROMs, **USB thumb** drives, smart phones, and PDAs

Registry – Nguồn gốc

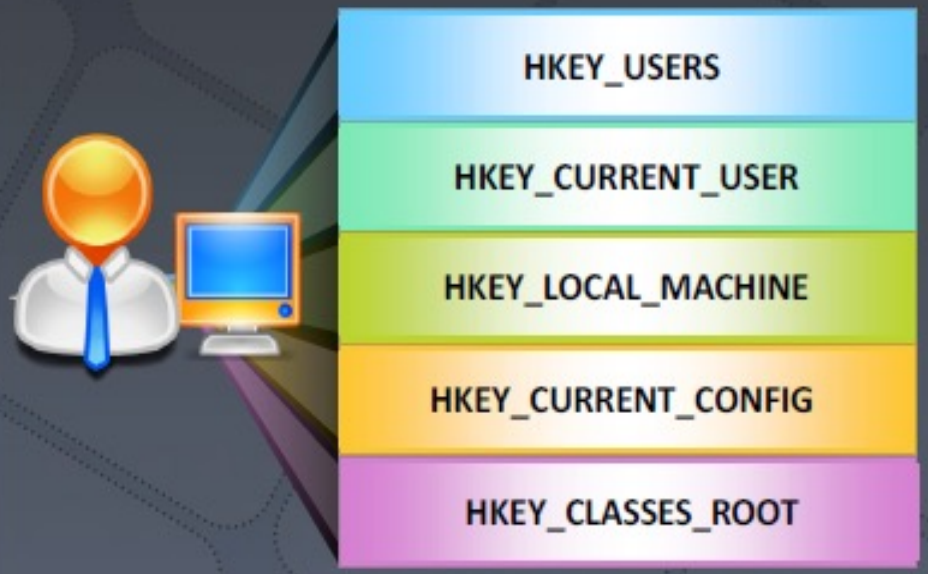
- Trước khi có Windows Registry: (DOS, Windows 3.x), thông tin Hệ điều hành chứa trong các tập tin INI.
- SYSTEM.INI - Tập tin này kiểm soát tất cả các phần cứng trên hệ thống máy tính.
  WIN.INI - Tập tin này kiểm soát tất cả các màn hình và các ứng dụng trên hệ thống.
- Các ứng dụng khác sử dụng các tập tin INI riêng được liên kết với WIN.INI.
- Từ Windows 9x/NT 3.5 đã đưa ra hệ thống Registry quản lý trên các tập tin System.dat, và User.dat.

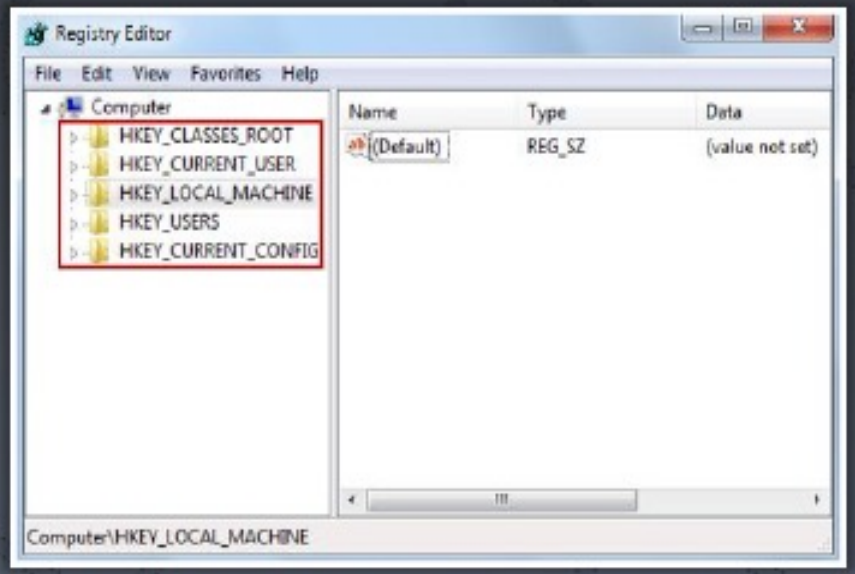
Registry – Các thông tin có thể thu thập

- Cấu hình hệ thống
- Thiết bị trên hệ thống
- Tên người dùng
- Thiết lập cá nhân và tuỳ chọn cho trình duyệt
- Hoạt động duyệt web
- Các file được mở
- Các chương trình được thực hiện
- Các mật khẩu
- ...

Inside the Registry (Cont'd)

- An Administrator can interact with the Registry through intermediate programs
- Graphical user interface (GUI) Registry editors such as Regedit.exe or Regedt32.exe are commonly used as intermediate programs
- There are five root folders in the Registry Editor:





Registry Editor view showing five root folders

Inside the Registry (Cont'd)

Hives play critical role in the function of the system:

HKEY_USERS
It contains all the actively loaded user profiles for that system

HKEY_CLASSES_ROOT
This hive contains configuration information relating to which application is used to open various files on the system

HKEY_CURRENT_USER
It is the active, loaded user profile for the currently logged -on user

HKEY_CURRENT_CONFIG
This hive contains the hardware profile information of the system used during startup

HKEY_LOCAL_MACHINE
This hive contains a vast array of configuration information for the system including hardware settings and software settings

Inside the Registry

The contents of much of the Registry visible in the Registry Editor can be found in several files

Registry Path	File path
HKEY_LOCAL_MACHINE\System	%WINDIR%\system32\config\System
HKEY_LOCAL_MACHINE\SAM	%WINDIR%\system32\config\Sam
HKEY_LOCAL_MACHINE\Security	%WINDIR%\system32\config\Security
HKEY_LOCAL_MACHINE\Software	%WINDIR%\system32\config\Software
HKEY_LOCAL_MACHINE\Hardware	Volatile hive
HKEY_USERS*User SID*	User profile (NTUSER.DAT); "Documents and settings*User* (changed to "Users*User*" on Vista)
HKEY_USERS\.Default	%WINDIR%\system32\config\default

- Registry paths are volatile and do not exist in files on the hard drive
- These hives are created during system startup and are not available when the system shuts down

Registry Structure within a Hive File

- Various components of the Registry called "cells" have a specific structure and contain specific information
- The various types of cells are:

Key cell

It contains Registry key information and includes offsets to other cells as well as the LastWrite time for the key

1

Value cell

It holds a value and its data

2

Subkey list cell

It is made up of a series of indexes pointing to key cells, these are all subkeys to the parent key cell

3

Value list cell

It is made up of a series of indexes pointing to values cells, these are all values of a common key cell

4

Security descriptor cell

It contains security descriptor information for a key cell

5

Cấu trúc cơ bản file *.reg

[Đường-dẫn-đến-Key]

“Tên Value”=kiểu dữ liệu:giá trị (nếu kiểu dữ liệu value là DWORD hoặc BINARY)

Tên Value”=”giá trị” (nếu kiểu dữ liệu value là một chuỗi)

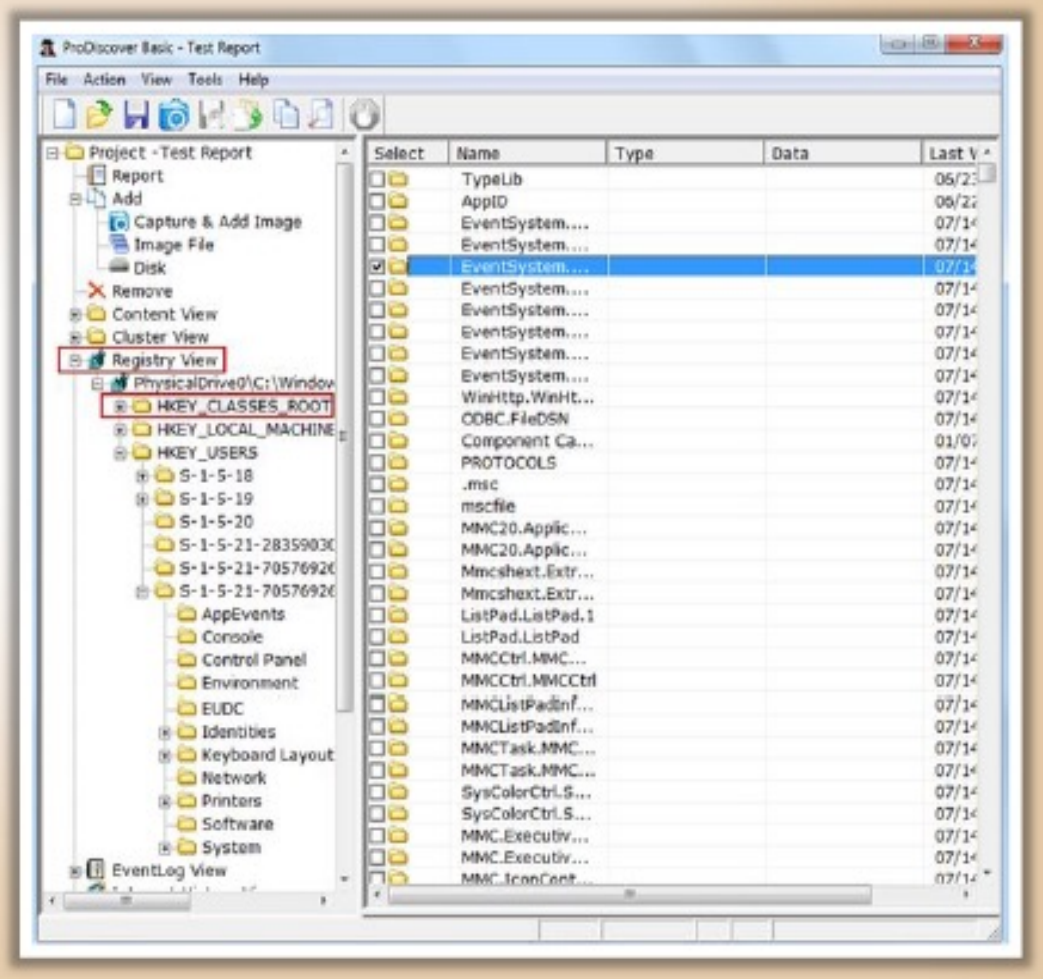
```
3
4   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Mouclass]
5
6   "ErrorControl"=dword:00000001
7
8   "Group"="Pointer Class"
9
10  "Start"=dword:00000001
11
12  [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]
13
14  "Type"=dword:00000001
15
16  "DisplayName"="Mouse Class Driver"
17
```

Các kiểu dữ liệu sử dụng trong Registry?

- **REG_BINARY:** Kiểu nhị phân 32bit.
- **REG_DWORD:** Kiểu Double Word cho phép nhập theo cơ số 16 (HEX) hoặc cơ số 10 (DECIMAL).
- **REG_EXPAND_SZ:** Kiểu chuỗi mở rộng đặc biệt. VD: "%SystemRoot%" thay cho đường dẫn thay cho đường dẫn *Windows\System32*.
- **REG_MULTI_SZ:** Kiểu chuỗi đặc biệt.
- **REG_SZ:** Kiểu chuỗi chuẩn.

Registry Analysis

- During live response, you can retrieve and analyze much of the information in the Registry, and the complete data during post-mortem investigation
- ProDiscover tool is used to access the Registry during post-mortem analysis
- Steps to obtain information using ProDiscover:
  - Load the case into ProDiscover
  - Right-click Windows directory in Content View
  - Choose Add to Registry Viewer
  - It locates files and displays them on the Registry Viewer

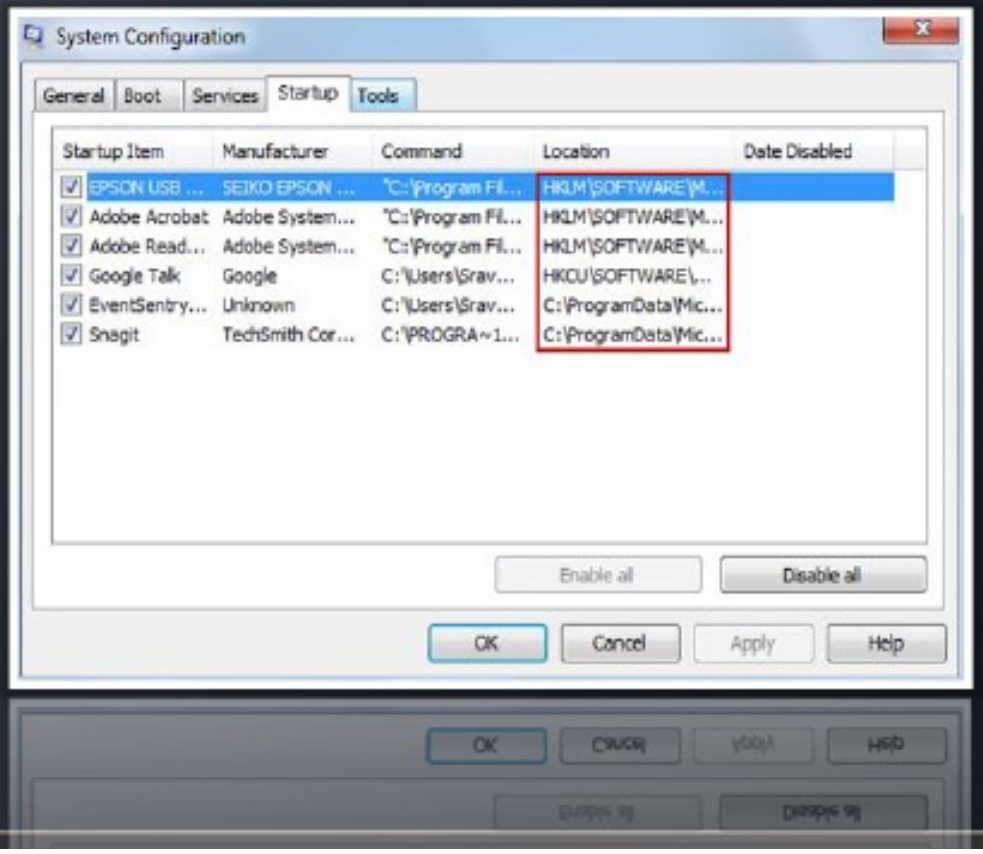


Autostart Locations

- Autostart allows applications to be launched without the user's interaction
- On a live Windows XP and 7 system, a command called `MSConfig` launches the System Configuration utility
- In the Location column the Registry keys examined are the Run key from both the `HKEY_CURRENT_USER` and `HKEY_LOCAL_MACHINE` hives

- Path for the autostart option:

  Start → Run → type msconfig → press Enter

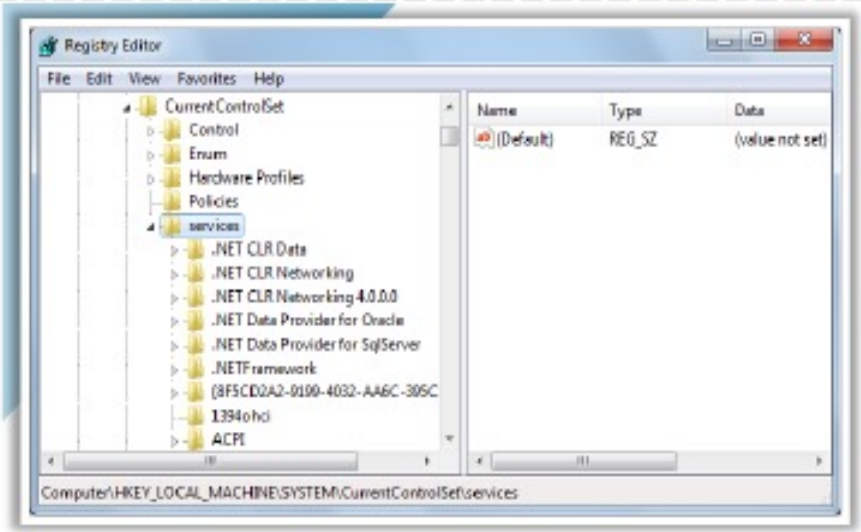


System Boot

- Malware can be launched within the autostart locations of the Registry during the system boots, even without user-intervention
- Example: Windows service at `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services`

- Intrusion analysis can be performed using ProDiscover, which locates the ControlSet marked Current and then sort the subkeys below the Services key based on their LastWrite times
  - If there is any mismatch between the LastWrite times and the actual time that the administrator launched legitimate programs, it implies that there is a possible intrusion

- When the system starts, value of the current ControlSet to be used is determined and the settings for that ControlSet are used
- Services listed in the ControlSet are scanned and services that are set to start automatically are launched



User Login

User Login

When a user logs in to a system, certain Registry keys are accessed and parsed so that listed applications can be run

The keys are listed below:

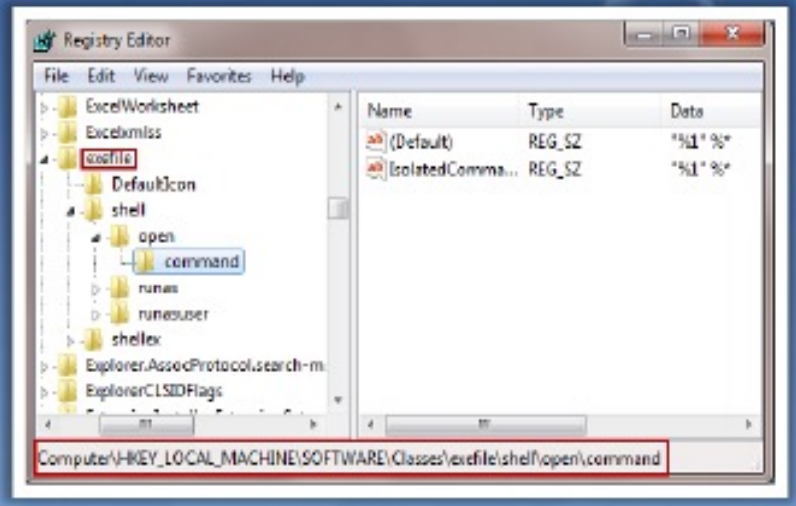
- HKEY_LOCAL_MACHINE\ Software \Microsoft\Windows\CurrentVersion\Runonce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKEY_LOCAL_MACHINE \ Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software \Microsoft\Windows\CurrentVersion\RunOnce

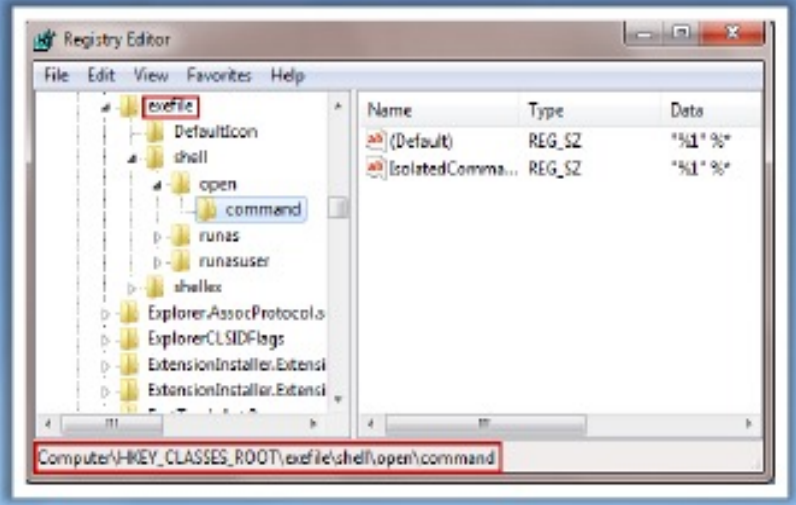
When user logs into the system, keys 1, 3, 5, and 6 are parsed, and the programs listed are run

If the system is started in safe mode, by default these Run keys are ignored

User Activity

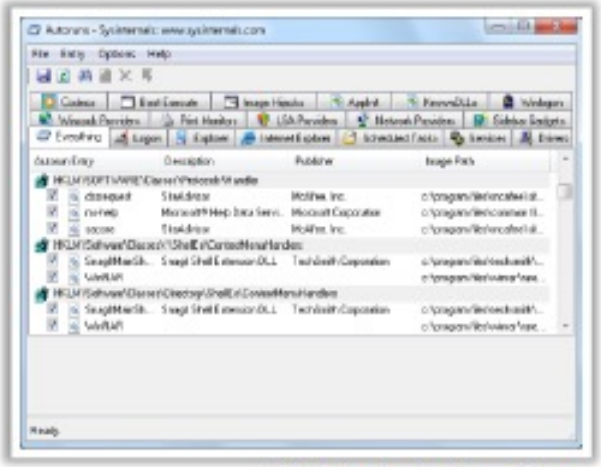
- Autostart Registry locations are accessed when the user performs any action such as opening an application like **Outlook or IE**
- Look for malware in these locations:
  - `HKEY_LOCAL_MACHINE\Software\Classes\Exefile\Shell\Open\command`
  - `HKEY_CLASSES_ROOT\Exefile\Shell\Open\Command`
- Windows provides the ability to alert external functions when certain events occur on the system, such as when a user logs on or off or when the screensaver starts
- These notifications are handled by the Registry key:
  - `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\`
- Sort the sub-keys beneath **Notify** based on their **LastWrite** times and pay attention to the entries near to the date of the suspected incident
- Check for the entries that list DLLs in the **DLLName** value that have suspicious file version information or no file version information at all





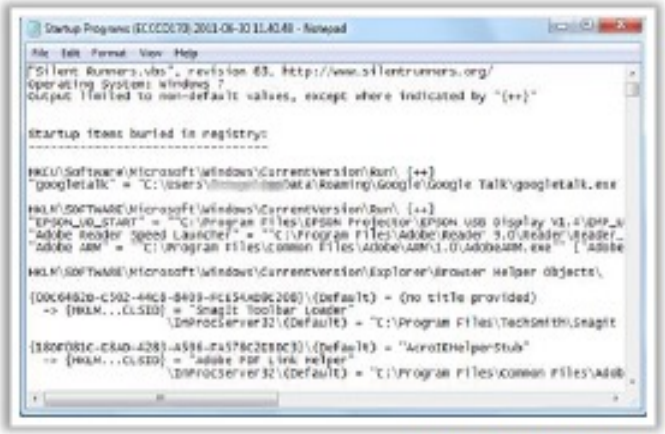
Enumerating Autostart Registry Locations

- Use AutoRuns tool to retrieve information from a number of autostart locations on a live system
- It retrieves entries from a number of Registry keys and displays the result
- It retrieves the description and publisher from the executable file pointed to by each Registry value and listed in the Image Path column



http://technet.microsoft.com

- This information assists investigators to check if anything suspicious is running in the autostart locations
- Visual Basic Script called Silent Runners is the tool for enumerating the contents of autostart registry locations



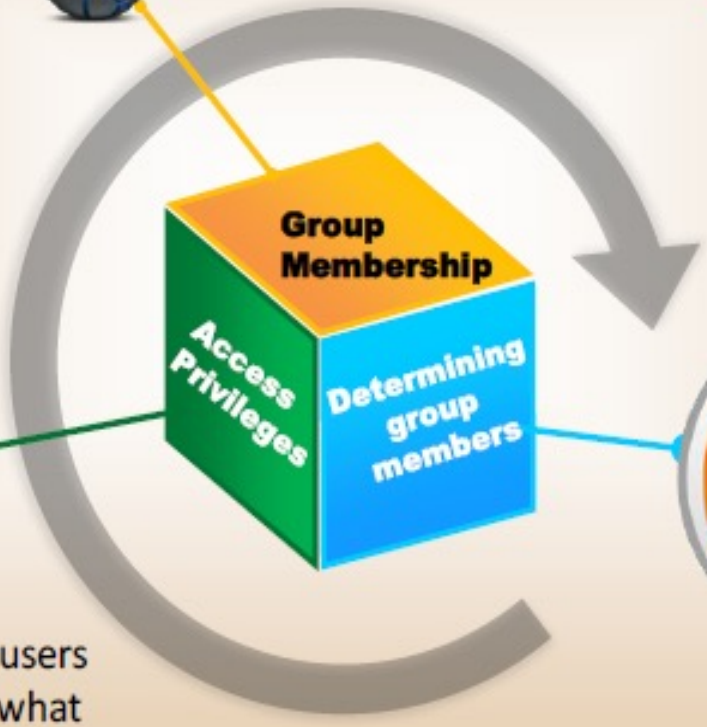
www.silentrunners.org

Finding Users (Cont'd)

1. Information about users is maintained in the Registry in the SAM hive
2. Information in the SAM hive is encoded in binary format, "sam.h" file is helpful in deciphering the structures and revealing information
3. The user's information is maintained in the F value located in the following path:
   - `SAM\SAM\Domains\Account\Users\{RID}`
4. F value within the key is a binary data type and must be parsed appropriately to extract all the information
5. Important dates are available in the contents of the binary data for the F value such as time/date stamps, represented as 64-bit FILETIME objects. The values and their locations are:
   - Bytes 8–15 represent the last login date for the account
   - Bytes 24–31 represent the date that the password was last reset
   - Bytes 32–39 represent the account expiration date
   - Bytes 40–47 represent the date of the last failed login attempt

Finding Users (Cont'd)

1. Information about group membership is maintained in:
   - `SAM\SAM\Domains\Builtin\Aliases key`

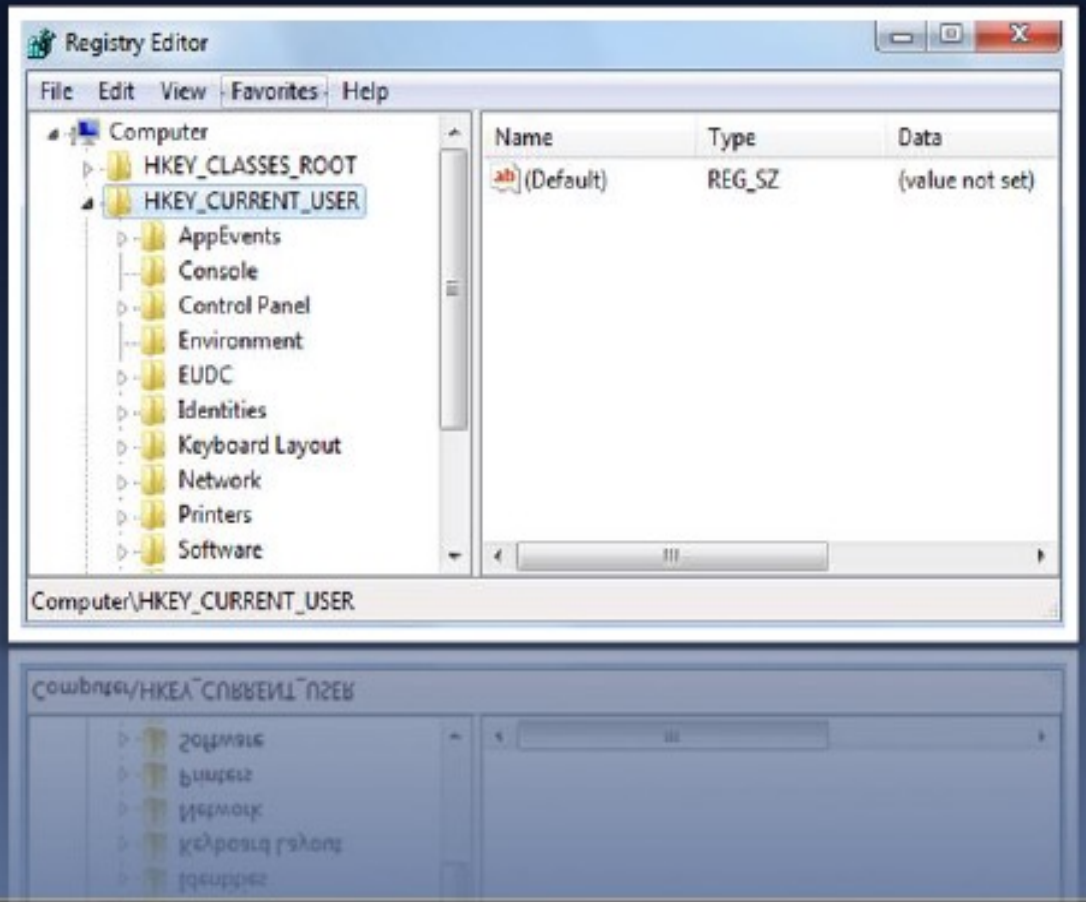


2. Each of the RID subkeys beneath the Aliases key has a C value that is a binary data type and must be parsed to determine which users are members of the group

3. It is important to know which users had access to the system and what level of access they had in order to understand the context of a case

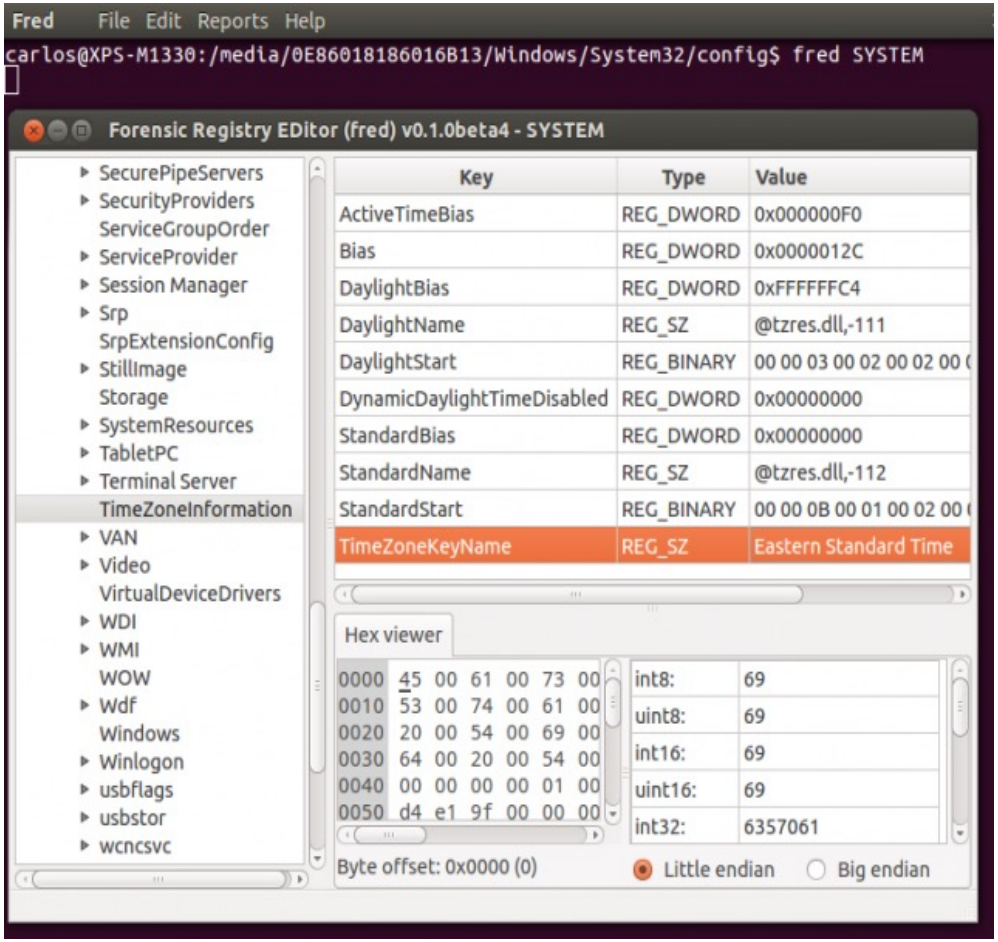
Tracking User Activity

- Registry keys that track user's activities can be found in the `NTUSER.DAT` file
- When a user performs a particular action, the registry key's `Lastwrite` time is updated
- These registry keys track the user's activity and add or **modify timestamp information** associated with the Registry values, this timestamp information is maintained in the value data
- Majority of the user's activities are recorded in the `HKEY_CURRENT_USER hive`



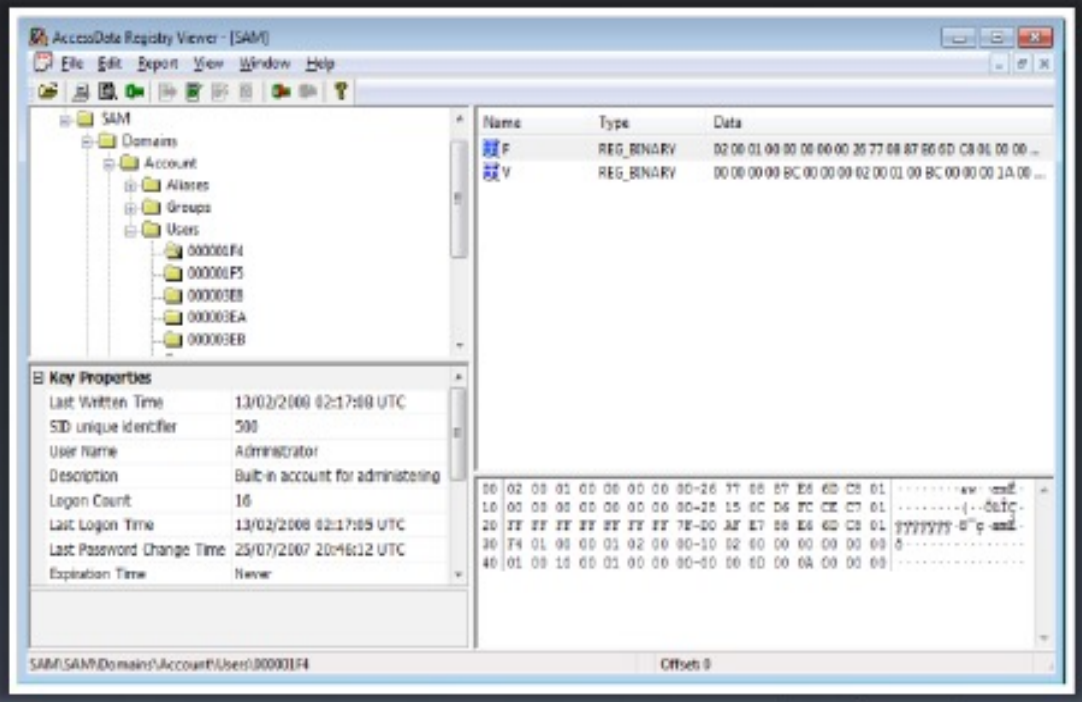
Forensic Registry EDitor

- Được cung cấp tại: https://www.pinguin.lu/fred
- Là phần mềm mã nguồn mở được viết bởi Daniel Gillen trên Linux, Windows cho phép xem và tìm kiếm chứng cứ số trên các vùng ẩn chứa Registry



Registry Viewer Tool: Registry Viewer

- AccessData Registry Viewer allows you to view the contents of **Windows operating system registries**
- It provides access to a **registry's protected storage**, which contains passwords, usernames, and other information not accessible in Windows Registry Editor



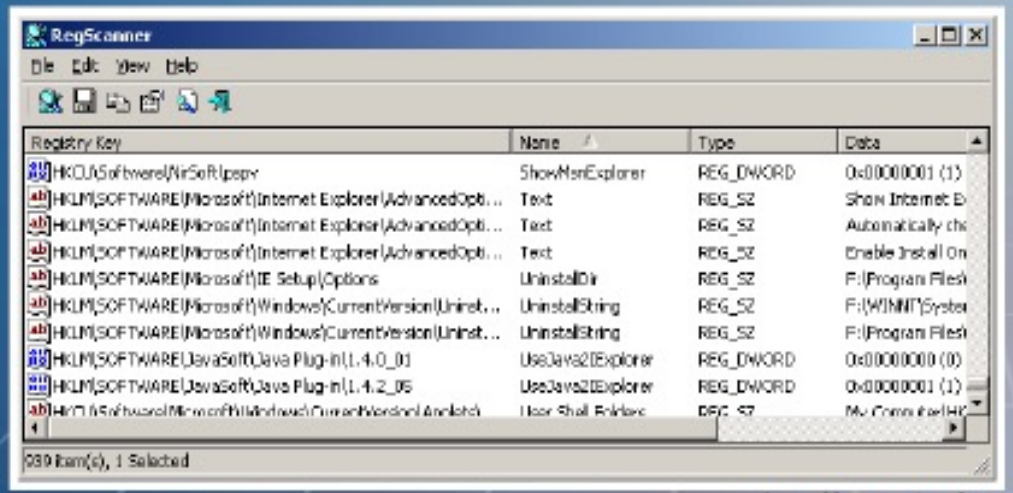
http://accessdata.com

Registry Viewer Tool: RegScanner

- RegScanner is a small utility that allows you to scan the Registry, find the desired Registry values that match the specified search criteria, and display them in one list

  Features

  - It displays the entire search result at once, so you do not have to press F3 in order to find the next value
  - In addition to the standard string search, RegScanner can also find Registry values by data length, value type (REG_SZ, REG_DWORD etc.), and by modified date of the key
  - It finds a unicode string located inside a binary value
  - It allows you to make a case sensitive search



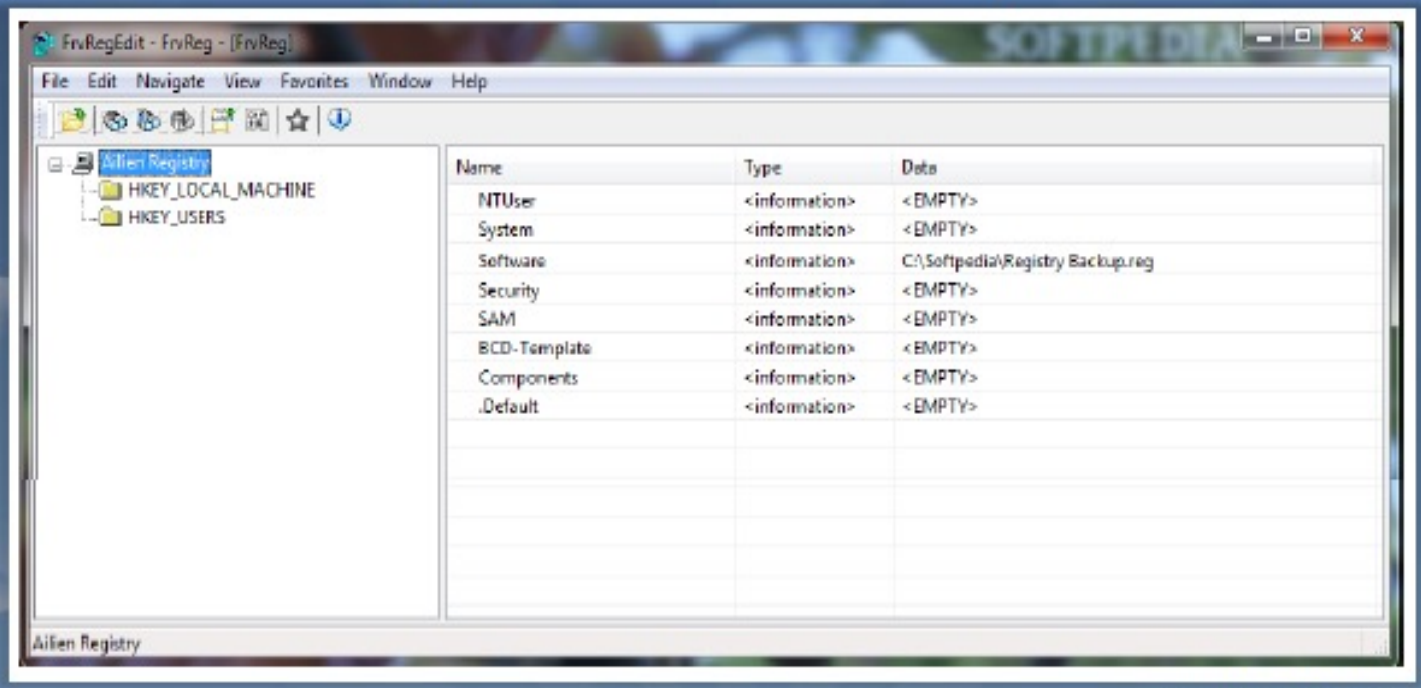
http://www.nirsoft.net

Registry Viewer Tool: Alien Registry Viewer

Alien Registry Viewer is similar to the **RegEdit application** included with Windows, but unlike RegEdit, it works with **standalone registry files**

It allows you to **explore** registry files, **search** for specific key names and values, **export** registry data into a `.REG` file and **bookmark** registry keys as favorites

It works with registry files copied from other computers



http://lastbit.com

RECOVERYING DELETED FILES & DELETED PARTITIONS

Deleting Files

File deletion is a way of removing a file from a computer's file system

The reasons for deleting files are:

- Freeing the disk space
- Removing duplicate or unnecessary data to avoid confusion
- Making sensitive information unavailable to others

Users can delete files in several different ways. Files are moved to the **Recycle Bin** in the following ways:

- By right-clicking on a file and selecting delete from the menu
- Selecting the file and pressing the delete key
- Selecting delete from the side menu in Windows XP
- From a context menu command or some other function in a software application (usually configurable)
- By a computer virus
- By dragging and dropping a file into the Recycle Bin icon

What Happens When a File is Deleted in Windows?

When a file is deleted, the operating system marks the file's name in the MFT with a special character that indicates that the file has been deleted

The first letter of a file name is replaced by a hex byte code E5h

Corresponding clusters in FAT are marked as unused

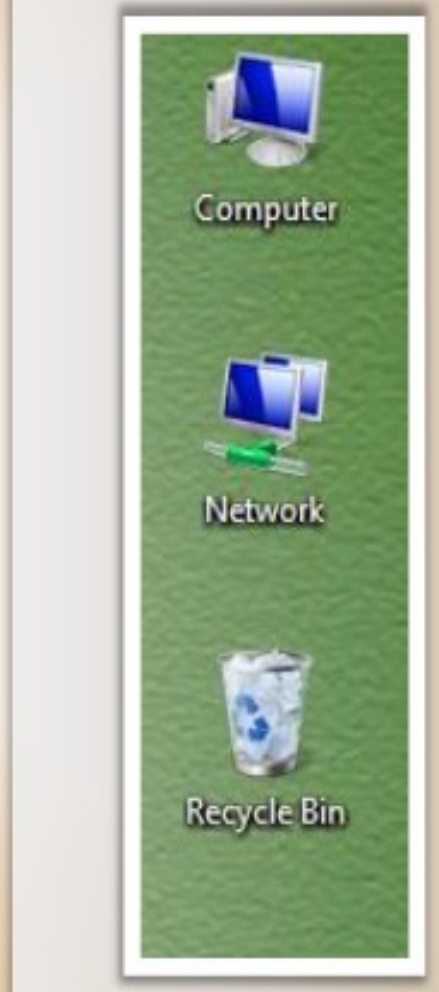
Index field in MFT is marked with a special code in NTFS

The computer now looks at the clusters occupied by that file as being empty and therefore avails space to store a new file

The deleted file can be recovered if the space is not allocated to any other file

Recycle Bin in Windows (Cont'd)

- You can retrieve files from the Recycle Bin that have been deleted
- When a file is deleted, it is sent to the Recycle Bin, where it remains until the Recycle Bin is emptied
- The Restore all items option of the Recycle Bin properties, allows you to restore the data to its original location
- After the Recycle Bin is emptied, the data still remains in its original location on the hard drive for a period of time
- The data will disappear only when the operating system over-writes the original location of the file
- Data deleted from removable media such as floppy disks is not stored in the Recycle Bin



Storage Locations of Recycle Bin in FAT and NTFS Systems

Each drive contains a folder to store deleted files; deleted items are stored at Drive:\$Recycle.Bin folder in Windows Vista and later versions of Windows

Deleted files in older FAT file system (Windows 98 and prior) are stored in Drive:\RECYCLED whereas in NTFS file system (Windows 2000, XP, NT) these are stored in Drive:\RECYCLER folder

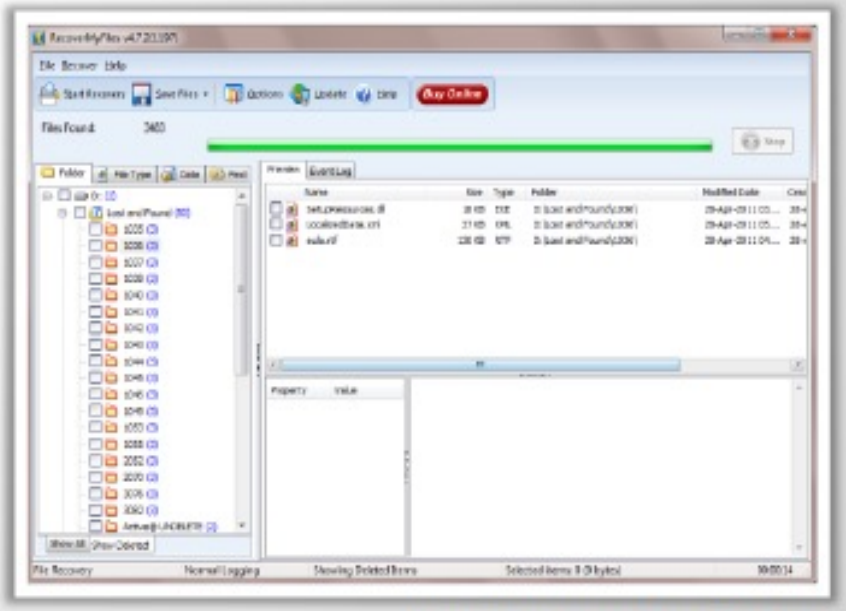
All recycled files on a FAT system are dumped into a single C:\RECYCLED directory, whereas in an NTFS system, these are categorized into directories named as C:\RECYCLER\S-.... (prior to Windows Vista) and C:\$Recycle.Bin\S-.... based on the user's SID

There is no size limit for Recycle Bin in Vista and later versions of the Windows whereas in older versions it was limited to a maximum of 3.99 GB; items larger than the storage capacity of the Recycle Bin cannot be stored in the Recycle Bin

Các công cụ phục hồi Files

Recover My Files

Recover My Files data recovery software recovers deleted files emptied from the Windows Recycle Bin, or lost due to the format or corruption of a hard drive, virus or Trojan infection, unexpected system shutdown, or software failure

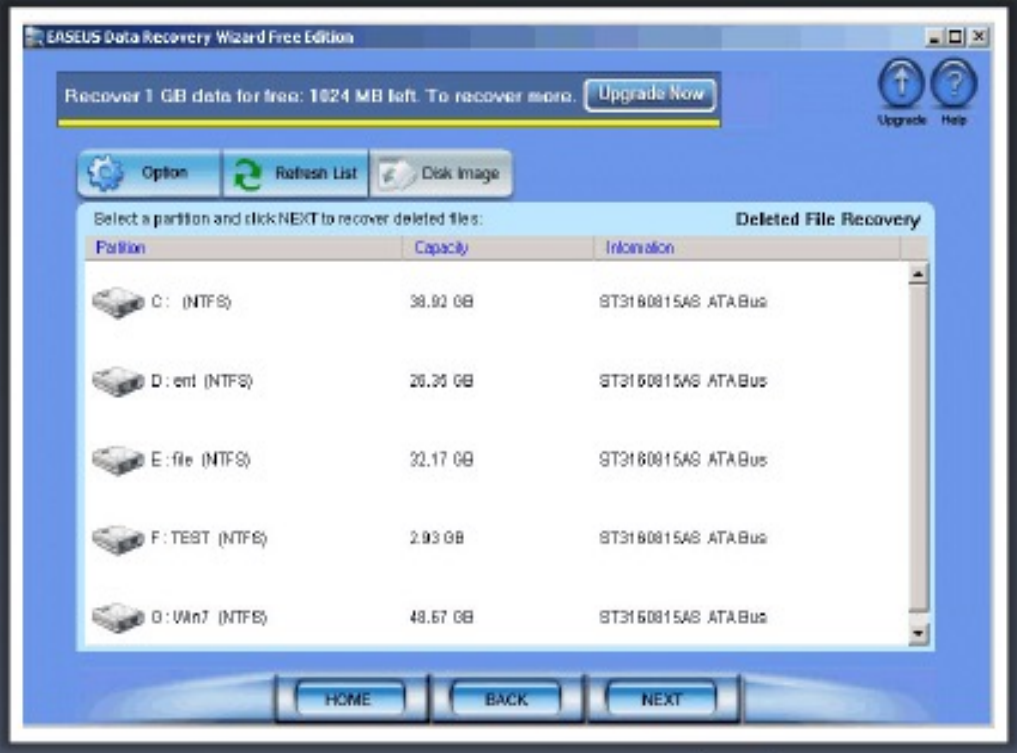


http://www.recovermyfiles.com

EASEUS Data Recovery Wizard

EASEUS Data Recovery Wizard provides a comprehensive data recovery solution for computer users to **recover lost data** due to partition loss or damage, software crash, virus infection, and unexpected shutdown

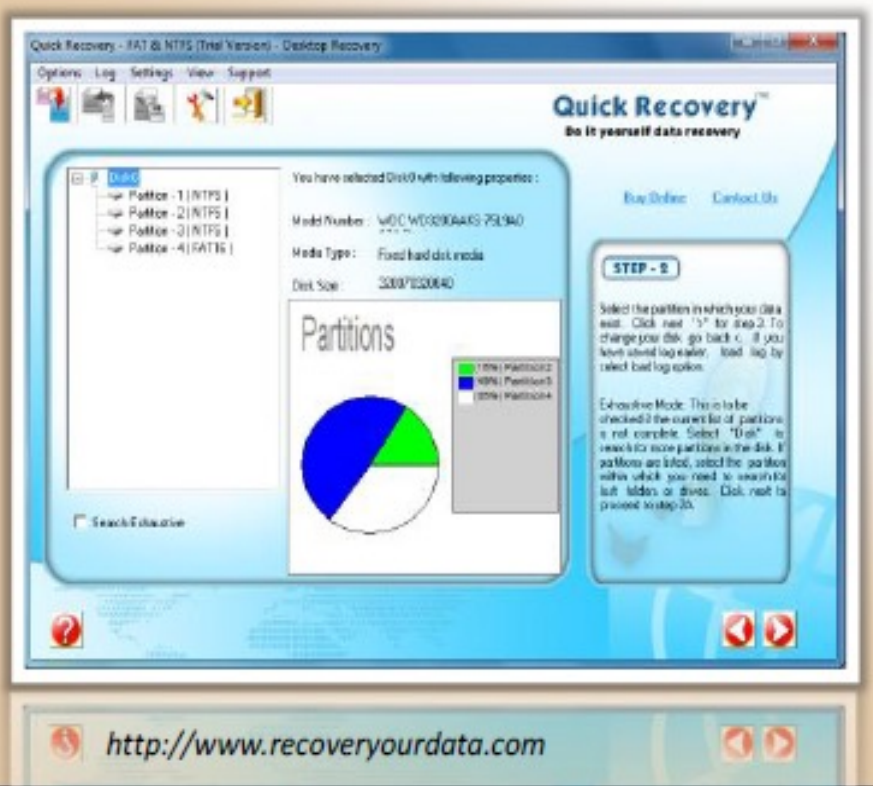
- Recover deleted or lost files emptied from the Recycle Bin
- File recovery after accidental format, even if you have reinstalled Windows
- Disk recovery after a hard disk crash
- Recover office documents, photos, images, videos, music, email, etc.
- Recover from hard drive, USB drive, memory card, memory stick, camera card, zip, floppy disk, or other storage media

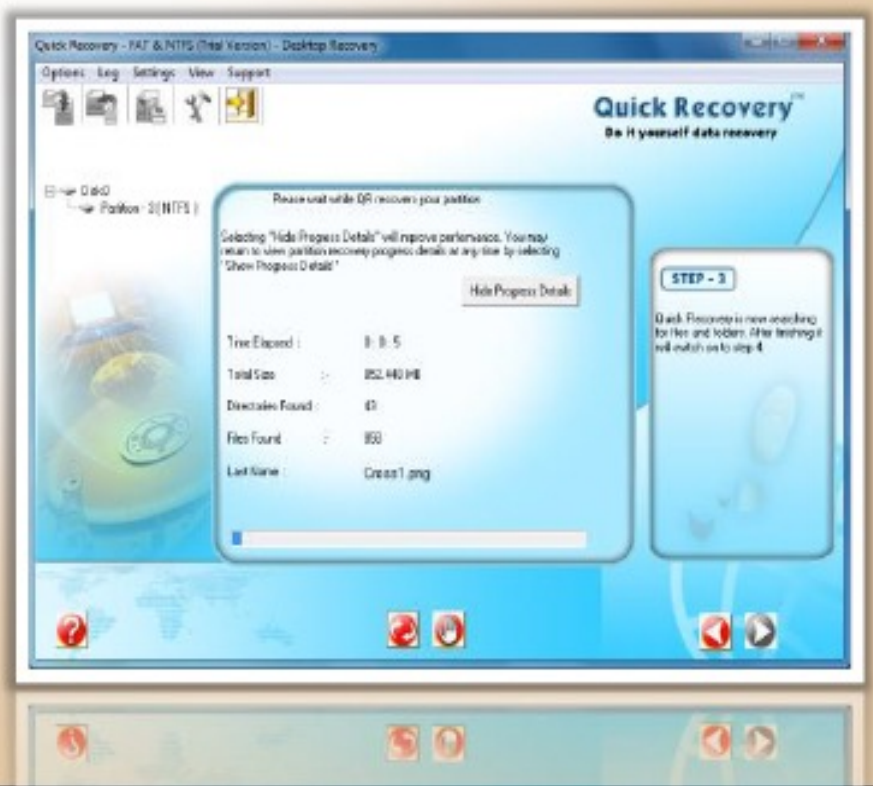


http://www.easeus.com

Quick Recovery

- Quick Recovery data recovery software recovers files from inaccessible, lost, missing, damaged or formatted drives





Tools to Recover Deleted Files

Total Recall
http://www.totalrecall.com

PC Tools File Recover
http://www.pctools.com

Advanced Disk Recovery
http://www.systweak.com

Data Rescue PC
http://www.prosofteng.com

Windows Data Recovery Software
http://www.diskdoctors.net

Smart Undelete
http://www.recoverdeletedfilestool.com

R-Studio
http://www.data-recovery-software.net

FileRestore Professional
http://www.pcrecovery.com

Tools to Recover Deleted Files

Deleted File Recovery Software
http://www.deletedfilerecovery.org

UndeletePlus
http://undeleteplus.com

DDR Professional Recovery Software
http://www.recoverybull.com

Search and Recover
http://www.iolo.com

Data Recovery Pro
http://www.paretologic.com

File Scavenger
http://www.quetek.com

GetDataBack
http://www.runtime.org

Filesaver
http://www.file-saver.com

Tools to Recover Deleted Files

Virtual Lab
http://www.binarybiz.com

Recover4all Professional
http://www.recover4all.com

Active@ UNDELETE
http://www.active-undelete.com

eData Unerase
http://www.octanesoft.com

Win Undelete
http://www.winundelete.com

Active@ File Recovery
http://www.file-recovery.net

R-Undelete
http://www.r-undelete.com

FinalRecovery
http://www.finalrecovery.com

Disk Partitions

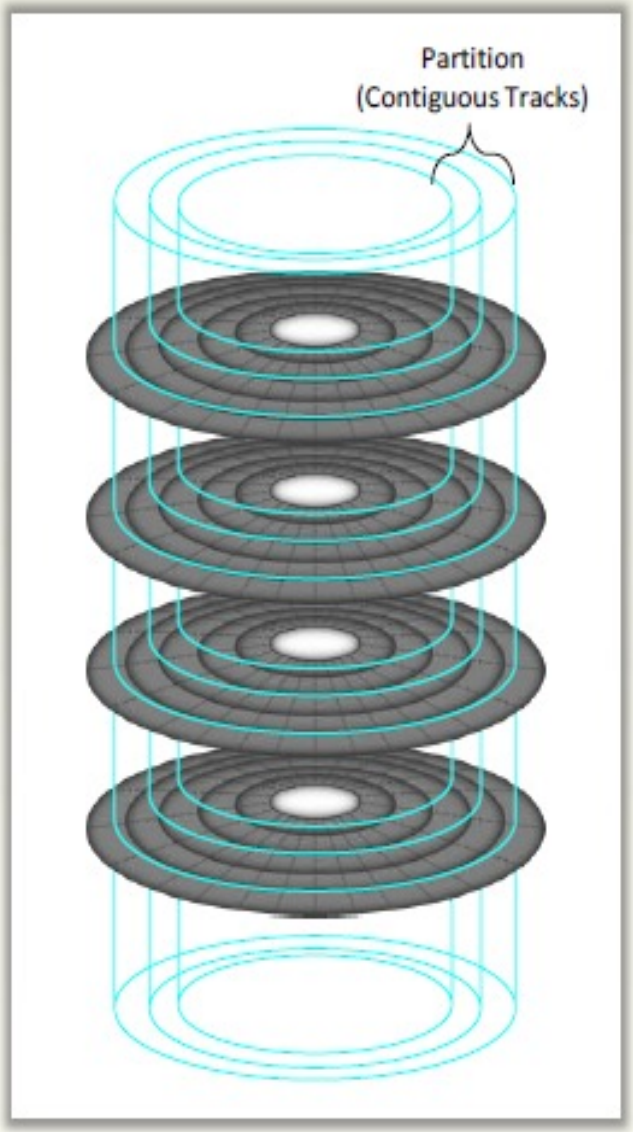
- Hard disk drive partitioning is the creation of logical divisions upon a hard disk that allows one to apply operating system-specific logical formatting

Primary Partition

- It is the drive that holds the information regarding the operating system, system area, and other information required for booting
- In MS-DOS and earlier versions of Microsoft Windows systems, the first partition (C:) must be a "primary partition"

Extended Partition

- It is the logical drive that holds the information regarding the data and files that are stored in the disk



Disk Partition

- Disk partition is the space defined on a hard drive to store data (such as files and documents) and for the system to store all files needed to boot Windows
- Disk partitions have names; generally a single letter and a colon (C:)
- Hard drives are partitioned to:
  - Separate the operating system from data files
  - Run multiple operating systems from the same disk
  - Make partitions independent. Other partitions will not be broken with one partition destroyed
  - Logically organize data
  - Ensure computers run fast

Deletion of Partition

System users may **accidentally delete useful partitions**:

- Accidentally delete partitions in Partition Manager/Disk Management
- Accidentally delete partitions in the progress of Windows Installation

What happens when a **partition is deleted**?

- All data on that deleted partition or logical drive is lost
- Deleting a partition on a dynamic disk can delete all the dynamic volumes on the disk, thus leaving the disk in a corrupt state

- When a hard drive partition is deleted, it does not mean deleting everything, just the partition that marks how the partition is setup
- Deleted partition can be recovered as it is not originally deleted, by using a software that reestablishes those parameters

Recovery of the Deleted Partition (Cont'd)

- Recovery of the deleted partition is the process by which the investigator evaluates and extracts the deleted partitions

- Recovery helps in recovering the partitions that are lost accidentally, or due to virus, software malfunction, or even sabotage

- Partition Recovery utility helps in recovering all important data lost after accidentally losing a partition

Recovery of the Deleted Partition (Cont'd)

Method 1 | Method 2 | Method 3

- Restart the system with a Windows install CD in the system
- Hit the respective keys listed on the screen to go to the BIOS
- In the BIOS, check for the menu "boot priority" or "boot order" to set the CD as the first boot device
- Restart the system and let Windows start the installation process
- Accept all the choices to let the Windows install, but opt "Repair" rather than "Install"
- Now a DOS-like screen appears, type "fixboot" and press "Enter"
- Restart the system and check if the deleted partition is restored

Recovery of the Deleted Partition (Cont'd)

Method 1 | **Method 2** | Method 3

- Shut down the system and take the hard drive out
- Install the hard drive as a slave to another drive on a working system
- Now attempt to recover the deleted partition on the original system

Note: This method is not the safest way to avoid losing data

Recovery of the Deleted Partition

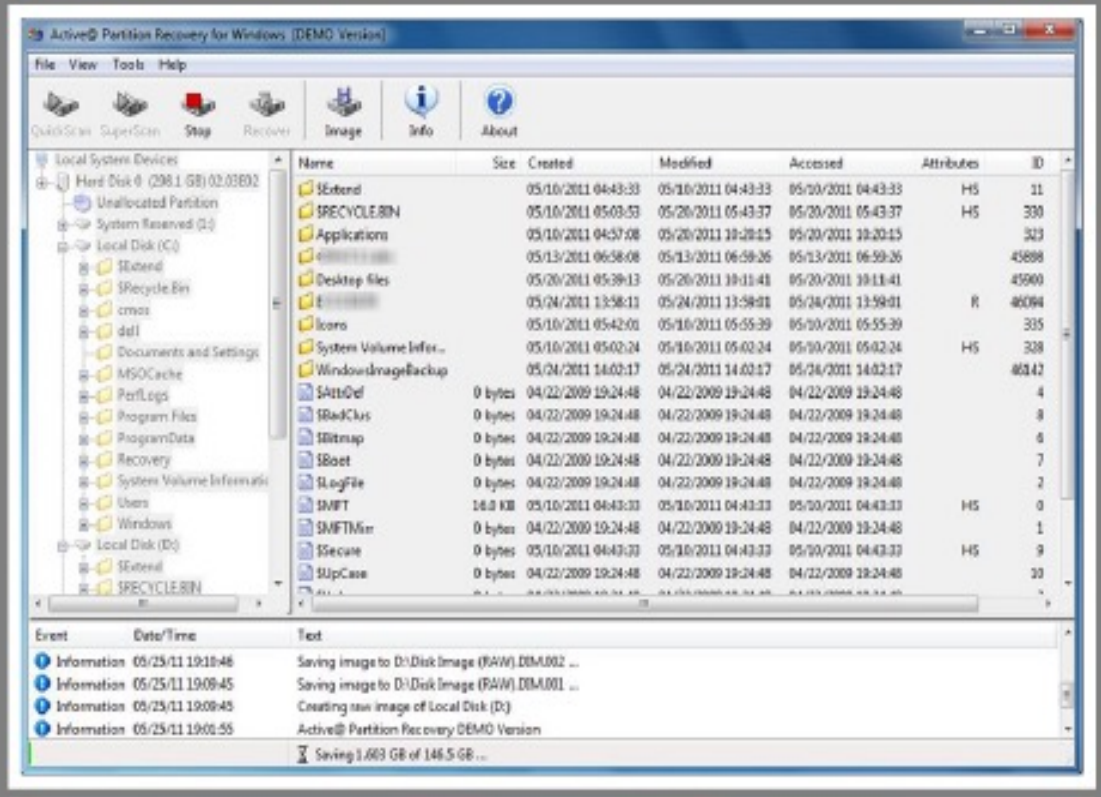
Method 1 | Method 2 | **Method 3**

- Use third-party partition recovery software to recover the drive
- Run the program and follow the instructions to recover the partition
- Once restored, copy the files off of the drive that had the partition recovered onto another drive, this prevents corruption of files
- Some of the best partition recovery software includes:

- Active@ Partition Recovery for Windows
- Acronis Recovery Expert
- DiskInternals Partition Recovery
- NTFS Partition Data Recovery
- GetDataBack
- EASEUS Partition Recovery
- Advanced Disk Recovery
- Power Data Recovery

Active@ Partition Recovery for Windows

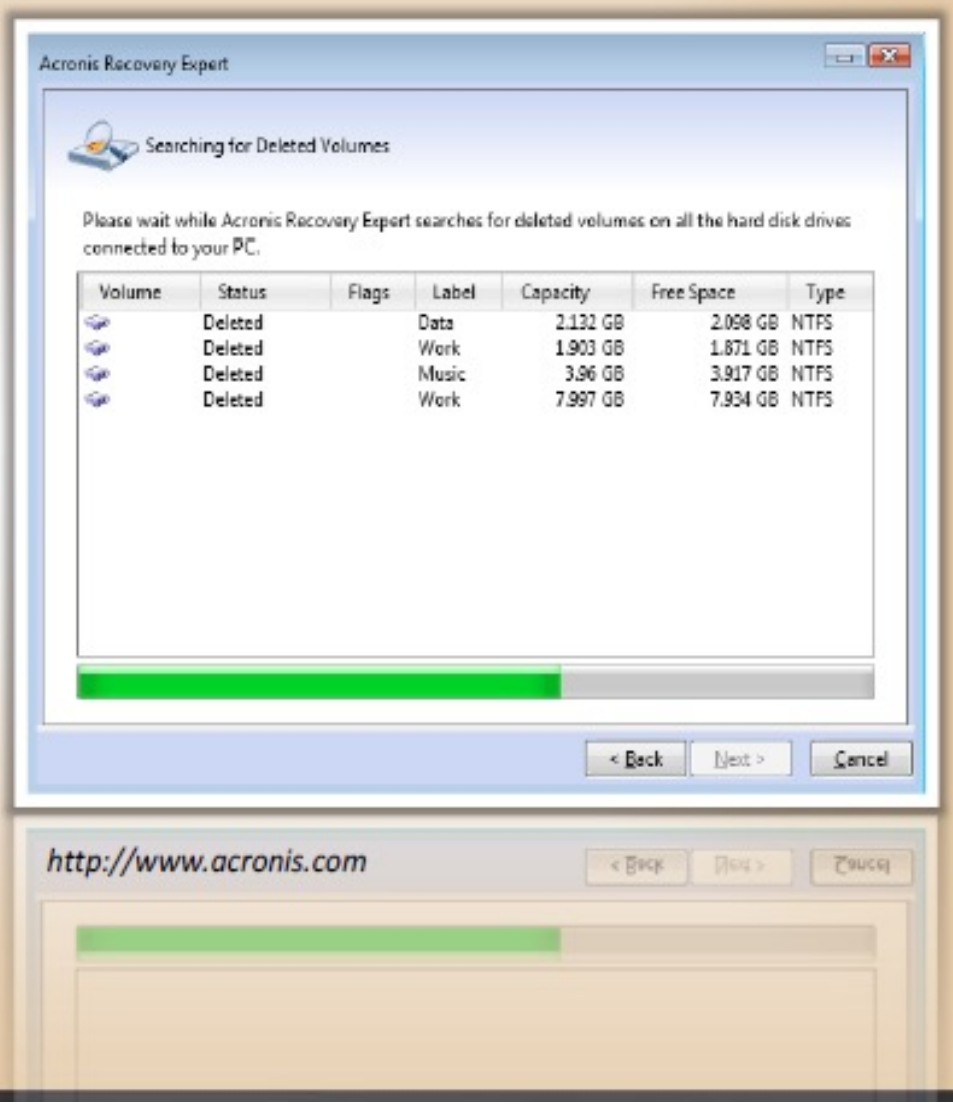
Active@ Partition Recovery for Windows recovers deleted or damaged partitions located on data volumes, attached HDDs, as well as on the external USB drives and Memory Cards



http://www.partition-recovery.com

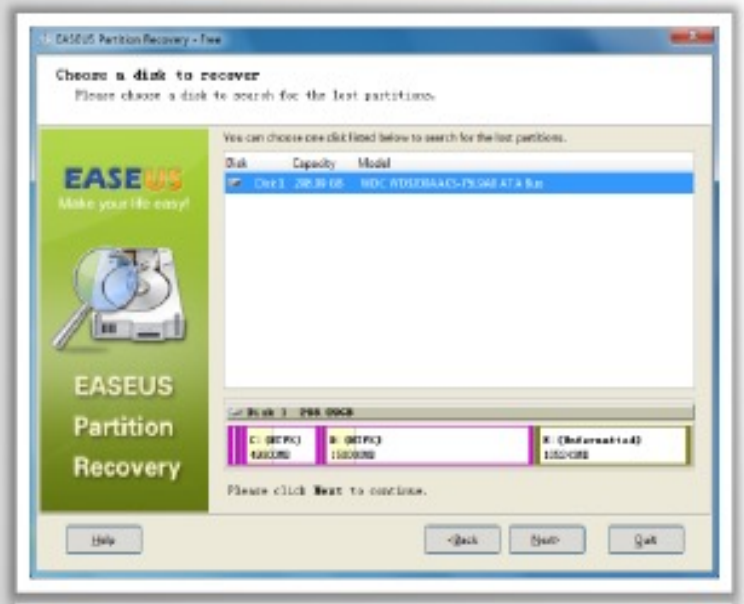
Acronis Recovery Expert

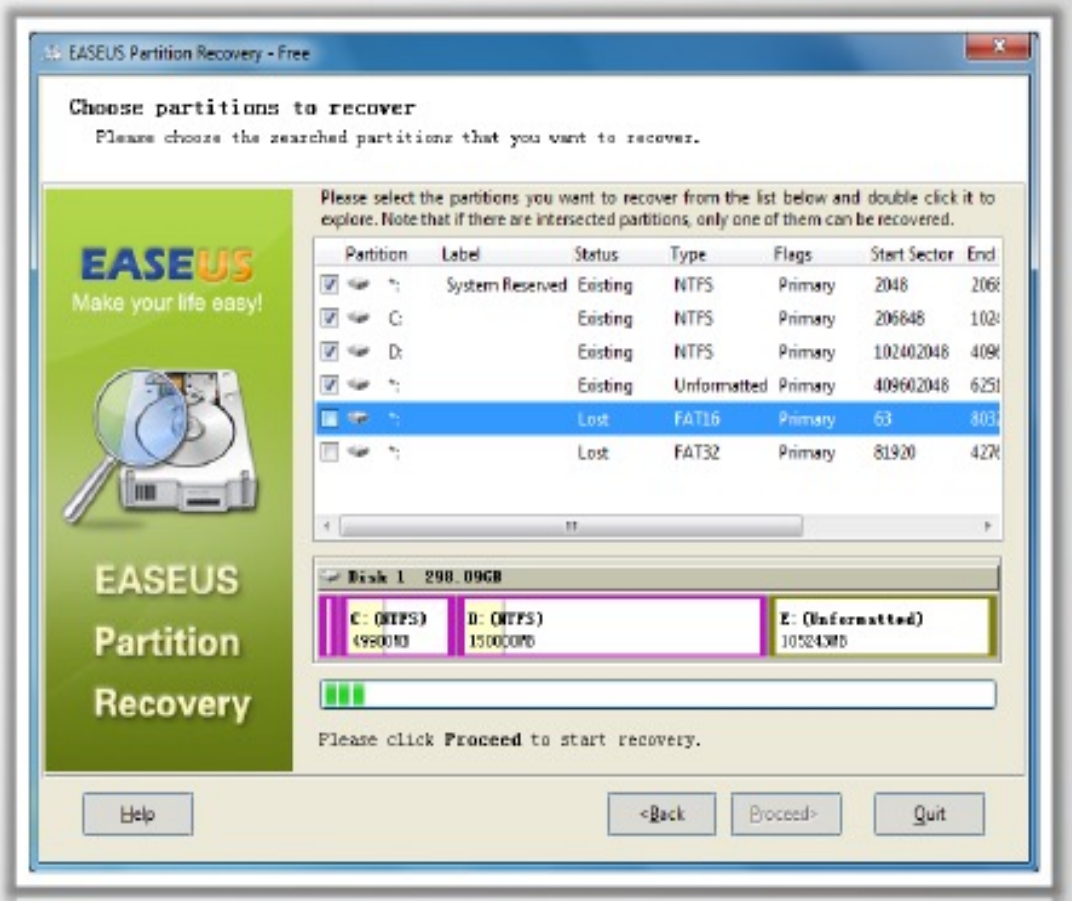
- Acronis Recovery Expert is a data partition and disk recovery tool that repairs the results of a personal error, hardware or software failure, virus attack or hacker's intrusive destruction. It recovers deleted or lost partitions
- Features:
  - Recovers deleted or lost partitions on hard drive
  - Boots from bootable CDs, DVDs, USB flash drives or USB hard disk drives

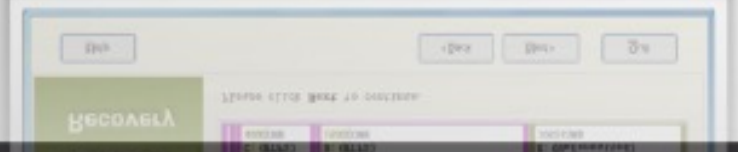


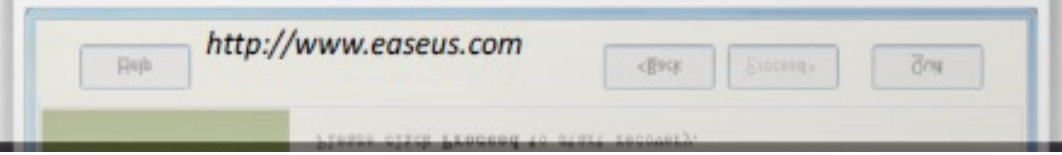
EASEUS Partition Recovery

EASEUS Partition Recovery is a partition recovery software for hard disk. It is designed to recover the deleted or lost partitions on a hard drive









Tools to Recover Deleted Partitions

Handy Recovery
http://www.handyrecovery.com

Power Data Recovery
http://www.mt-solution.ca

TestDisk for Windows
http://www.cgsecurity.org

Quick Recovery for Mac
http://www.data-recovery-software.in

Stellar Phoenix Windows Data Recovery
http://www.stellarinfo.com

Partition Find & Mount
http://findandmount.com

ARAX Disk Doctor
http://www.disk-doctor.com

Advance Data Recovery Software Tools
http://www.recoverdatatools.com

Tools to Recover Deleted Partitions

TestDisk for MAC
http://www.cgsecurity.org

Kernel for FAT and NTFS – Windows Disk Recovery
http://www.nucleustechnologies.com

Disk Drill
http://www.cleverfiles.com

Stellar Phoenix Mac Data Recovery
http://www.stellarinfo.com

ZAR Windows Data Recovery
http://www.z-a-recovery.com

AppleXsoft File Recovery for Mac
http://www.applexsoft.com

Quick Recovery for FAT & NTFS
http://www.unistal.com

TestDisk for Linux
http://www.cgsecurity.org

References

- CHFIv8 Slides: Module 8, 9, 10

Q&A

TRƯỜNG ĐH CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH & TRUYỀN THÔNG

Digital Forensics
Pháp chứng Kỹ thuật số

#5: Windows Forensics & File Recovery

Spring 2022

ThS. Lê Đức Thịnh
thinhld@uit.edu.vn