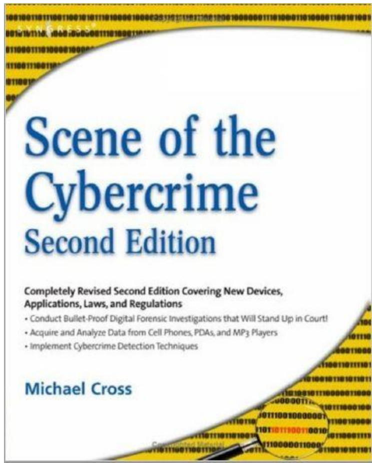
Chapter – 7

“Acquiring, Duplicating and Recovering Deleted Files ”

Book Reference: Shinder L. D., Cross M., Scene of the Cybercrime, Syngress.



SYNGRESS

Scene of the Cybercrime
Second Edition

Completely Revised Second Edition Covering New Devices, Applications, Laws, and Regulations

- Conduct Bullet-Proof Digital Forensic Investigations that Will Stand Up in Court!
- Acquire and Analyze Data from Cell Phones, PDAs, and MP3 Players
- Implement Cybercrime Detection Techniques

Michael Cross

Outline

- Recovering Deleted Files and Deleted Partitions
- Recovering "Deleted" and "Erased" Data
- Data Recovery in Linux
- Recovering Deleted Files
- Recovering Deleted Partitions
- Data Acquisition and Duplication
- Data Acquisition Tools
- Recovering Data from Backups
- Finding Hidden Data
- Locating Forgotten Evidence
- Defeating Data Recovery Techniques.

Introduction

- Data needs to be acquired, before it can be analyzed for forensic evidence.

- This means the data needs to be duplicated so that the person performing the analysis can extract vital information from it without modification of the original data.

- This can demand using any number of tools to duplicate the data so that an exact, sector-by-sector mirror image of the disk is generated. This enables the forensic analyst to view any data that ***is hidden, fragmented, or deleted***.

- A file may be deleted
  - on purpose or by accident,
  - as a normal process of an application, or
  - as the result of a virus, intrusion, or malicious software. For example:
    - **Chernobyl virus**, delete files automatically and erase the core system code
    - **Wiper malware** acts like ransomware but in reality is a destructive form of malware that erases data from victims' systems, even if they make ransom payments.

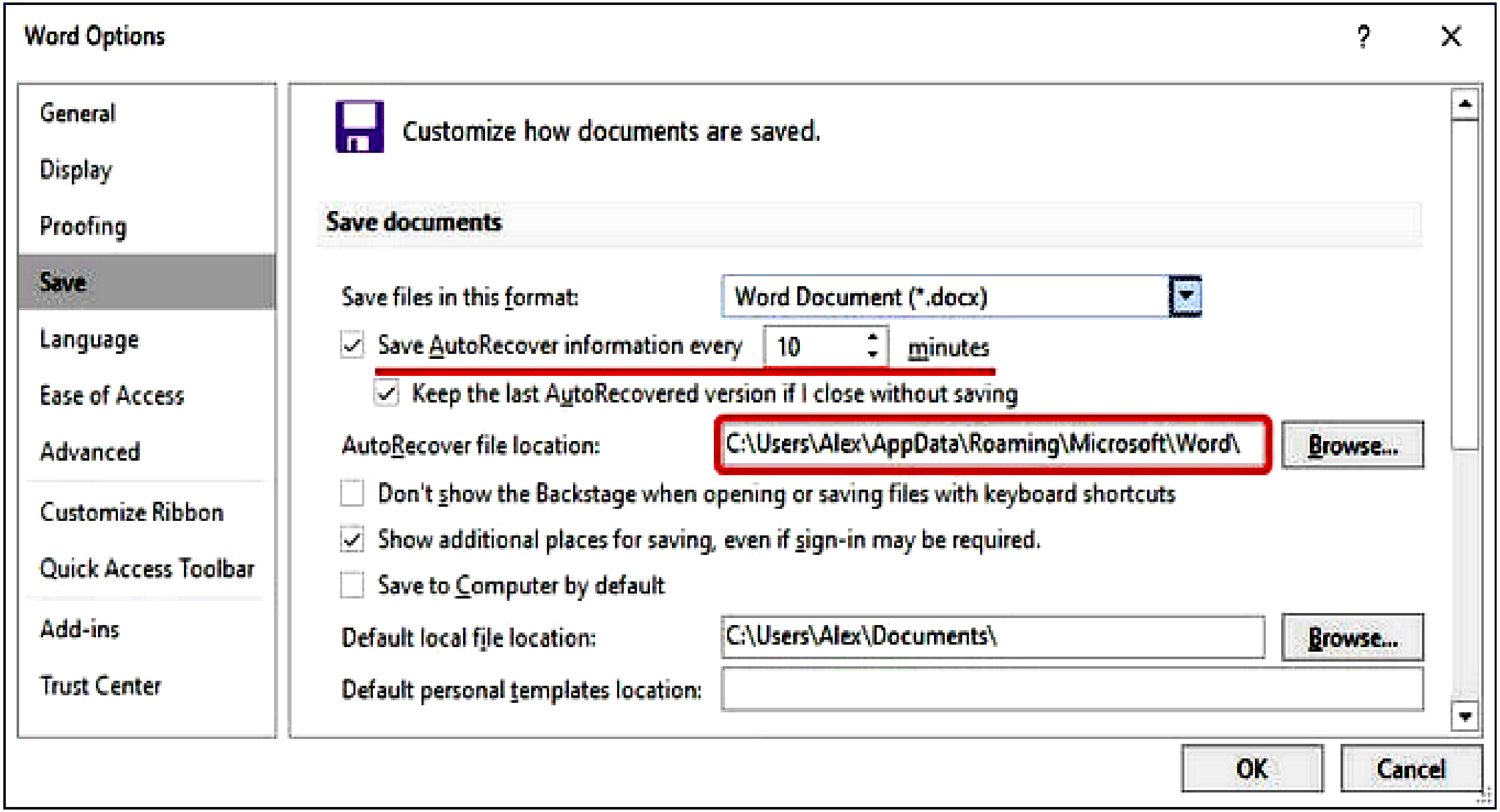
- An entire partition may also be lost, causing everything on a volume to appear unrecoverable.

- However, various tools may be used to recover the deleted data from a hard disk or other storage media.

- The files may be corrupted or damaged (This may happen if the hardware or the software of a system accidentally alters the configuration of the file), hence additional software may be needed to repair the file.

- Regardless of the cause; there are many ways to recover data which at first sight appear to be lost.

Within this window, you can find the AutoRecover location for where your files are being saved to.



Word Options

Customize how documents are saved.

Save documents

Save files in this format: Word Document (*.docx)

☑ Save AutoRecover information every 10 minutes

☑ Keep the last AutoRecovered version if I close without saving

AutoRecover file location: C:\Users\Alex\AppData\Roaming\Microsoft\Word\

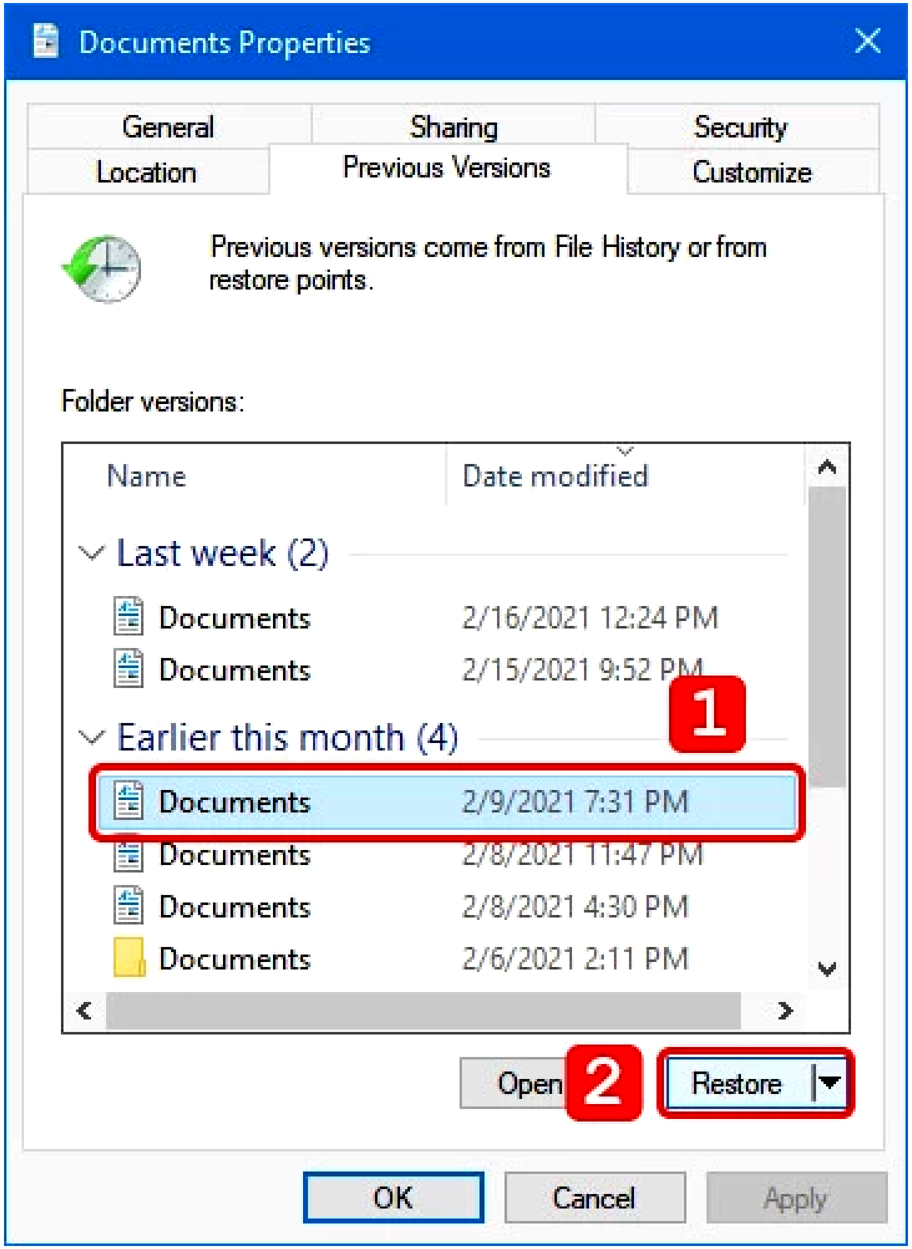
□ Don't show the Backstage when opening or saving files with keyboard shortcuts

☑ Show additional places for saving, even if sign-in may be required.

□ Save to Computer by default

Default local file location: C:\Users\Alex\Documents\

Default personal templates location:



Previous versions come from File History or from restore points.

Folder versions:

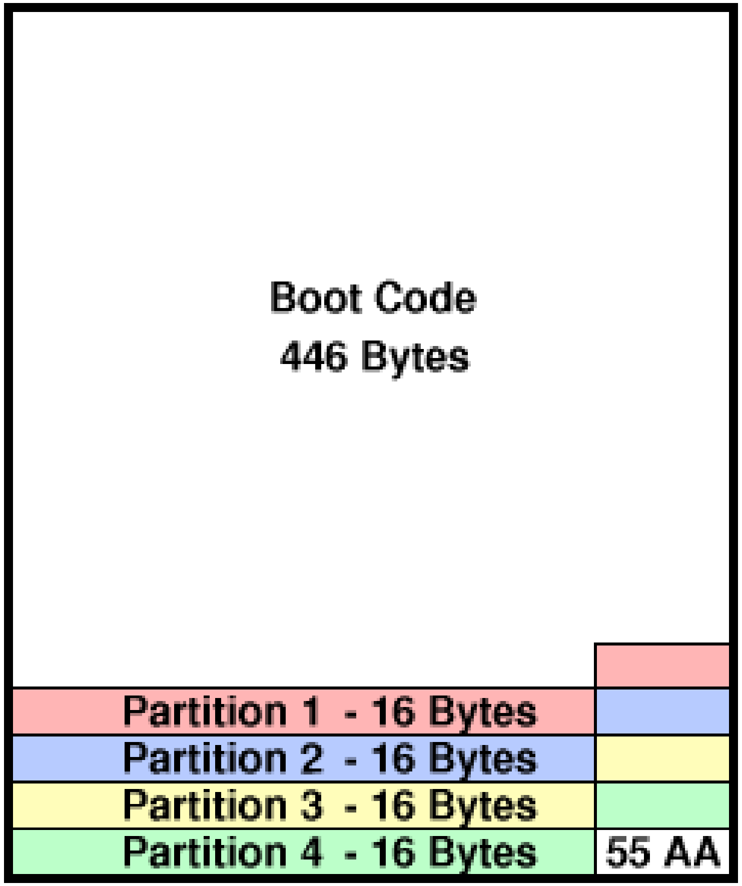
Name	Date modified
Last week (2)	
Documents	2/16/2021 12:24 PM
Documents	2/15/2021 9:52 PM
Earlier this month (4)	
Documents	2/9/2021 7:31 PM
Documents	2/8/2021 11:47 PM
Documents	2/8/2021 4:30 PM
Documents	2/6/2021 2:11 PM

Recovering Deleted Files and Deleted Partitions

- In the organization, there is probably an inventory of assets.
- It may be as simple as a typed out list for insurance purposes, or a database containing records of every desk, computer, printer, and every other asset owned by the organization.
- Similarly on computer, a table of records is used to maintain information about the files saved on your hard disk.
- Simple deleting a file on your hard disk doesn’t necessarily make the data disappear.
- Files are stored on hard disks and other media in the form of Clusters.
- *Clusters are two or* more sectors of a hard disk, and are the smallest unit of disk space that can be allocated to store a file.
- When a file is saved, information on which clusters are used to store the file is kept in a file allocation table.
- A *file allocation table is used to keep track of files on FAT file systems, whereas on* New Technology File System (NTFS) volumes a *Master File Table (MFT) is used.*
- *Using such tables,* the operating system can maintain where files are located. ▶
- When a file is deleted, the record of the file is removed from the table, thereby making it appear as though it doesn’t exist anymore. The clusters used by the file are marked as being free, and can now be used to store some other data.
- However, the data may still reside in the clusters of the hard disk.

- Partitions are used to create a logical division of a hard disk.
- Even if multiple partitions aren't used, the entire disk can be set as a single partition, formatted to use a particular file system (such as FAT or NTFS) and given a drive letter (such as C:, D:, etc.).
- Information about how partitions are set up on a machine is stored in a *partition table, which is stored* in the Master Boot Record (MBR).
- When the computer is booted, the partition table allows the computer to understand how the hard disk is organized, and then this information is passed to the operating system when it is started.
- When a partition is deleted, the entry in the partition table is removed, making the data inaccessible.
- However, even though the partition entry has been removed, the data still resides on the hard disk.
- Many different tools are available to recover deleted files and deleted partitions from a hard disk.
- Depending on how the data was deleted, and whether it was overwritten before it could be recovered and there is the possibility that files and partitions can be restored.

Partition Table



Recovering “Deleted” and “Erased” Data

A *deleted file is any file that has been logically erased from the file system, but may still remain physically on storage media*.

Deleting a file

- Hard disk usually fill up quickly from all of the temporary files, backup files, and other data written to a disk by the operating system or other software installed on a computer.

- Every operating system provides a way to remove data from a hard disk.

- Although the OS and applications on a machine will generally clean these up when they are no longer needed, this isn’t always the case.

- In addition, there are also files that users of the computer have created and no longer need anymore.

- How a file is deleted can vary.

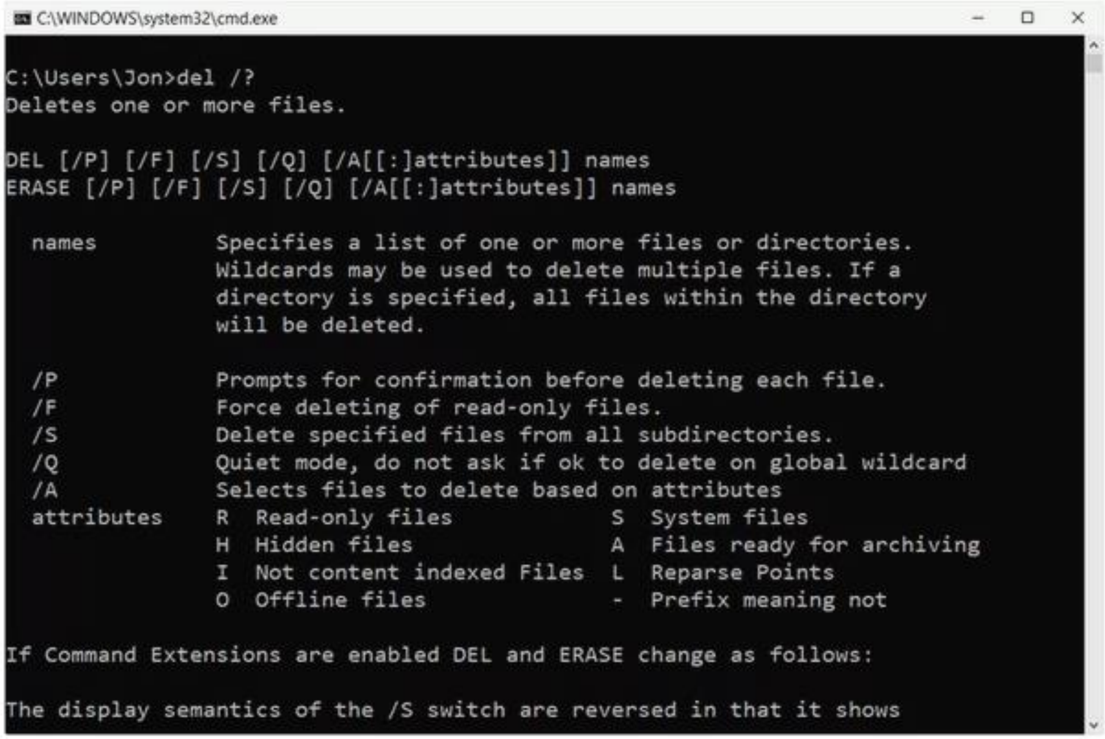
- For many people, deleting a file means selecting a file and pressing the Del or Delete key on their keyboard, there are other ways in which a file may be deleted.

Command-Line Delete

- One way to delete a file is from a command prompt.
- *Command Prompt is a window that provides an interface to* enter the commands to perform certain actions.
- Commands to delete files or directories from the command line:
  - ❑ *DEL*
  - ❑ *ERASE*
- In using these command, the file that is deleted will have the pointer to that file removed from the table (The FAT file system uses a file allocation table to keep track of files, whereas NTFS uses an Master File Table), **but the data remains on the hard disk.**

In using these command, the file that is deleted will have the pointer to that file removed from the table (The FAT file system uses a file allocation table to keep track of files, whereas NTFS uses an Master File Table), **but the data remains on the hard disk.**

This gives analyst the opportunity to acquire the data using file recovery or forensic tools.



```
C:\Users\Jon>del /?
Deletes one or more files.

DEL [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names
ERASE [/P] [/F] [/S] [/Q] [/A[[:]attributes]] names

  names         Specifies a list of one or more files or directories.
                Wildcards may be used to delete multiple files. If a
                directory is specified, all files within the directory
                will be deleted.

  /P            Prompts for confirmation before deleting each file.
  /F            Force deleting of read-only files.
  /S            Delete specified files from all subdirectories.
  /Q            Quiet mode, do not ask if ok to delete on global wildcard
  /A            Selects files to delete based on attributes
  attributes    R  Read-only files            S  System files
                H  Hidden files               A  Files ready for archiving
                I  Not content indexed Files  L  Reparse Points
                O  Offline files              -  Prefix meaning not

If Command Extensions are enabled DEL and ERASE change as follows:

The display semantics of the /S switch are reversed in that it shows
```

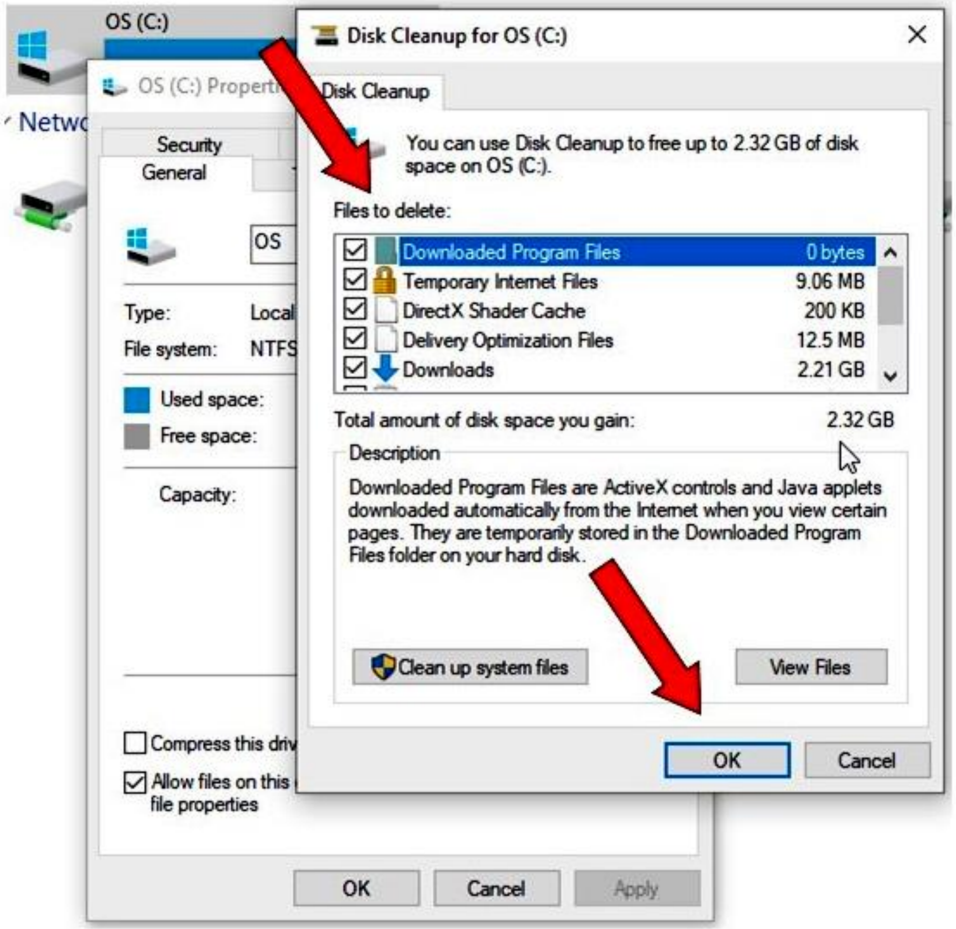
Moving Files : Another method of deleting a file involves moving it.

- If the file is moved from one directory to another on the same partition, the table used to keep track of where files are stored is updated.
- Because the file still resides on the same partition, a pointer to the file's location is updated.
- Here, the record showing the file's location is modified to reflect that it's now in another directory, but nothing else about the file changes.
- Also, any attributes on the file (such as whether the file is compressed, permissions etc) remains the same.
- When a file is moved from one hard disk or partition to another, it is actually a multistep process of copying and deleting the file.
  - **First**, a new copy of the file is created on the target partition location.
  - Once the file has been copied, the original file is then deleted.
- This process also requires some **updations in the FAT or MFT tables.**
- A new entry is created in the table on the partition where it has been copied, while the record for the deleted file is removed from the table on its partition.
- When a file is moved from one partition to another, it can offer greater possibilities for recovering a file that has been deleted.
- If a file is moved to another partition and then deleted later, the file has essentially been deleted twice.
- Hence, recovery can be made from the partition on which it was deleted, and also from the partition from which it was moved.

Using Software Programs to Delete :

- Another way in which files are deleted is when a software program that does the deletion task.
- Sometimes files are not properly removed, and a considerable number of files may continue to reside on a hard disk.
- This is the reason for tools such as Disk Cleanup, which removes files and programs from a computer.
- Software will generally clean up by deleting old setup, temporary, and backup files when they're no longer needed.
- Disk Cleanup will check for files that can be safely removed so that more disk space is available for use and performance is improved.

Disk Cleanup



Disk Cleanup for OS (C:)

You can use Disk Cleanup to free up to 2.32 GB of disk space on OS (C:).

Files to delete:

☑	Downloaded Program Files	0 bytes
☑	Temporary Internet Files	9.06 MB
☑	DirectX Shader Cache	200 KB
☑	Delivery Optimization Files	12.5 MB
☑	Downloads	2.21 GB

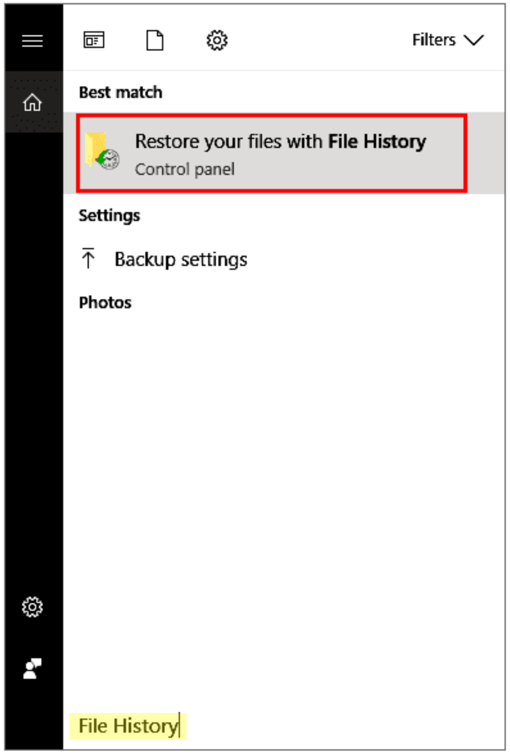
Total amount of disk space you gain: 2.32 GB

Description

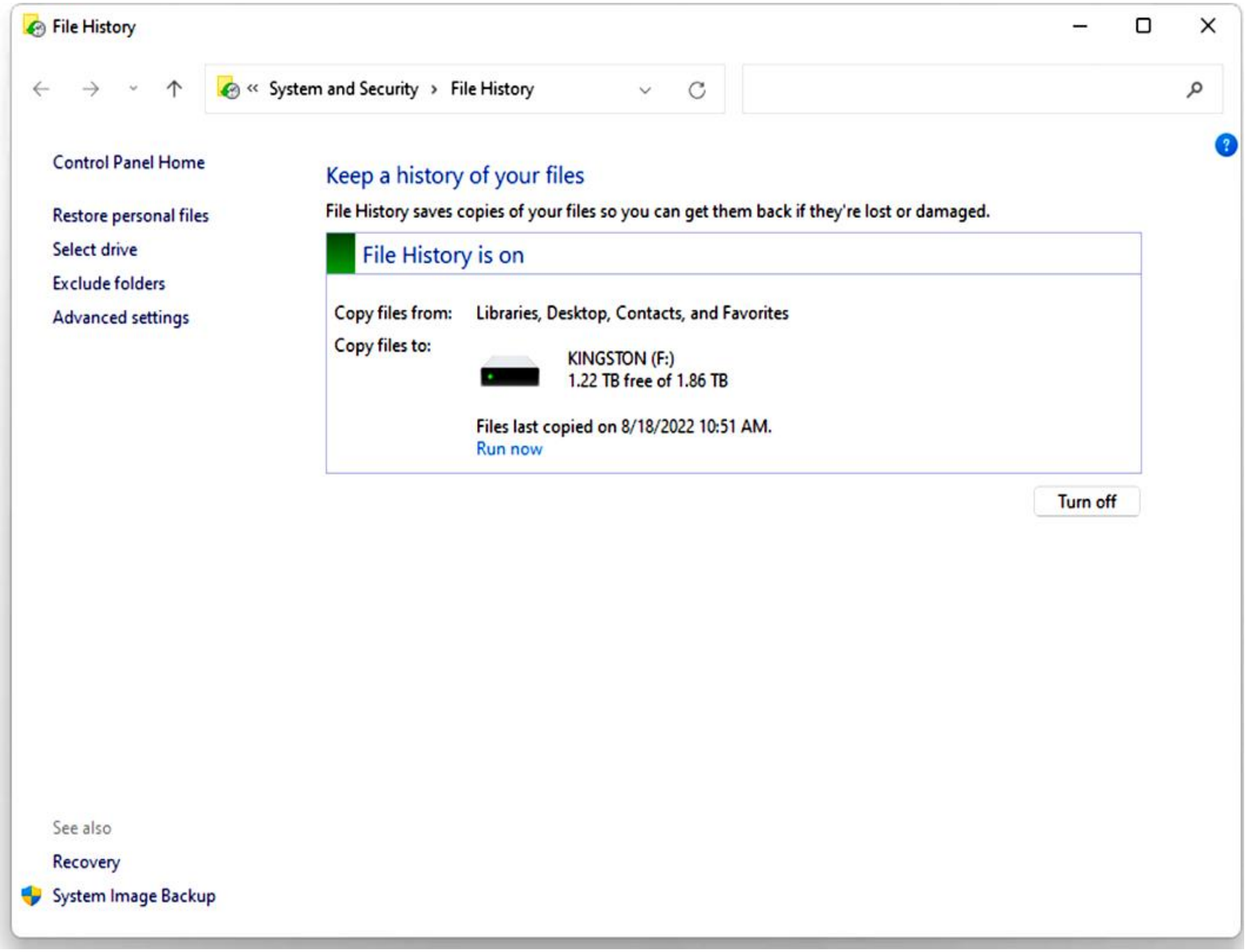
Downloaded Program Files are ActiveX controls and Java applets downloaded automatically from the Internet when you view certain pages. They are temporarily stored in the Downloaded Program Files folder on your hard disk.

Clean up system files

Undo Disk Cleanup in Windows 11/10/8/7 and Restore Deleted Files



File History



Keep a history of your files

File History saves copies of your files so you can get them back if they're lost or damaged.

File History is on

Copy files from: Libraries, Desktop, Contacts, and Favorites

Copy files to: KINGSTON (F:)
1.22 TB free of 1.86 TB

Files last copied on 8/18/2022 10:51 AM.

Forensics: You could look through either the **UserAssist** registry entries for each user (located in `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist`), or check the **prefetch** files (located at `%SystemRoot%\Prefetch`).

Both maintain a list of run programs on the machine including the last time they were run and the number of times said program was run.

Most privacy protection tools and many disk sanitizers are effective against casual observers, but leave many traces behind that can be easily discovered during an investigation.

Many disk cleaners will provide options to clean up:

- Cache and history for popular Web browsers
- Chat logs produced with some other popular instant messengers like skype
- Provide “secure delete” option to wipe files
- Clean some (but almost never all) of the following: jumplists, thumbnails databases, temporary files, registry Items, recycle bin etc.

Even though ,some traces are still left after running a disk cleaning tools for example:

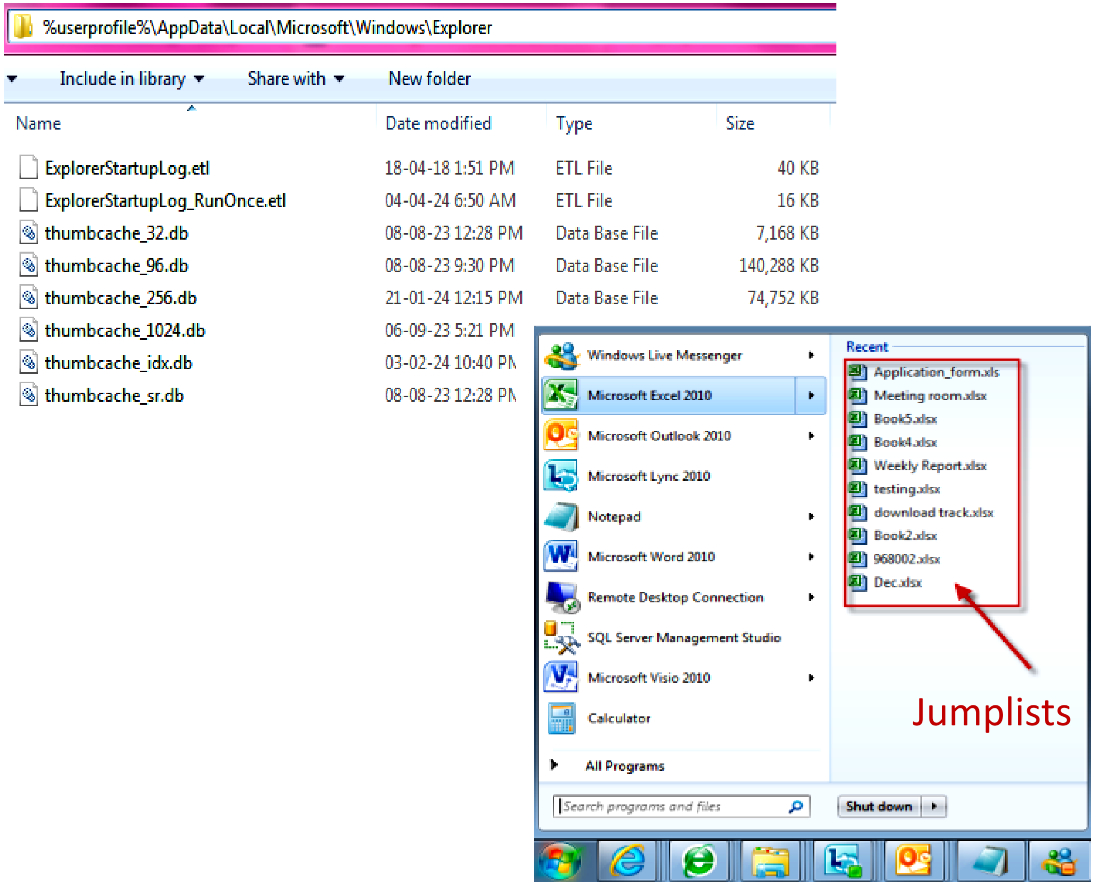
Deleted digital pictures, but did not clean thumbnails cache. ***%userprofile%\AppData\Local\Microsoft\Windows\Explorer***

Deleted documents, but did not clean Windows jumplists : **C:\Users\xxx\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations**

Deleted main Skype database but did not touch chatsync

Failed to delete files that were currently opened (e.g. deleted files from the browser cache but could not delete the index database)

Deleted files but left corresponding Registry entries intact



%userprofile%\AppData\Local\Microsoft\Windows\Explorer

Name	Date modified	Type	Size
ExplorerStartupLog.etl	18-04-18 1:51 PM	ETL File	40 KB
ExplorerStartupLog_RunOnce.etl	04-04-24 6:50 AM	ETL File	16 KB
thumbcache_32.db	08-08-23 12:28 PM	Data Base File	7,168 KB
thumbcache_96.db	08-08-23 9:30 PM	Data Base File	140,288 KB
thumbcache_256.db	21-01-24 12:15 PM	Data Base File	74,752 KB
thumbcache_1024.db	06-09-23 5:21 PM		
thumbcache_idx.db	03-02-24 10:40 PN		
thumbcache_sr.db	08-08-23 12:28 PN		

The Recycle Bin

- Files can be deleted by using commands and utilities, and performing actions such as moving files.

- With each method, the files are no longer visible to the operating system, and are considered “permanently” deleted.

- But Data can still be recovered, Until the data is overwritten or destroyed using the methods.

- The operating system considers the file “permanently” deleted because there are no programs native to the OS that will allow you to restore the files.

- A *Recycle Bin or Trash* is a repository where files are temporarily stored after they are deleted.

- The previously deleted items can be browsed and manually drag and drop items out of the trash, or delete all of the items.

- When a file is deleted from the desktop or by using Windows Explorer, the file is moved to the Recycle Bin with a record of its original location.

- The file is not actually been deleted; its pointer has simply been changed to show that it now resides in the Recycle Bin.

- If a file or directory was deleted and you tried to open it in the Recycle Bin to view its contents, double-clicking on it would display only the properties of the deleted item.

- In the Recycle Bin, however, you can restore or “permanently” delete individual items so that the space can be made available for storing other files.

What Gets Deleted?

- Recycle Bin is a repository for deleted items, but everything that is deleted does not all goes to Recycle bin.

- Any items stored on local hard drives that were deleted using Windows Explorer or the desktop will appear in the Recycle Bin.

❑ Any items you delete using application software that is Windows-compliant will send a deleted item to the Recycle Bin.

- **For example:** Selecting the item and pressing the Delete key on your keyboard would send the item to the Recycle Bin.

- However, many application programs are not compliant and simply delete the item, never to be seen again without the use of data recovery or forensic software. **For example:**
  - When utilities such as Disk Cleanup, or the command-line *DEL and ERASE* commands are used, the files bypass the Recycle Bin and are simply deleted.

❑ The same may occur if software on your machine was cleaning up files after an installation or shutting down.

For example:

In case of Windows Updates, the files used to install programs, patches, and service packs would be deleted and would never appear in the Recycle Bin.

❑ Files are also not send to recycle bin if they are not on the local hard drives. Files that on a mapped network drive, a compressed folder, a floppy disk, or any other form of removable storage media, the file would also not be sent to the Recycle Bin on deletion.

- The same may occur if a file that is too large for the Recycle Bin, it gets deleted.

- Due to insufficient space in the Recycle Bin for a file or directory that's deleted, a warning message will appear informing that it will be deleted.

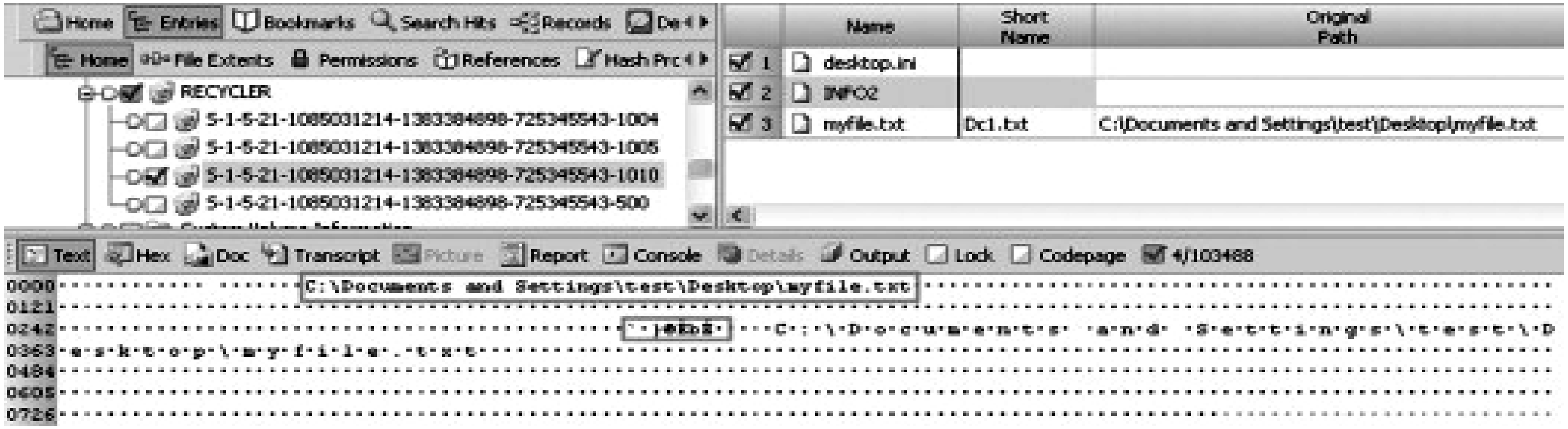
Undeleting from recycle bin and Permanently Deleting a File

- When a file is deleted it is indicated as being located in the Recycle Bin directory in the root drive of the partition on which it was deleted.

- The file is then renamed, using the following syntax: *D<original drive letter><#>.<original extension>*

- **For Example:** C:\myfile.txt is to be deleted, and this was the second file that was deleted and residing in the Recycle Bin. The file would be renamed Dc2.txt.

- The file original name and location are stored in a hidden index file named INFO, which is located in the Recycle Bin folder(for Vista OS). INFO file allows the file to be automatically restored to its original location.



```
RECYCLER
  S-1-5-21-1085031214-1383384898-725345543-1004
  S-1-5-21-1085031214-1383384898-725345543-1005
  S-1-5-21-1085031214-1383384898-725345543-1010
  S-1-5-21-1085031214-1383384898-725345543-500
```

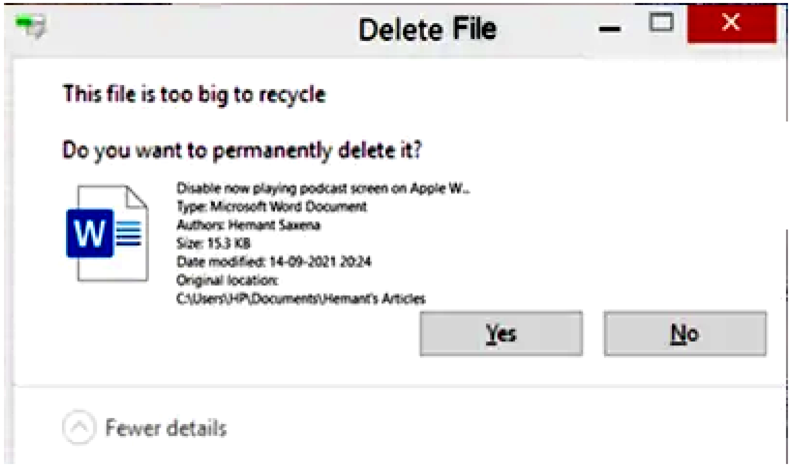
	Name	Short Name	Original Path
☑ 1	desktop.ini		
☑ 2	INFO2		
☑ 3	myfile.txt	Dc1.txt	C:\Documents and Settings\test\Desktop\myfile.txt

```
0000············ ······C:\Documents and Settings\test\Desktop\myfile.txt····························
0121················································································
0242·······································  ·  ·······C·:·\·D·o·c·u·m·e·n·t·s· ·a·n·d· ·S·e·t·t·i·n·g·s·\·t·e·s·t·\·D
0363·e·s·k·t·o·p·\·m·y·f·i·l·e·.·t·x·t·······················································
0484················································································
0605················································································
0726················································································
```

- Deleting or emptying files from the Recycle Bin permanently deletes them from the system, and makes it so that they can be recovered only with data recovery or forensic software.

- Although the Recycle Bin can be configured so that files are immediately deleted, you can also delete a file and not have it go to the Recycle Bin on a file-by-file basis.

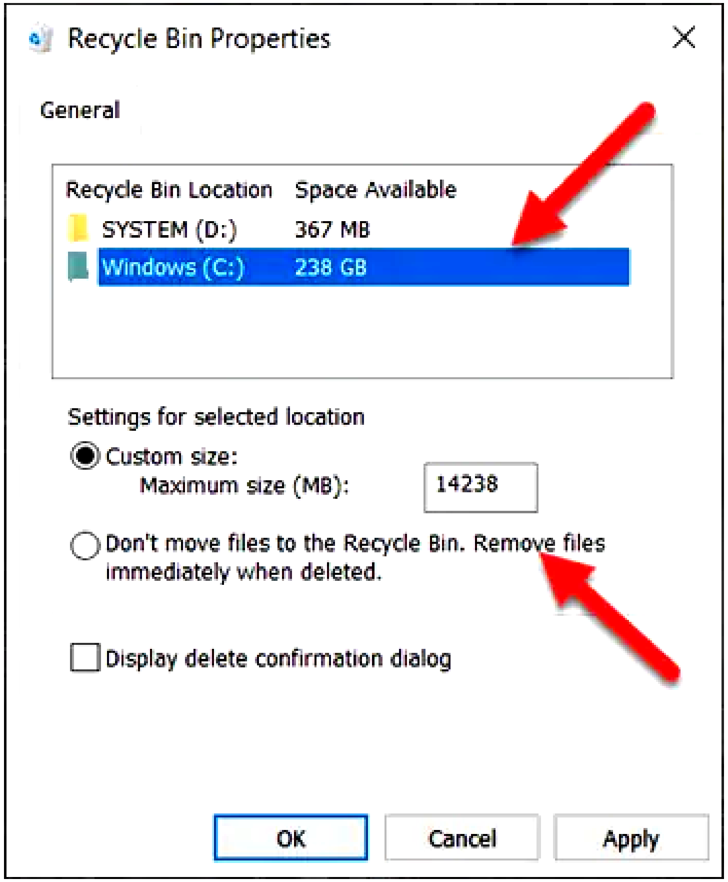
- If you wanted to bypass the Recycle Bin and simply delete the file, you would select the file you want to delete, and then hold down **Shift + Del key.**


Delete File

This file is too big to recycle

Do you want to permanently delete it?

Disable now playing podcast screen on Apple W...
Type: Microsoft Word Document
Authors: Hemant Saxena
Size: 15.3 KB
Date modified: 14-09-2021 20:24
Original location:
C:\Users\HP\Documents\Hemant's Articles


Recycle Bin Properties

General

Recycle Bin Location	Space Available
SYSTEM (D:)	367 MB
Windows (C:)	238 GB

Settings for selected location

● Custom size:
Maximum size (MB): 14238

○ Don't move files to the Recycle Bin. Remove files immediately when deleted.

□ Display delete confirmation dialog

Other ways by which data gets deleted in Windows

- **Human error**: users are more likely to make a mistake that results in the loss of important files.
- **Software issues**: A software bug can cause an application or even the entire operating system to suddenly stop working, leaving you no time to save your work and prevent data loss.
- **Data corruption**: A file can become corrupted and impossible to open because of software and hardware issues alike. When that happens, you might be able to repair the damage using dedicated tools, or you can always recover a functioning version of the file from a backup.
- **Hardware malfunction**: Modern storage devices can store huge quantities of data and do so without costing too much money, but their reliability is still unpredictable and stories of sudden malfunction are not rare.
- **Unpredictable disasters**: A particularly close lightning strike or a single spilled cup of coffee can render an entire storage device—or even an entire computer—unusable, causing an instant loss of valuable data.
- **Malware**: One of the most common malware threats today, for example: ransomware, causes data loss by encrypting files and demanding a ransom payment for their decryption.
- **Upgrading gone wrong**: Most Windows power users agree that it’s better to perform a clean install when installing a new version of Windows because upgrading from an older version doesn’t always go according to plan (For ex: incomplete bios updates), and data loss may occur.

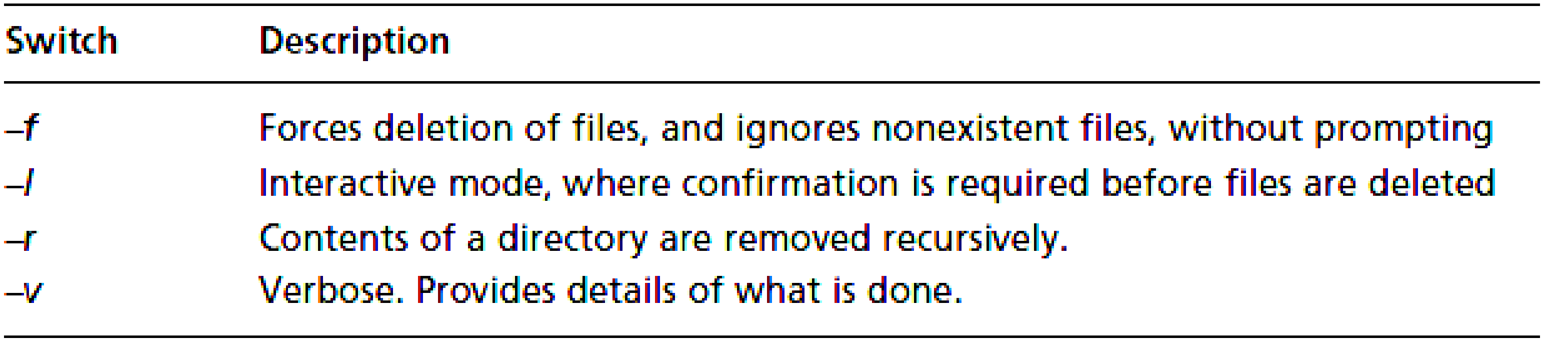
Data deletion in Linux

- First how files are deleted in linux.

- To delete a file in Linux or UNIX, you would use the *rm /rmdir command.*

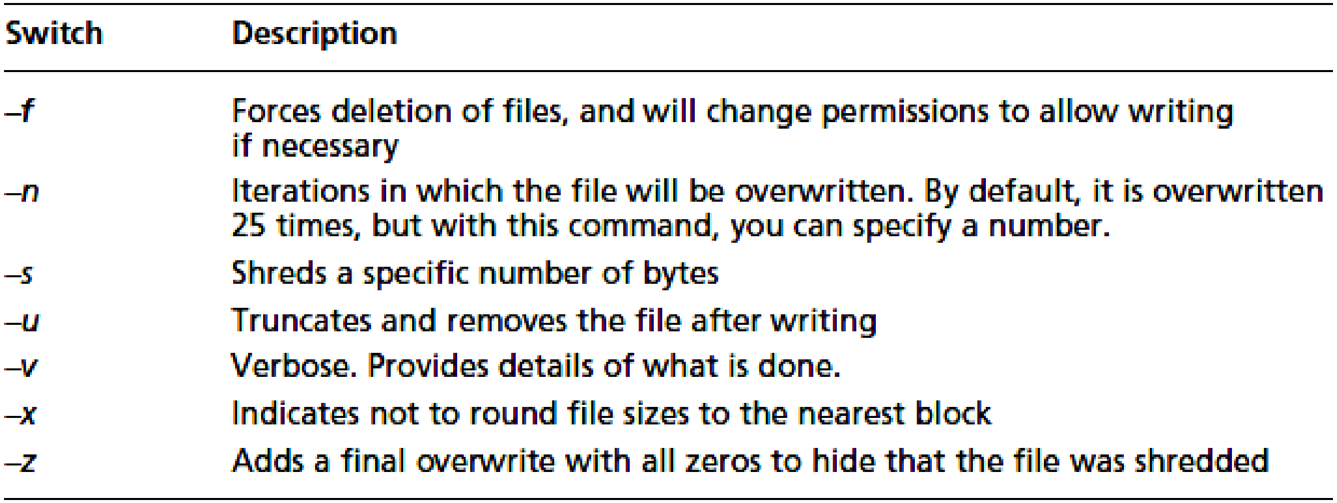
- *Deleting a file with this command won't prompt you* for any confirmation by default, so once it's deleted you'll have to rely on data recovery software to restore the file.

- *rm commond also uses no of switches shown bellow:*



Switch	Description
–*f*	Forces deletion of files, and ignores nonexistent files, without prompting
–*I*	Interactive mode, where confirmation is required before files are deleted
–*r*	Contents of a directory are removed recursively.
–*v*	Verbose. Provides details of what is done.

- Another way of deleting files in Linux and UNIX is to use the ***shred command***.
- With this command, the file is deleted and overwritten to ensure that it can’t be recovered.
- By overwriting the data on a disk, the file cannot be recovered.
- Therefore, it is important that this command is used only when user is absolutely sure that the file is to be destroyed.
- Number of options with this command are listed as follows:



Switch	Description
–f	Forces deletion of files, and will change permissions to allow writing if necessary
–n	Iterations in which the file will be overwritten. By default, it is overwritten 25 times, but with this command, you can specify a number.
–s	Shreds a specific number of bytes
–u	Truncates and removes the file after writing
–v	Verbose. Provides details of what is done.
–x	Indicates not to round file sizes to the nearest block
–z	Adds a final overwrite with all zeros to hide that the file was shredded

- Any files deleted using the rm or shred command bypass the Recycle Bin.
- Although the shred command overwrites the data so that it can’t be restored, the rm command doesn’t modify the data after deleting it.
- This means that any files deleted using the rm command could be restored using recovery tools.

Formating

- Data written on a hard disk generally stays there unless it is overwritten or destroyed.

- Many people, think that formatting a hard disk erases all its data, but this is not necessarily so.

- *Formatting defines the structure of the disk.*

❑ *Low-level formatting (LLF), which physically defines where the tracks and sectors are on the disk and marks them blank* i.e. **it does erase data**. After you low-level format hard drives, all the data, partitioning table, boot sectors, file formats, identification ID, and everything related to the drive will be deleted. However, modern disks are formatted at the low level at the factory; users do not perform LLF on today's Integrated Drive Electronics (IDE) and Small Computer System Interface (SCSI) disks.

1. HDD Low Level Format Tool
2. Lowvel tool
3. Diskpart utility

❑ *High-level formatting (HLF) refers to the process of redefining the file system structure*. High-level formatting is a kind of logical formatting. It creates file system structures like Master Boot Record and File allocation tables on the disk. It aims for installing a new or used USB/hard drive for computers with file systems like NTFS, FAT32, exFAT, etc. Thus, we say a disk is quick formatted in FAT or formatted in NTFS.

1. File Explorer
2.Disk Management

- There is always the chance that tools can be used to restore the data with HLF, provided a file hasn't been overwritten or damaged in some way.

Recovering Deleted Files

- ***Data recovery*** *is* a process of recovering data that was lost or deleted to make it available again.

- *Why am I recovering it? This question in itself will decide whether you will need to perform data recovery* or computer forensics.

- Although the two terms are often used interchangeably, there is a difference in why the data is being acquired;

- Data recovery seeks to **restore (partial/complete) data**, whereas computer forensics seeks to **obtain data of evidential value** (complete and authentic) that can be produced in court.

- Data recovery software is extremely useful in situations where someone has accidentally deleted files from his or her computer or other media, **For example:**
  - when an officer has deleted his or her important document like curriculum vitae, notes that were stored in a Microsoft Word document, or other data that isn't evidence in a case.
  - However,, such software isn't suitable for obtaining evidence from a suspect computer.

- Standard data recovery software may not guarantee that the file won't be modified when it is recovered, or the software may generate temporary files that could damage other data on the disk.

- *Computer forensics* is a process of gathering and examining evidence to establish facts so that accurate testimony and evidence can later be presented in court or other hearings.

- To preserve data, special computer forensic software is necessary.
- **For example:**
  - Investigation of any incident, will eventually go to court. If the software used wasn't designed for forensic use, it can alter or damage data on the disk, and therefore compromise the investigation.

- In any situation where investigation is done on an *intrusion, policy violations, cybercrimes*, or other incidents in which data could be used as evidence, one should always take the side of caution and only use computer forensic tools.

- Regardless of which type of tool you use, you should never install the software on the drive containing the data that needs to be recovered. **For example:**
  - If a file is accidentally deleted on your C: drive and then a downloaded and installed data recovery software to your C: drive, could overwrite the data that needs to be recovered in the first place.
  - Whereas, Computer forensic software may demand use of bootable disks to access the drive, or connect to the machine using a network cable.

- By sharing the drive and connecting to it over a network or using a network cable to connect two machines, the data can be restored without worrying about corrupting data on the disk.

- If the computer has two disk drives and you are performing data recovery, **you could also install the software on another disk drive**.

- Whenever using tools, remember that the integrity of the data which is to be recovered is of high importance, and necessary actions are taken to prevent it from being damaged.

Deleted File Recovery Tools

- ***Data recovery tools*** are designed to restore data that has been deleted or corrupted from any number of sources, including :
  - ❑ Hard disks,
  - ❑ CDs, DVDs, Blu-ray discs, HD-DVDs,
  - ❑ Floppy disks ,
  - ❑ Memory cards used in digital cameras, pendrives and other storage media.
  - ❑ Mobile phones internal memory
- Depending on the features of the software, it will scan the media and look for any corrupted or deleted files and display which ones are available for recovery, allowing you to pick and choose which ones will be restored.

- In some cases, the tools will even repair damaged files so that data can be accessible again.

- It's important to note that the effectiveness of file repair software can vary depending on factors such as the **severity of the damage**, **the complexity of the file format**, and the **capabilities of the specific software being used**. In some cases, particularly with severely corrupted files, it may not be possible to fully recover the data.

- Even though many deleted file recovery tools aren't suitable for computer forensics, It is important that security professionals realize these tools are available on the Internet or are included with operating systems.

- It is possible that before a forensic examination of the computer is performed, the user of the computer or a member of the information technology (IT) staff may attempt to use such tools.

General process of how file repair software typically works:

1. **Identification of File Format**: The software first needs to recognize the format of the file being repaired. Different file formats have different structures and may require specific repair techniques.

2. **Analysis of File Structure**: Once the file format is identified, the software analyzes the structure of the file to understand its components, such as headers, data blocks, and metadata.

3. **Detection of Errors or Corruption**: The software then scans the file to identify any errors, corruption, or missing data. This could include identifying incorrect data, missing sections, or inconsistent structures.

4. **Repair Algorithms**: Based on the analysis, the software employs various repair algorithms to attempt to fix the identified issues. These algorithms can range from simple techniques such as removing or replacing corrupted data to more complex methods like reconstructing missing sections based on surrounding data.

5. **Data Recovery**: In cases where data is missing or corrupted beyond repair, some file repair software may attempt to recover as much usable data as possible by extracting intact portions or using data from redundant parts of the file.

6. **Verification and Validation**: After repair attempts are made, the software typically verifies the integrity of the repaired file to ensure that it meets the expected standards and doesn't introduce further errors.

7. **Output**: Finally, the repaired file is generated as the output. Depending on the software and the extent of the damage, the output may be a fully repaired file, a partially recovered file with some data loss, or a report detailing the remaining issues.

1. Undelete Tools

- Using commands such as *DEL and ERASE* from the command line or holding down the Shift key when deleting a file will bypass the Recycle Bin.
- To restore the file, you need to use tools that will search the hard disk for deleted files and allow you to undelete them.
- A number of tools are available with various features that make undeleting files easier.
- They should be used as soon as possible, however, to avoid any other data overwriting the file.

Undelete

- Undelete is an external command that is available for the following Microsoft operating systems as undelete.exe .
- **UNDELETE followed by the path to the file that needs to be restored**.

```
UNDELETE  C:\MYTEXT.TXT  /all
```

- However, a **number of other programs use this name**, but are designed for newer operating systems. These include:
  - ❑ Active@ UNDELETE (www.active-undelete.com), which can recover data from basic volumes, including RAID volumes, and large hard disks that are more than 500GB in size. It also supports recovery form removable storage media such as USB Flash Drives, ZIP drives, memory sticks and cards, and so forth.
  - ❑ UNERASER (www.uneraser.com), which can access deleted files and supports local files, compressed files, and MBR backups, and can access sectors of the disk drive via a Disk Viewer feature. The UNERASER tool can run from either a bootable floppy disk or a CD. It provides a Bootable ISO CD-Image and Bootable Floppy Creator to create the disk or CD that can then be used to recover files.

- R-Undelete from r-Tools Technology (www.r-undelete.com), which restores deleted files, but also provides an easy-to-use wizard that takes you through the steps of recovering a file. It also provides features that allow you to reconstruct damaged graphics, audio, and video files. Before recovering files, you can preview the file to determine whether you actually want to restore it or leave it deleted.

- Easy-Undelete (www.easy-undelete.com), which will restore not only files from hard disks using FAT12, FAT16, FAT32, and NTFS file systems, but also non-Microsoft partitions such as Linux and Macintosh OS X. It also supports other storage media, such as memory cards used in digital cameras, and it includes a preview feature that allows you to view images before restoring them. In addition, it provides a hexadecimal preview feature that allows you to view the contents of clusters.

- WinUndelete (www.winundelete.com), which allows you to recover files from Microsoft file systems with the original created and modified storage dates. It provides a search feature to scan for specific files, and allows you to filter results by extensions and file types. It also allows you to preview certain types of data before restoring them, such as Microsoft Office documents, images, and plain text.

- Mycroft V3, which is computer forensic software that is developed by DIBS USA, and is available from www.dibsusa.com. The software runs from a bootable disk, and provides a search engine that is used to scan a computer for data on the disk.

2. Recycle Bin Replacements

- Tools are also available that can be install to replace the existing Recycle Bin on Windows machines.

- When these tools are installed, the deleted file is sent to the tool and not to the Windows Recycle Bin.

- Try to identify whether these tools have been installed on a suspect machine so that you can determine whether deleted files may exist in alternative locations.

Two popular tools for replacements for the Recycle Bin include:

- Undelete from Condusiv Diskeeper Corporation (www.undelete.com), which replaces the Recycle Bin with a *Recovery Bin*. Once you install Undelete, any file that's deleted is sent to the Recovery Bin, allowing you to search the bin and restore any files that were accidentally deleted.

- It even provides the ability to view versions of files that were deleted, to select the correct version to restore. If you had a Microsoft Word, Excel, or PowerPoint file that was overwritten, you could use the Recovery Bin to restore a previous version.

- Fundelete is a tool that replaces the Recycle Bin on systems running Windows so that any files that are deleted from the Command Prompt, or using Shift + Del command or within a program can be recovered.

- It also provides filter options so that files with specific file extensions aren't sent to the Fundelete Bin.

3. CD/DVD Data Recovery

- Data recovery software's are also specifically designed to restore damaged and deleted files stored on CDs and DVDs.
- When data is stored on CDs and DVDs, the data can be deleted from rewriteable discs, and can be damaged by scratches, damage, and defects in the media.
- Some of the more popular programs that you can use to restore this data include:
  - ❑ CDRoller
  - ❑ IsoBuster
  - ❑ CD Data Rescue
  - ❑ InDisk Recovery

CDRoller

- CDRoller recovers data written to CDs and DVDs.
- It not only allows recovery of data from CD-ROM, CD-R, and a variety of other CD and DVD formats.
- It provides the ability to split recovered VOB and VRO files (created by DVD video recorders) into separate clips, and can convert raw video into MPEG files, thereby allowing to create a new video from damaged data.
- This tool also provides software to burn data onto CDs and DVDs, allowing to back up any data before there is a problem or once it has been recovered.
- It supports the ISO 9660 file system, Joliet extensions (ISO 9660:1988) for long filename support, and discs formatted in the Universal Disk Format (UDF) file system.

IsoBuster

- **IsoBuster** recovers data from CDs and DVDs as well as from Blu-ray and HD-DVD discs. It also supports ISO 9660, Joliet, and UDF; will scan for IFO, BUP, and VOB file systems on audio and videoDVDs; and supports Mount Rainier CD-RW and DVD+RW discs.

- IsoBuster is also one of the few tools that provide support for discs created using Mac OS file systems.

- It has an HFS Reader to support HFS (hierarchical file system) and HFS Plus file systems, and built-in support for Resource Fork extensions in ISO 9660 and UDF file systems.

CD Data Rescue

- **CD Data Rescue** is a tool developed by Naltech Software (www.naltech.com) and is designed to recover data from damaged, scratched, and defective CD-ROM, CD-R, and CD-RW discs.
- It supports Mount Rainier/EasyWrite MRW discs, and can recover data created by CD writing software in ISO and UDF formats.

InDisk Recovery

- **InDisk Recovery**, developed by OctaneSoft (www.octanesoft.com), is designed to recover data from
- damaged, scratched, defective, or otherwise unreadable CD and DVD discs.
- It supports the ISO-9660, UDF, and Joliet file systems.

Microsoft Office Repair and Recovery

- A file may be corrupted from improperly shutting down the application or computer, or records within a database may be deleted accidentally.
- To restore the data within these files, you can use any of the following products:
  - ❑ OfficeFIX
  - ❑ Repair My Excel
  - ❑ Repair My Word

OfficeFIX

OfficeFIX is a suite of products from Cimaware Software (www.cimaware.com) that is designed to repair and recover data from damaged files that were created with Microsoft Office products. The following tools are included in the suite:

- **AccessFIX** A tool with features to recover, repair, and undelete Access databases. It recovers the data stored in tables, as well as forms, reports, macros, and other data and elements of the database. It has functions that will restore deleted records from tables, and restores password protected files regardless of whether you have the password.

- **ExcelFIX** A tool used to recover corrupted Excel files. It will extract the information from a damaged Excel spreadsheet and store it in a new file, complete with any data, formulas, and other content.

- **WordFIX** A tool used to recover Word files. Not only can it recover the text, but higher editions of this tool can also **recover formatting, tables of contents, embedded images, and other data**.

- **OutlookFIX** A tool used to repair files used in Microsoft Outlook. It provides the ability to recover damaged or deleted e-mail, calendars, notes, attachments, and other elements in Outlook. It also provides an inbox repair tool, and has the ability to split large files into smaller ones to solve the 2 GB limitation on Personal Folders Files (PST).

Repair My Excel and Repair My Word

- A number of other products are designed to repair Microsoft Office products. GetData Software Development (www.getdata.com) provides a number of recovery tools, including:

- **Repair My Excel (www.repairmyexcel.com)** Used to recover spreadsheets created in Excel, including formulas, formatting, and other elements of the file's contents.

- **Repair My Word (www.repairmyword.com)** Used to recover text from corrupt or damaged Word files. Once recovered, it can then be saved in another Word document.

Compressed Files

- Because the compressed file may be damaged, it means that any files stored inside it are inaccessible.
- This means that before recovering a Word document, image, or other file, the compressed file created with a tool such as PKZIP, WinZip, WinRAR, or other compression software must be repaired.

Zip Repair

- **Zip Repair** is another tool developed by GetData Software Development (www.getdata.com) which can be used to repair corrupted ZIP files that have been compressed using WinZip or other software.

- It supports large file sizes of 2GB or more, and can even repair and extract data from spanned ZIP volumes that have been split into smaller sets of data.

- Spanned ZIP files are often used to make large ZIP files into smaller pieces, allowing them to be e-mailed without worry of any e-mail size limitations.

Deleted Images

- Deleted images are common type of data that needs to be recovered.
- Images may be corrupted or deleted from hard disks, or directly from the memory card used in a digital camera.
- At times, the image may have been damaged, and repair of the file is necessary. A number of different tools are available for recovering lost images.

eIMAGE Recovery

- eIMAGE Recovery, developed by OctaneSoft (www.octanesoft.com), is designed to recover any digital images or media that may have been lost or deleted from memory cards used by digital cameras.
- It can restore files from any number of different media, including Compact Flash, SmartMedia, memory sticks, mmd, XD, multimedia, or secure digital memory cards.

Canon RAW File Recovery Software

- Canon RAW File Recovery Software (CRW Repair), a free tool developed by GetData Software Development. Canon cameras usually store images in a JPEG format, with RAW images stored inside a file with a .crw extension.
- The CRW file is generally used for processing photos, and allows the photo's exposure, white balance, and other elements to be manipulated.
- The CRW file also allows users of the camera to access the JPEG quickly.
- Unfortunately, because it is a complex file, it can easily be corrupted by such things as a change in file size.
- CRW Repair will examine the file size to ensure that it's correct, and has the ability to access and extract the JPEG image.

ImageRecall

- ImageRecall Software (www.imagerecall.com) provides several editions of software that could be used to retrieve corrupted or deleted files.
- Using this software, images and videos data can be obtained and restored from memory cards, USB storage devices, and other storage media.
- The tool also provides a Thumbnail viewer that allows you to view small images of the pictures available to recover.

RecoverPlus Pro

- RecoverPlus Pro is a tool that allows you to recover digital images that may have been damaged or deleted, and is available from www.arcksoft.com.
- It provides recovery of a wide variety of graphics formats, and will attempt to adjust the image to improve it during recovery.
- It will attempt to repair any images that are unreadable, and will repair RAW files such as Canon CRW, CR2, and Nikon NEF.
- It provides a preview pane, which allows you to view a full-size image as well as thumbnails that are rendered from the image file.
- RecoverPlus Pro also provides a number of options for how files are scanned and undeleted, including performing a deep level scan on damaged media.

Zero Assumption Digital Image Recovery

- Zero Assumption Digital Image Recovery was a free stand-alone digital image recovery tool developed by Zero Assumption Recovery ZAR(www.z-a-recovery.com).
- However, the stand-alone version of this tool is discontinued, as its features are included in the trial and full versions of ZAR.
- As part of ZAR, Digital Image Recovery is designed to restore pictures from digital memory cards. The types of images it can restore are GIF, JPEG, TIFF, CRW, CR2, MOV, and WAV files.

DiskInternals Flash Recovery

- DiskInternals (www.diskinternals.com) provides a number of data recovery solutions, including DiskInternals Flash Recovery.
- It is designed to recover deleted or corrupted pictures from memory cards, including those that have been reformatted or lost due to a hardware malfunction.
- It provides an easy-to-use interface that allows images to be recovered using a wizard that takes the user step by step through the recovery process.

PC Inspector Smart Recovery

- PC Inspector Smart Recovery is a free tool developed by CONVAR that can be used to restore files from memory cards and memory sticks used with digital cameras.
- It acquires read-only access to the memory card, ensuring that the data isn’t altered.

Deleted Partitions

- The disk volume can be divided into logical partitions(identified by different drive letters) for the purposes of organization of the data.
- Each logical partition can be formatted separately so that each one uses a different file system.
- Partitioning schemes and tools differ depending on the operating system and file system.
- Well, Partitioning utilities do not erase the data on a disk; they only delete and manipulate the partition tables.
- Tools such as **Partition Magic** warn that their use will erase the data on a disk, this is not true; the warning is intended for the average user who will not be able to recover the data after using the utility.
- Generally, partition utilities will delete the entry for that partition in the partition table so that any space associated with the partition becomes unallocated.
- Even if the tool overwrites the first sector (sector 0) of the partition before removing it, a backup of the boot sector may still be available and can be restored.

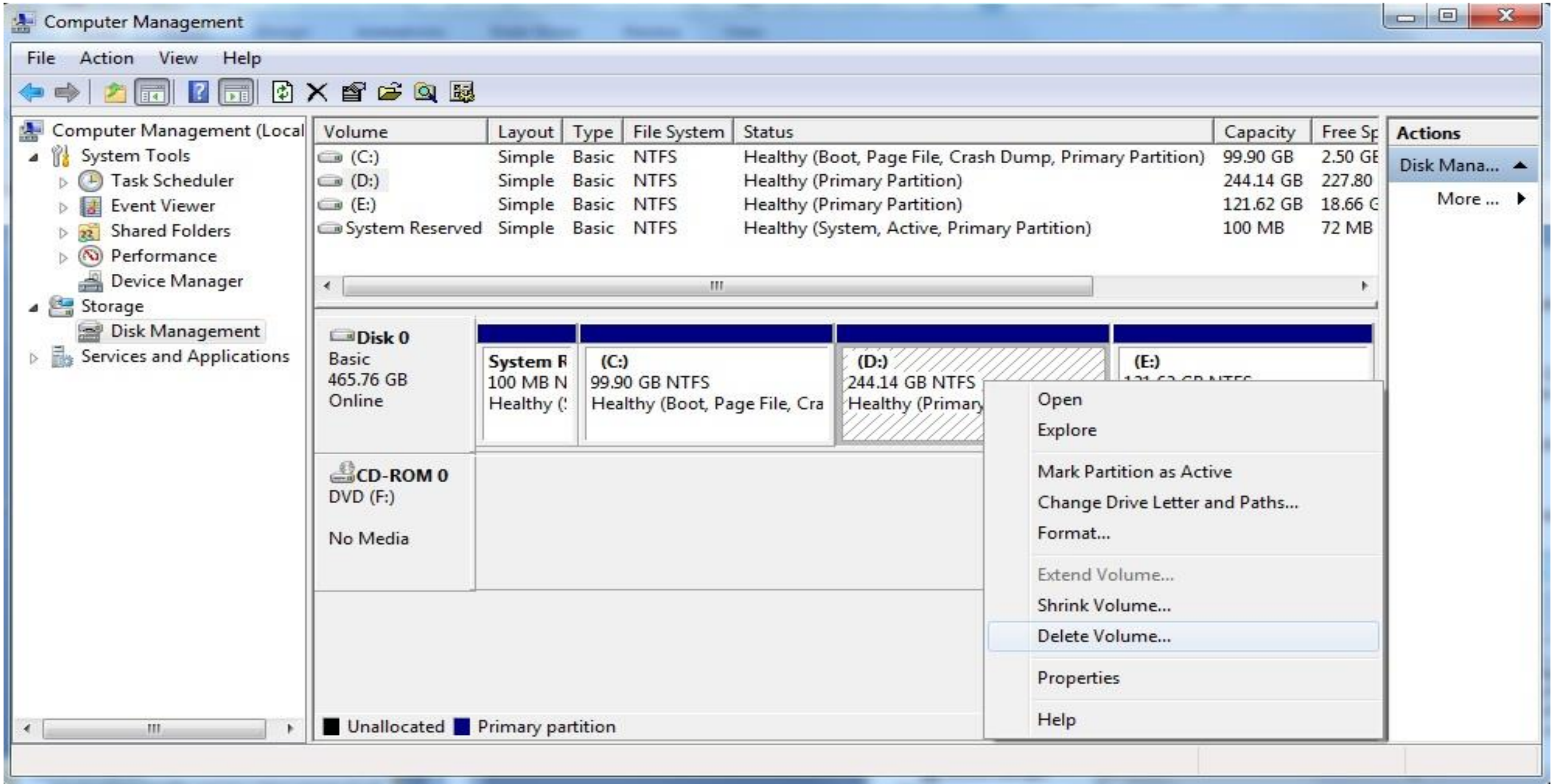
Deleting Partitions Using Windows

- You can create and delete partitions in Windows using the ***Computer Management (Local) console***, which is used to control various aspects of your computer.

- To open the console, you can open the console through the Control Panel. When the Control Panel opens, you would then double-click Administrative Tools, and then double-click Computer Management.

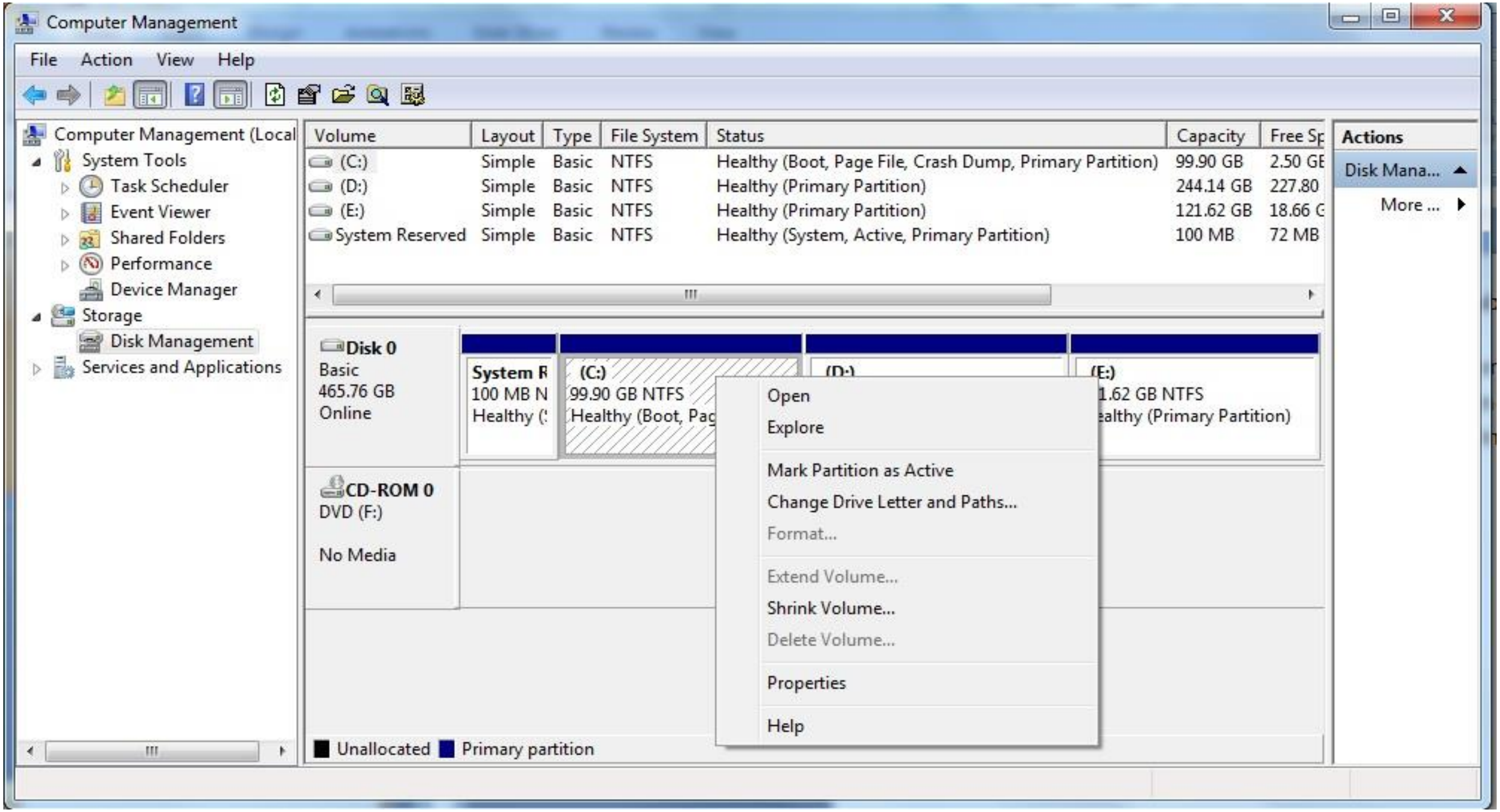
- It is important to note, however, that to access this tool, you need to use an Administrator account or be a member of the Administrators group.

- The Computer Management console provides access to a variety of tools that you can use to manage your computer.



Volume	Layout	Type	File System	Status	Capacity	Free Sp
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	99.90 GB	2.50 GE
(D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	244.14 GB	227.80
(E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	121.62 GB	18.66 G
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	72 MB

- However, the Delete Partition menu item will not be enabled in certain circumstances, where it is impossible to delete the partition:
  - □ A system volume (which contains files to boot the computer)
  - □ A volume with an active paging file or crash dump (memory dump).
  - □ An extended partition that isn't empty. Before deleting an extended partition, all of the logical drives in that partition must be deleted first.



Volume	Layout	Type	File System	Status	Capacity	Free Sp
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)	99.90 GB	2.50 GE
(D:)	Simple	Basic	NTFS	Healthy (Primary Partition)	244.14 GB	227.80
(E:)	Simple	Basic	NTFS	Healthy (Primary Partition)	121.62 GB	18.66 G
System Reserved	Simple	Basic	NTFS	Healthy (System, Active, Primary Partition)	100 MB	72 MB

Deleting Partitions from the Command Line

- Partitions can be deleted from the command line, using disk partitioning utilities that require you to type commands from a prompt.

- Two commands on different versions of Windows:
  - *FDISK*
  - *DISKPART*

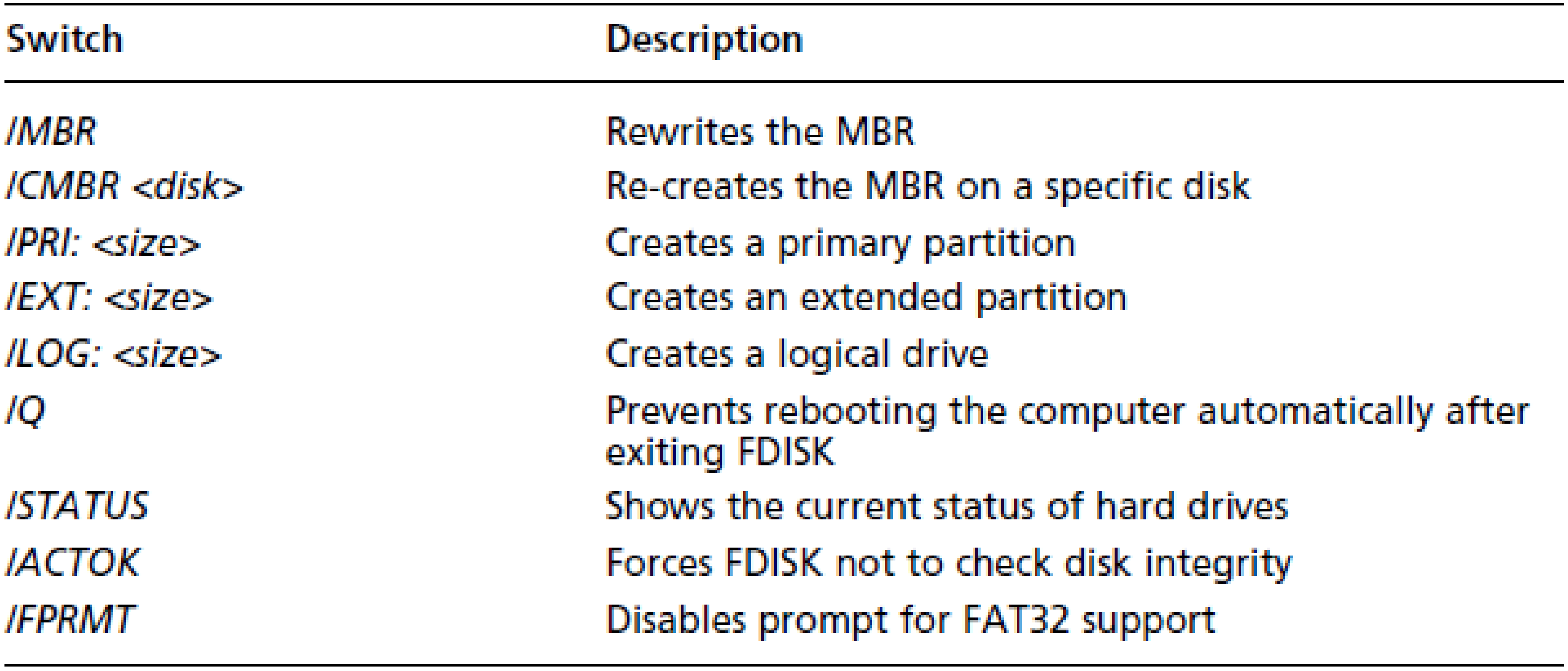
- Using either of these tools, you can view a listing of partitions, determine the number or drive letter of the disk, and delete any existing partitions.

- You must be an Administrator or a member of the Administrators group.
- Again with these utilities, you can't delete a system volume, a boot volume, or a volume with an active paging file or crash dump.

- Also, any logical drives needs to be deleted before deleting an extended partition.

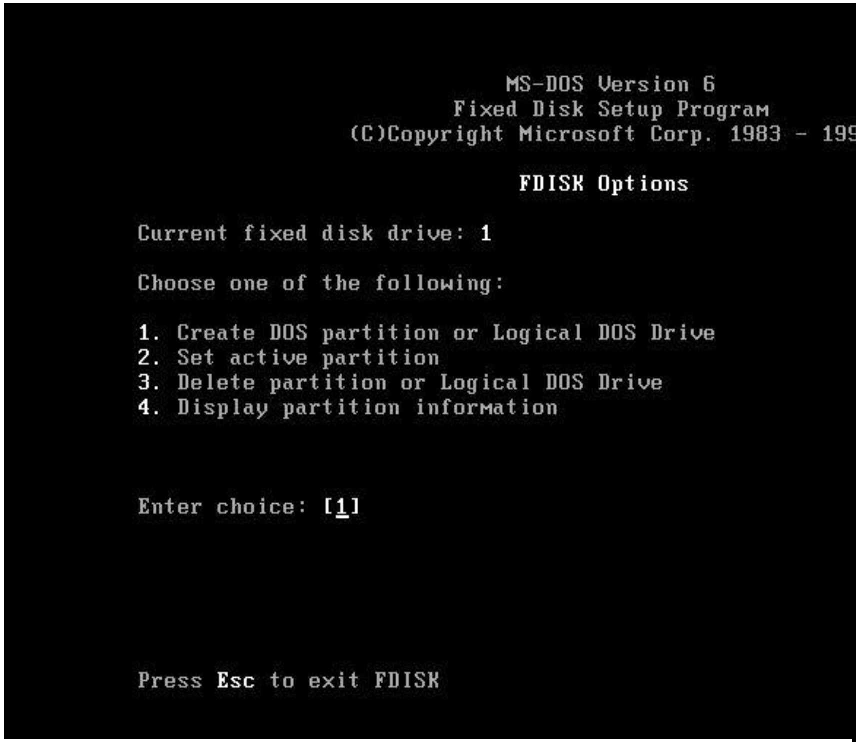
Fdisk

- FDISK is a command line interpreter that is used to create and delete partitions on computers running MS-DOS, Windows 9*x, Windows NT, or Windows Me.*
- A number of switches can be used with this command to view information and perform various actions on a hard disk.
- When you type **FDISK without any of these switches, a series of screens will enable you to** navigate through the process of partitioning the disk.

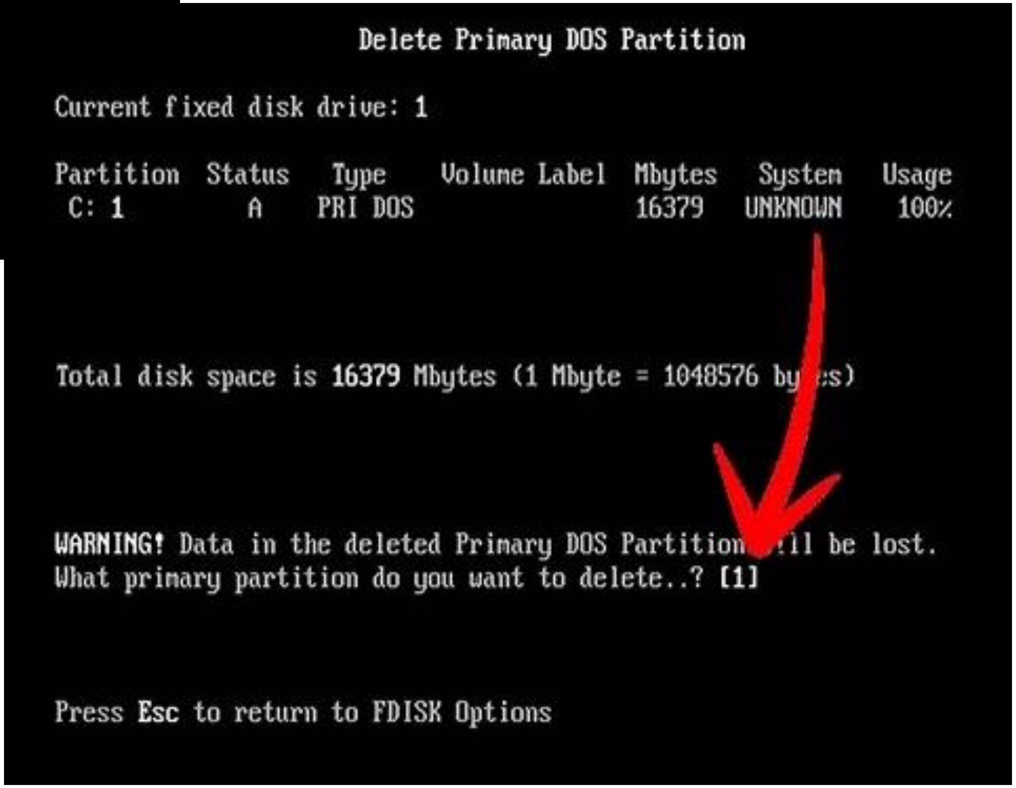


Switch	Description
/MBR	Rewrites the MBR
/CMBR <disk>	Re-creates the MBR on a specific disk
/PRI: <size>	Creates a primary partition
/EXT: <size>	Creates an extended partition
/LOG: <size>	Creates a logical drive
/Q	Prevents rebooting the computer automatically after exiting FDISK
/STATUS	Shows the current status of hard drives
/ACTOK	Forces FDISK not to check disk integrity
/FPRMT	Disables prompt for FAT32 support

MS DOS FDISK



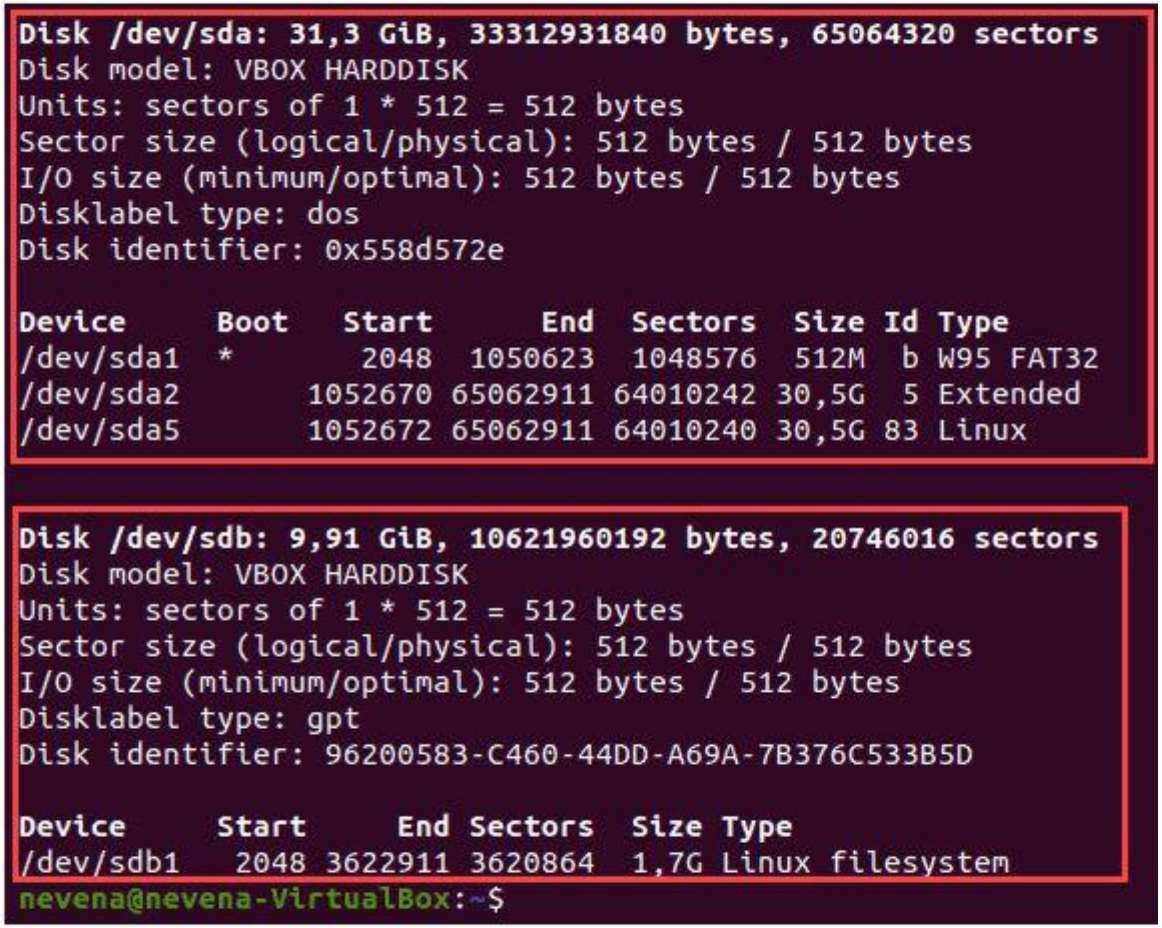
```
                     MS-DOS Version 6
                  Fixed Disk Setup Program
          (C)Copyright Microsoft Corp. 1983 - 1993

                       FDISK Options

     Current fixed disk drive: 1

     Choose one of the following:

     1. Create DOS partition or Logical DOS Drive
     2. Set active partition
     3. Delete partition or Logical DOS Drive
     4. Display partition information



     Enter choice: [1]





     Press Esc to exit FDISK
```



```
                 Delete Primary DOS Partition

Current fixed disk drive: 1

Partition  Status   Type    Volume Label  Mbytes   System   Usage
 C: 1         A    PRI DOS                16379   UNKNOWN   100%



Total disk space is 16379 Mbytes (1 Mbyte = 1048576 bytes)



WARNING! Data in the deleted Primary DOS Partition will be lost.
What primary partition do you want to delete..? [1]



Press Esc to return to FDISK Options
```

LINUX

Fdisk : to display or manipulate a disk partition table.



```
Disk /dev/sda: 31,3 GiB, 33312931840 bytes, 65064320 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x558d572e

Device     Boot   Start      End  Sectors  Size Id Type
/dev/sda1  *       2048  1050623  1048576  512M  b W95 FAT32
/dev/sda2       1052670 65062911 64010242 30,5G  5 Extended
/dev/sda5       1052672 65062911 64010240 30,5G 83 Linux


Disk /dev/sdb: 9,91 GiB, 10621960192 bytes, 20746016 sectors
Disk model: VBOX HARDDISK
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 96200583-C460-44DD-A69A-7B376C533B5D

Device     Start     End Sectors  Size Type
/dev/sdb1   2048 3622911 3620864  1,7G Linux filesystem
nevena@nevena-VirtualBox:~$
```

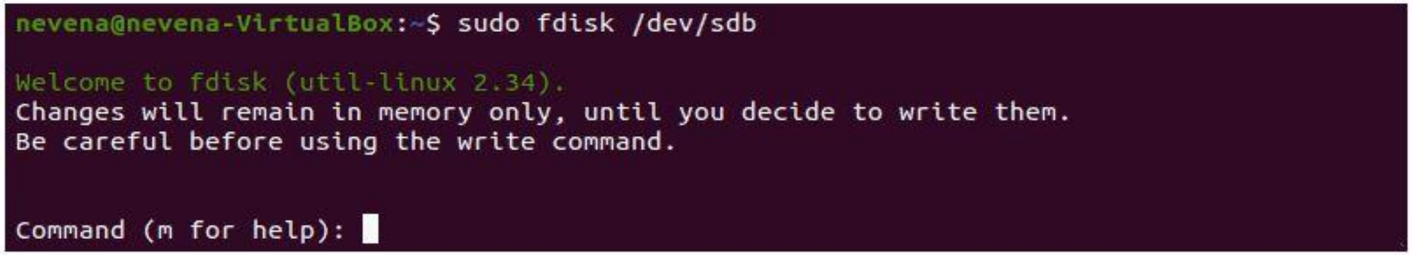
Select the disk that contains the partition you intend to delete.

Common disk names on Linux include:

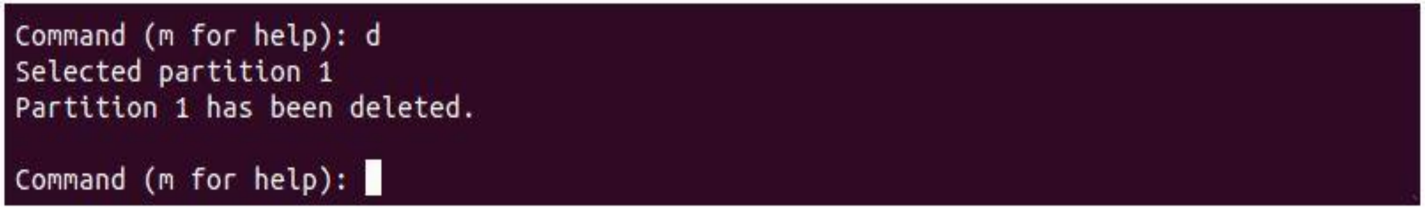
Type of disk	Disk names	Commonly used disk names
IDE	/dev/hd[a-h]	/dev/hda, /dev/hdb
SCSI	/dev/sd[a-p]	/dev/sda, /dev/sdb
ESDI	/dev/ed[a-d]	/dev/eda
XT	/dev/xd[ab]	/dev/xda

To select a disk, run the following command:

```
sudo fdisk /dev/sdb
```



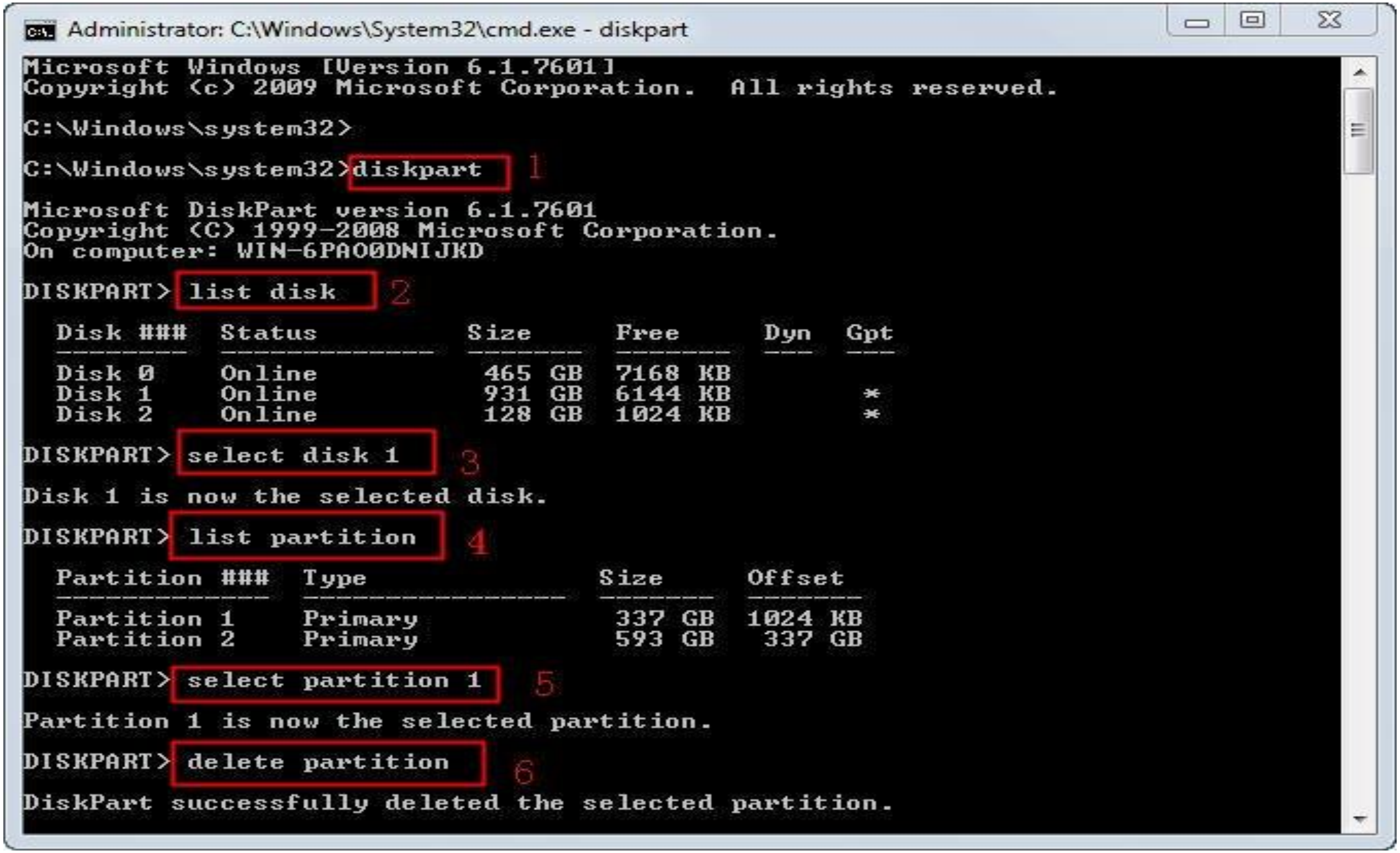
```
nevena@nevena-VirtualBox:~$ sudo fdisk /dev/sdb

Welcome to fdisk (util-linux 2.34).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.


Command (m for help): 
```



```
Command (m for help): d
Selected partition 1
Partition 1 has been deleted.

Command (m for help): 
```

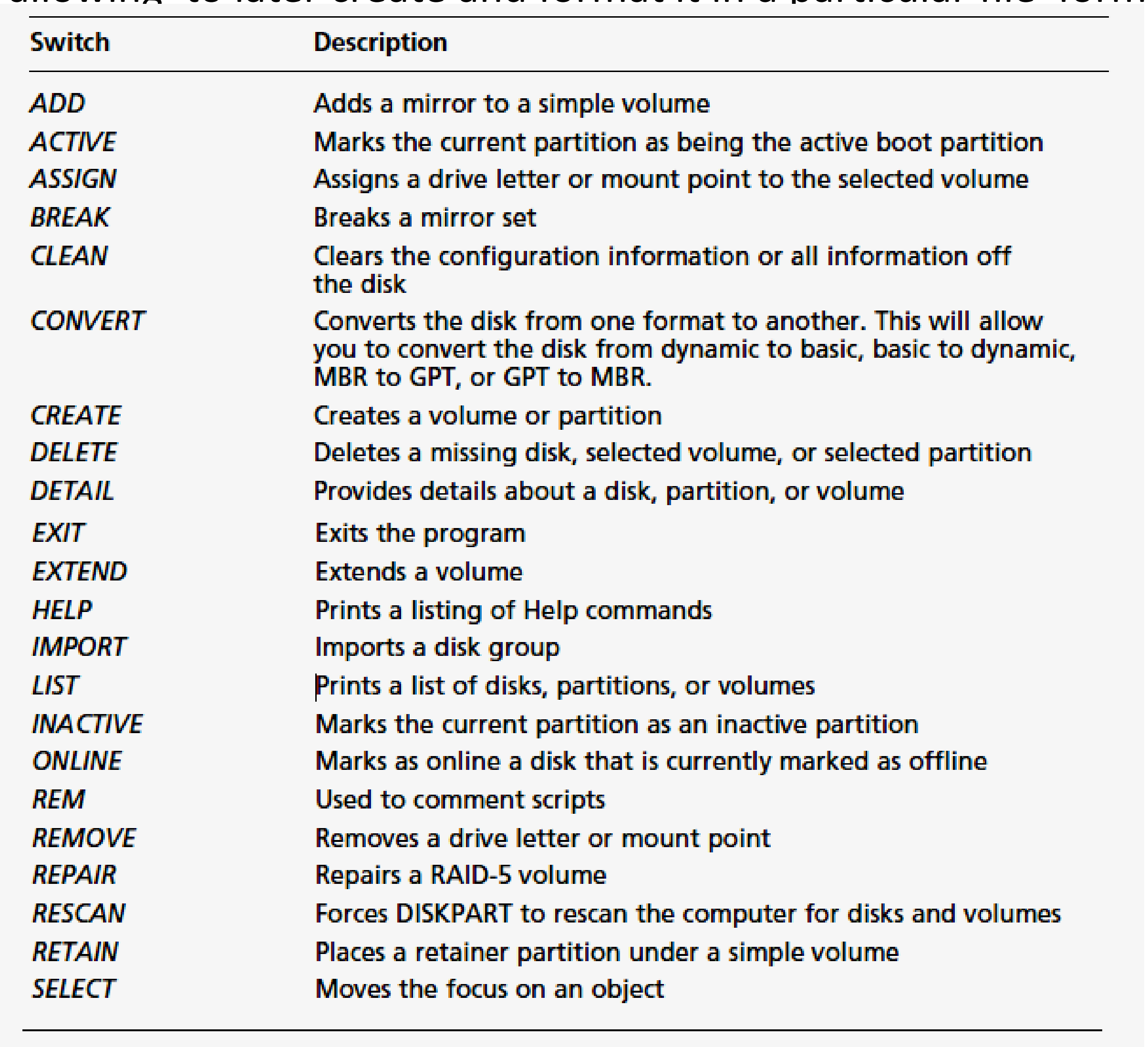
DISKPART

- DISKPART is a command-line interpreter that is used to create and delete partitions on computers running Windows 2000, XP, Vista, Window 7/10 . Unlike FDISK, it doesn’t provide a series of menus that can be navigated to delete partitions.
- Typing diskpart at the prompt will activate the command-line interpreter, allowing you to enter different commands.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>

C:\Windows\system32>diskpart   1

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: WIN-6PAO0DNIJKD

DISKPART> list disk   2

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online          465 GB  7168 KB
  Disk 1    Online          931 GB  6144 KB        *
  Disk 2    Online          128 GB  1024 KB        *

DISKPART> select disk 1   3

Disk 1 is now the selected disk.

DISKPART> list partition   4

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Primary            337 GB  1024 KB
  Partition 2    Primary            593 GB   337 GB

DISKPART> select partition 1   5

Partition 1 is now the selected partition.

DISKPART> delete partition   6

DiskPart successfully deleted the selected partition.
```

- A number of switches can be used through DISKPART to view information on disks and partitions on your hard disk, as well as perform tasks such as creating and deleting partitions.
- Using a combination of these switches, a partition can be deleted from a computer, and also allowing to later create and format it in a particular file format.



Switch	Description
ADD	Adds a mirror to a simple volume
ACTIVE	Marks the current partition as being the active boot partition
ASSIGN	Assigns a drive letter or mount point to the selected volume
BREAK	Breaks a mirror set
CLEAN	Clears the configuration information or all information off the disk
CONVERT	Converts the disk from one format to another. This will allow you to convert the disk from dynamic to basic, basic to dynamic, MBR to GPT, or GPT to MBR.
CREATE	Creates a volume or partition
DELETE	Deletes a missing disk, selected volume, or selected partition
DETAIL	Provides details about a disk, partition, or volume
EXIT	Exits the program
EXTEND	Extends a volume
HELP	Prints a listing of Help commands
IMPORT	Imports a disk group
LIST	Prints a list of disks, partitions, or volumes
INACTIVE	Marks the current partition as an inactive partition
ONLINE	Marks as online a disk that is currently marked as offline
REM	Used to comment scripts
REMOVE	Removes a drive letter or mount point
REPAIR	Repairs a RAID-5 volume
RESCAN	Forces DISKPART to rescan the computer for disks and volumes
RETAIN	Places a retainer partition under a simple volume
SELECT	Moves the focus on an object

Partition Recovery Tools

- Deleting the partition is similar to removing the table of contents from a book; none of the information outside the table is missing, it just requires other methods to find it.
- *Partition recovery tools perform a number of automated tasks that will attempt to restore a damaged* or deleted partition, and/or restore data from that partition.
- Some of the automated tasks include:
  - ❑ Determining the error on the disk
  - ❑ Scanning the disk space for a partition boot sector or damaged partition information, and then attempting to reconstruct the partition table entry. By finding the partition boot sector, it will have all the information necessary to reconstruct the entry in the partition table.

- Because both NTFS and FAT32 volumes maintain backup boot sectors, the volume can be recovered by restoring the boot sector.

- Damaged partitions can occur from power or software failure, a root directory being damaged by a virus, formatting, and being deleted with tools such as FDISK, DISKPART, or the Disk Management tool in the Computer Management console.
- Problems can also occur when the partition table, MFT, root directory, or boot record is lost or corrupt.
- Each of these can cause Windows not to recognize the hard disk, requiring partition recovery tools to be used to recover the partition and data.
- A number of tools are available for partition recovery, each of which has various features that can make it easier to restore data that may have been lost from accidental deletion or damage to the partition.

Active@ Partition Recovery

- It recovers FAT12, FAT16, FAT32, and NTFS partitions and logical drives.

- It also provides the ability to create an image file of the drive to back up data on a disk, as well as back up MBR, partition table, and boot sectors, which can be restored after a problem occurs.

- It extensively scan the hard disk to locate deleted partitions and logical drives.

- Once they are detected, you can then undelete primary and extended partitions or logical drives to restore the data.

- This tool provides the ability to preview files and folders located on the deleted partition or drive before it’s recovered.

- Different versions of Active@ Partition Recovery software are available to use, including:

- **Active@ Partition Recovery for DOS,** which is a DOS-based version of the tool and is used if the system partition has been lost, or if the computer doesn’t boot in Windows.
- It is small enough to run from a bootable floppy, and supports IDE, ATA, and SCSI hard drives.

- **Active@ Partition Recovery for Windows**, which is the Windows-based version of the tool and is used if a nonsystem partition is lost, or when the computer boots in Windows.

- It can also be used to restore a deleted partition on a USB Flash Drive or memory card. It supports IDE, ATA, SATA, and SCSI drives.

Active@ Disk Image

- Active@ Disk Image is a DOS-based tool designed to completely back up and restore an image of your entire hard disk, FAT12, FAT16, FAT32, and NTFS partitions and logical drives.
- This tool allows you to create compressed images that contain a mirror of the drive's surface, or compressed data images that contain data stored in the clusters.
- You can preview the data stored in one or more image files before restoring them.

GetDataBack

- It will restore data from a variety of sources, including hard disks, memory cards,USB Flash Drives, iPods, and other media. Two versions of this software are available :

  ❑ GetDataBack for NTFS
  ❑ GetDataBack for FAT

- Each tool can be used on a remote computer, allowing you to connect over a network or serial cable to restore a damaged or deleted partition.
- This can be useful if you don't want to remove the drive and attach it to another computer, or use DOS-based tools to recover the partition.
- It provides a wizard-like interface that allows you to specify settings to optimize the recovery process, selecting whether to use default settings, whether damage was caused by partitioning software such as FDISK or by formatting the drive, or whether a new operating system was installed.
- If there is no problem with the partition, you can also set the tool to simply recover deleted files.

NTFS Deleted Partition Recovery

- NTFS Deleted Partition Recovery is a tool that is designed to recover partitions and perform other tasks to restore data that may have resulted in a loss of data.
- It can retrieve data from high level formatted, corrupted, or otherwise damaged partitions, as well as from other storage media such as ZIP drives, USB Flash Drives, memory cards, and so forth. It is available from www.techddi.com.

Handy Recovery

- Handy Recovery is a tool for recovering deleted, damaged, and formatted partitions, and is available from www.handyrecovery.com.
- Using this tool, you can search for files by name and restore entire folders and their contents.
- You can browse data on the disk, allowing you to see deleted files and folders with ones that haven't been deleted.
- It supports FAT12, FAT16, FAT32, and NTFS file systems, and will recover compressed and encrypted files stored on drives formatted as NTFS.
- It can also recover data from memory cards and other media. Each file that is displayed provides information on to the probability of successfully recovering it.

Acronis Recovery Expert

- Acronis Recovery Expert is another easy-to-use tool that recovers deleted or lost partitions which is available from www.acronis.com,
- It provides a series of wizards that take you step by step through the process of recovering data, and it supports FAT16, FAT32, NTFS, HPFS, Linux Ext2, Ext3, ReiserFS and Linux Swap file systems.
- It also provides features that allow you to work from bootable CDs and floppy disks, so you can recover system partitions or systems that fail to boot.

TestDisk

- TestDisk is a free tool that can be used to recover data and partitions that have been deleted or lost, and can run on a number of different systems including Windows NT/2000/XP/2003, Linux, FreeBSD, NetBSD, OpenBSD, SunOS, and Macintosh OS X.
- It has features to fix partition tables, recover FAT32 and NTFS boot sectors from a backup, and rebuild FAT12, FAT16, FAT32, and NTFS boot sectors.
- It can also locate Ext2 and Ext3 backup SuperBlocks and fix MFTs using an MFT mirror, and it provides other features that make it possible to recover partitions from a number of different systems. It is available from www.cgsecurity.org.

Scaven

- Scaven is a partition recovery tool that can perform multistring searches on hard disks, and recover deleted and lost data. It can recover data from accidentally formatted drives, drives with bad sectors, damaged MBRs, and lost partitions.

Recover It All!

- Recover It All! is a tool developed by DTIData, and is available from www.dtidata.com/recover_it_all.htm.

- It is designed to restore data lost from the disk, deleted files, and deleted or damaged partitions and boot sectors.

- It also provides an executable that will run from a floppy disk, allowing you to restore the partition even if the computer's operating system won't start, and will prevent overwriting data on the disk by installing the software.

Partition Table Doctor

- Partition Table Doctor is a partition recovery tool that checks and repairs the MBR, partition table, and boot sector, and recovers damaged or deleted data from FAT16, FAT32, NTFS, Ext2, Ext3, and Linux Swap partitions on IDE, ATA, SATA, SCSI, and removable hard disk drives.

- It provides features to browse the contents of a disk, and allows you to back up and restore the MBR, partition table, and boot sector. It is available from www.ptdd.com.

Data Acquisition and Duplication

- Electronic evidence is fragile by nature, and can easily be modified, damaged, or destroyed.

- Even booting a computer can erase temporary files, modify timestamps, or alter other data in addition to writing data and creating new files to the drive using the boot process.

- Beyond this, a computer could be booby trapped so that if a set of keys wasn't pressed at bootup or an incorrect password was entered, a program or script could run to reformat the hard disk or overwrite certain data, making retrieval of evidence more difficult or impossible.

- Because of this, data must be acquired or duplicated from a hard disk before any analysis takes place.

- *Data acquisition is the act or process of gathering information and* evidence.

- In computer forensics, data acquisition means using established methods to acquire data from a suspect computer or storage medium to gain insight into a crime or other incident, and potentially use it as evidence to convict a suspect.

- Another goal of data acquisition is to preserve evidence, so any tools that are used should not alter the data in any way, and should provide an exact duplicate.

- To prevent contamination, any data that is duplicated should be stored on forensically sterile medium, meaning that the disk has no other data on it, and has no viruses or defects.

- To effectively examine data on a suspect machine, a person performing a forensic examination of a machine needs to create an *image of the disk.*

- *When you create a disk image (a bitstream* copy), each physical sector of the disk is copied so that the data is distributed in the same way, and then the image is compressed into a file called an *image file*.

- *This image is exactly like the original,* both physically and logically.

- As an exact duplicate of the data on a suspect machine or storage medium, the mirror image includes hidden files, temp files, corrupted files, file fragments, and erased files that have not yet been overwritten. In other words, every binary digit is duplicated exactly.

- This is different from other methods that may be used to duplicate data for disaster recovery or other purposes where every scrap of data isn't necessary.

  For example, when tools to back up a hard disk are used, the only data duplicated is that which is visible to the file system.

- Similarly, a disk image may be created as a method of backing up a system

- If a disaster occurred and/or data needed to be restored, the backup or image could be used to recover data and get systems back online quickly.

- From the perspective of someone performing an investigation, backups on magnetic tape or image files stored to disks can be a useful source of evidence.

- Most organizations will have a regimen of nightly backups, in which data stored on servers and certain other computers on the network will be copied to magnetic tape or other storage media.

- Even individuals may back up important data to a disk or location on the network, creating an image of any data that was saved to the disk over a period of time.

- This can be important to an investigation, as a investigator can provide a timeline of what data was saved to certain files at what time.

  For example, if someone was embezzling from a company, it can be seen what entries that person added, deleted, and modified in a spreadsheet or database on a given day by restoring versions of the file from different backups.

- A number of tools can be used to duplicate data stored on magnetic tapes, and tools to mount an image file created with various types of software.

- By analyzing a duplicate of the image or backup, investigator can find important evidence without altering the original media or file.

- In an investigation, however, most of the time you'll need to use software to create an image of a hard disk, CDs, DVDs, floppy disks, USB Flash Drives, memory cards from digital cameras, and other storage media.

- The bitstream copy will contain all of the data stored on the device or removable media, and can later be analyzed for potential evidence.

- Because you don't boot from the hard disk of a computer you're investigating, you need to connect the computer you're using (with forensic software installed) to the suspect's machine via a network cable or serial cable.

- Once you've created a physical connection to the computer, you can then run the forensic software and create an image of the machine's hard disk.

- Forensic software may include a special program that can run from a bootable floppy, or be small enough to fit on a bootable CD or floppy.

- Upon booting from the CD or floppy, the program on the floppy or CD is run.

- Depending on the program, it may connect to the forensic software on your computer so that it can then make an exact image of the disk, or it may simply write the image file to your computer.

- Alternatively, you could also remove the hard disk from a suspect computer and connect it to your computer or to a device that provides write protection.

- Write protection prevents data from being written to the disk that you’re duplicating.

- When using any forensic software, it is always advisable to use hardware-based write-blocking.

- The hardware prevents the forensic software and the operating system you’re using from altering data on the suspect hard disk when you attach the hard drive to your computer.

- Once the hard disk is connected to your computer in this way, you can then begin running the forensic software so that a duplicate of the data is written to an image file on your machine.

- Once the image is created, you can then use the forensic software or other tools to mount the image. This allows the software to display the contents of the machine, and will allow you to view any data that exists on the machine from which it was acquired.

- Any software being used should mount the image as a read-only volume, so there is no way that any changes can be made to the data i.e. it will retain their original timestamps and other attributes.

- This allows you to view data in areas of the disk, including partition information, sectors, files stored on the machine, the directory structure, and other information.

Data Acquisition Tools

- A number of tools for forensic acquisition and analysis are available today.

- In deciding which tools to use, you should ensure that they do not modify data.

- You should also evaluate the reputations of these tools, and whether they have previously been accepted in court.

  For example: FTK Imager, EnCase has been widely accepted, so there would be less of a chance of it being heavily scrutinized.

- Because testifying in court can be stressful and you don't want to waste time justifying the tools you used to acquire evidence.

- Although you may still need to validate the tool that was used, using tools that are widely accepted and previously accepted can make the process easier in the court.

FTK Imager

- FTK Imager is an imaging tool developed by AccessData (www.accessdata.com) that allows to preview data and assess potential evidence on a machine.

- Using this tool, a forensic image of the data can be made, duplicating everything on the machine so that there is no chance of modifying the original data.

- By previewing the contents of the image and reviewing the duplicated data, It can be determined whether additional analysis is required using the Forensic Toolkit (FTK).

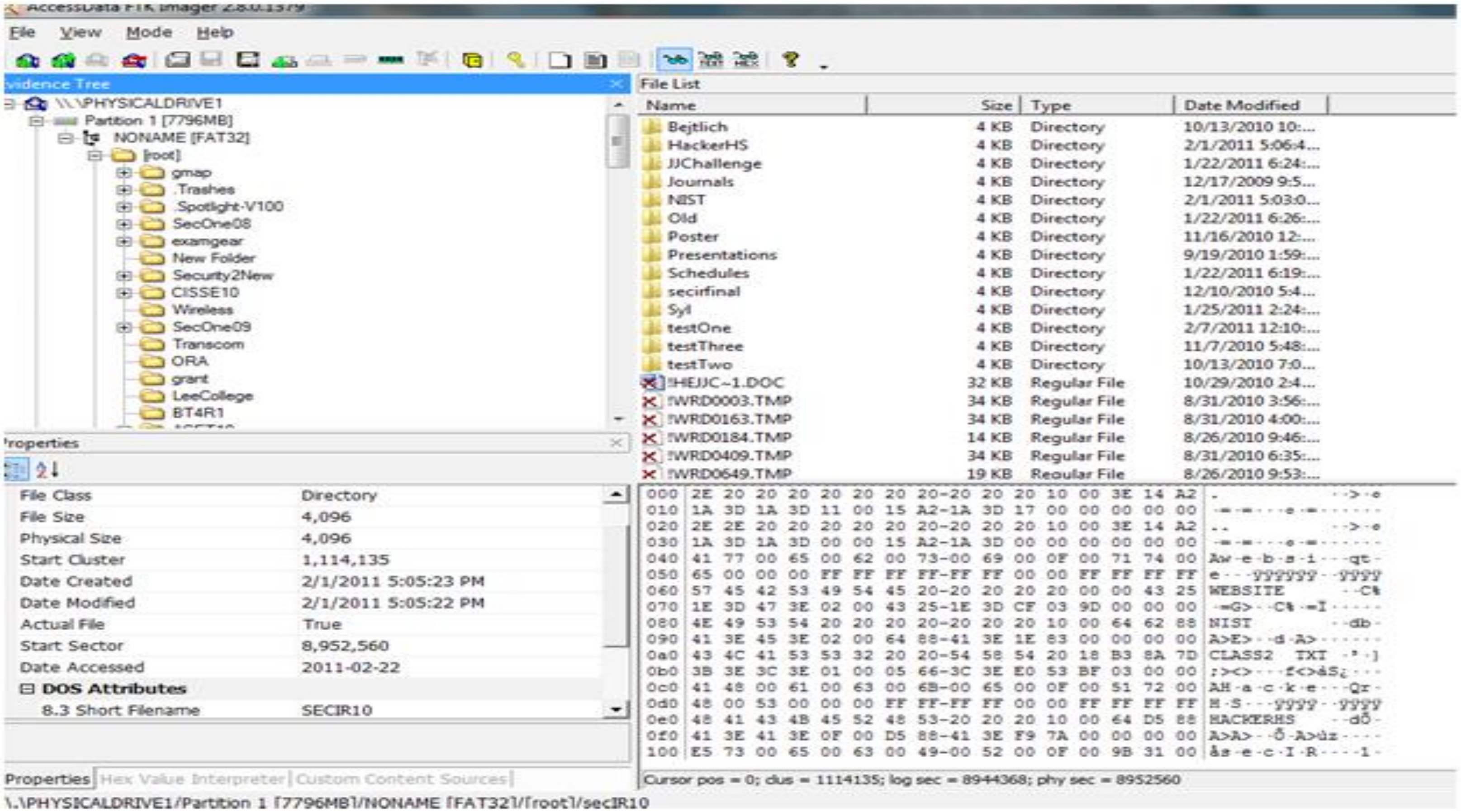
- Using FTK, you can view forensic images of hard disks, floppy disks, CDs, DVDs, and other storage media that was created with FTK Imager, or you can view images created with other tools.

- It will read image files created with ICS (Intelligent Computer System-Image MaSSter), SafeBack, and forensic, uncompressed images created with Ghost, and read or write image files in EnCase, dd Raw, SMART, and FTK image formats.

- This is particularly useful in situations such as when an internal investigation was conducted, a forensic image was created from a suspect computer, and police now need to view the evidence that was acquired.

- In addition to the image file formats that can be made for analyzing disks, there are also a number of file formats that can be read and created for CD and DVD forensics. These include ISOBuster CUE, CloneCD, Alcohol, PlexTools, Virtual CD, and many others.

- As shown in Figure, FTK Imager provides an easy-to-use interface.
- Once an evidence file is opened, you can view the folder structure in the Evidence Tree, located in the upper left-hand pane.
- By selecting a folder, you can then view files stored in that folder in the File List, located in the upper-right pane.
- To preview a particular file, you can select it in the upper pane, and view an image of pictures, hexadecimal data, text, and previews of other data in the lower right-hand pane.
- You can view additional information on the file, including any DOS attributes the file might have, in the Properties pane in the lower left-hand side of the screen.



Name	Size	Type	Date Modified
Bejtlich	4 KB	Directory	10/13/2010 10:...
HackerHS	4 KB	Directory	2/1/2011 5:06:4...
JJChallenge	4 KB	Directory	1/22/2011 6:24:...
Journals	4 KB	Directory	12/17/2009 9:5...
NIST	4 KB	Directory	2/1/2011 5:03:0...
Old	4 KB	Directory	1/22/2011 6:26:...
Poster	4 KB	Directory	11/16/2010 12:...
Presentations	4 KB	Directory	9/19/2010 1:59:...
Schedules	4 KB	Directory	1/22/2011 6:19:...
secirfinal	4 KB	Directory	12/10/2010 5:4...
Syl	4 KB	Directory	1/25/2011 2:24:...
testOne	4 KB	Directory	2/7/2011 12:10:...
testThree	4 KB	Directory	11/7/2010 5:48:...
testTwo	4 KB	Directory	10/13/2010 7:0...
!HEJJC~1.DOC	32 KB	Regular File	10/29/2010 2:4...
!WRD0003.TMP	34 KB	Regular File	8/31/2010 3:56:...
!WRD0163.TMP	34 KB	Regular File	8/31/2010 4:00:...
!WRD0184.TMP	14 KB	Regular File	8/26/2010 9:46:...
!WRD0409.TMP	34 KB	Regular File	8/31/2010 6:35:...
!WRD0649.TMP	19 KB	Regular File	8/26/2010 9:53:...

File Class	Directory
File Size	4,096
Physical Size	4,096
Start Cluster	1,114,135
Date Created	2/1/2011 5:05:23 PM
Date Modified	2/1/2011 5:05:22 PM
Actual File	True
Start Sector	8,952,560
Date Accessed	2011-02-22
⊟ **DOS Attributes**	
8.3 Short Filename	SECIR10

```
000 2E 20 20 20 20 20 20 20-20 20 20 10 00 3E 14 A2  .           ··>·e
010 1A 3D 1A 3D 11 00 15 A2-1A 3D 17 00 00 00 00 00  ·=·=···e·=······
020 2E 2E 20 20 20 20 20 20-20 20 20 10 00 3E 14 A2  ..          ··>·e
030 1A 3D 1A 3D 00 00 15 A2-1A 3D 00 00 00 00 00 00  ·=·=···e·=······
040 41 77 00 65 00 62 00 73-00 69 00 0F 00 71 74 00  Aw·e·b·s·i···qt·
050 65 00 00 00 FF FF FF FF-FF FF 00 00 FF FF FF FF  e···ÿÿÿÿÿÿ··ÿÿÿÿ
060 57 45 42 53 49 54 45 20-20 20 20 00 00 43 25     WEBSITE     ··C%
070 1E 3D 47 3E 02 00 43 25-1E 3D CF 03 9D 00 00 00  ·=G>··C%·=Ï·····
080 4E 49 53 54 20 20 20 20-20 20 20 10 00 64 62 88  NIST        ··db·
090 41 3E 45 3E 02 00 64 88-41 3E 1E 83 00 00 00 00  A>E>··d·A>······
0a0 43 4C 41 53 53 32 20 20-54 58 54 20 18 B3 8A 7D  CLASS2  TXT ·³·}
0b0 3B 3E 3C 3E 01 00 05 66-3C 3E E0 53 BF 03 00 00  ;><>···f<>àS¿···
0c0 41 48 00 61 00 63 00 6B-00 65 00 0F 00 51 72 00  AH·a·c·k·e···Qr·
0d0 48 00 53 00 00 00 FF FF-FF FF 00 00 FF FF FF FF  H·S···ÿÿÿÿ··ÿÿÿÿ
0e0 48 41 43 4B 45 52 48 53-20 20 20 10 00 64 D5 88  HACKERHS    ··dÕ·
0f0 41 3E 41 3E 0F 00 D5 88-41 3E F9 7A 00 00 00 00  A>A>··Õ·A>ùz····
100 E5 73 00 65 00 63 00 49-00 52 00 0F 00 9B 31 00  ås·e·c·I·R····1·
```

Cursor pos = 0; clus = 1114135; log sec = 8944368; phy sec = 8952560

\\.\PHYSICALDRIVE1/Partition 1 [7796MB]/NONAME [FAT32]/[root]/secIR10

- Using FTK imager to create a forensic image is relatively easy, as seen in the step-by-step instructions provided here, which outline how to acquire data from a CD/DVD or floppy. You would follow similar steps to acquire data from other media.

1. Once FTK Imager has been installed, from the Windows **Start menu, select Programs | AccessData | FTK Imager and then click on the FTK Imager menu item.**
2. When the programs open, click on the **File menu, and then click on the Add Evidence Item menu item.**
3. When the **Select Source dialog box appears, click on the option labeled Logical Drive.** Click the **Next button.**
4. When the **Select Drive dialog box appears, select the drive containing your floppy disk** or CD. Click **Finish.**
5. When the **Create Image dialog box appears, click Add.**
6. When the **Select Image Destination dialog box appears, specify where the image file** will be stored by entering a path into the field labeled **Image destination folder.**
7. In the field labeled **Image filename, enter the name you'd like to give the file without an** extension. Click **Finish.**
8. When the **Create Image dialog box appears again, click Start.**
9. Wait while FTK Imager creates a forensic image file of the data on the drive you specified. This may take several minutes. Once the **Status field indicates *Image created successfully,*** click the **Close button.**

Recovering Data from Backups

- **BACKUPS:** Often made for fault-tolerance purposes are- overlooked source of data recovery as they can be especially useful in cases where the cybercriminal might have been savvy enough to destroy data completely.
- There are several possible sources of backups that a suspect or system administrator might have created for fault-tolerance purposes:

1. **External Hard Drives or SSDs**: Individuals or system administrators may regularly back up data to external storage devices such as USB hard drives or solid-state drives (SSDs).
2. **Network-Attached Storage (NAS)**: In a networked environment, system administrators often use NAS devices to store backups centrally. These devices can be accessed by multiple computers on the network and provide a convenient backup solution.
3. **Cloud Storage Services**: Individuals and organizations increasingly rely on cloud storage services such as Google Drive, Dropbox, Microsoft OneDrive, or Amazon S3 for data backup and synchronization. Data can be automatically backed up to these services over the internet.
4. **On-Premises Backup Servers**: Some organizations maintain dedicated backup servers or appliances on-site to store backups of critical data. These servers may use technologies like RAID for fault tolerance.
5. **Tape Backup Systems**: Although less common than in the past, tape backup systems are still used by some organizations for long-term data retention and disaster recovery purposes.
6. **Disk Imaging Software**: System administrators may create disk images of computers or servers using specialized software. These disk images can be stored on various storage media for backup and recovery purposes.
7. **Virtual Machine Snapshots**: In virtualized environments, administrators often take snapshots of virtual machines to capture their state at a specific point in time. These snapshots can serve as backups in case of system failures or data corruption.
8. **Offline Storage Media**: Some individuals or organizations may store backups on offline storage media such as DVDs, Blu-ray discs, or magnetic tapes for long-term archival purposes.
9. **Backup Policies and Procedures**: Organizations typically have backup policies and procedures in place to ensure regular backups of critical data. These policies may include guidelines on backup frequency, retention periods, and verification processes.
10. **Mobile Devices**: Individuals may back up data from their mobile devices (such as smartphones and tablets) to cloud services or local computers for fault tolerance and data recovery purposes.

- You should request that the search warrant specify seizure of any tapes, disks, CD-ROMs, or other media commonly used to back up files, in addition to the computer equipment itself.

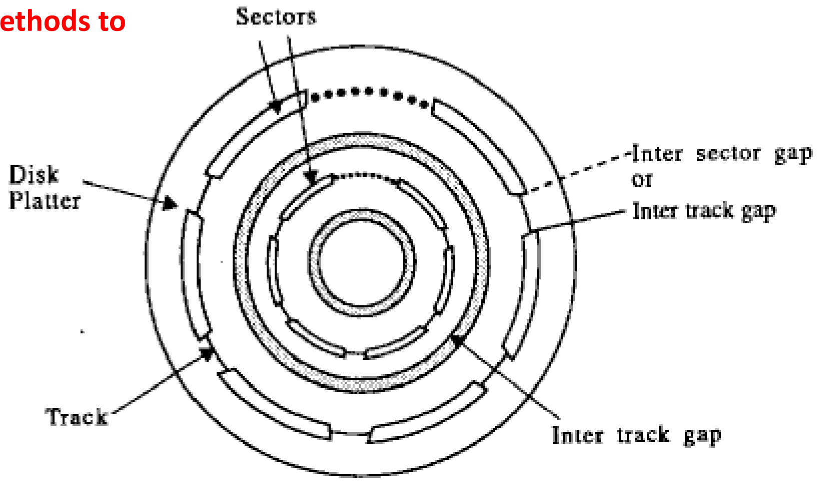
Finding Hidden Data

In many instances, data hidden on the hard disk can be very useful to investigators in building a case against a cybercrime suspect.

Some of this data might be ambient data . For example: data that was left behind when files were deleted or disks were repartitioned, data in rams , slacks etc.

Technically savvy individuals or cyber crime criminals can employ various methods to hide data or disguise its existence on a storage device

1. **Disk Editors**: Disk editing software allows users to directly manipulate the contents of a disk's sectors, bypassing the file system. Criminals may use disk editors to overwrite data in unused sectors or to hide sensitive information within existing files or sector gaps.
2. **Steganography Software**: Steganography is the practice of concealing messages or data within other non-secret data. Specialized steganography software enables users to embed hidden messages or files within images, audio files, or other media, making it difficult to detect without the proper decryption key or knowledge of the steganographic method used.
3. **Renaming Extensions**: Criminals may change file extensions to disguise the true nature of files. For example, they might rename an executable file (.exe) to have a .txt extension to make it appear as a harmless text document.
4. **Hidden Partitions**: Advanced users can create hidden partitions on storage devices, which are not readily visible through standard file system browsing tools. These hidden partitions can contain sensitive data that is not easily accessible to investigators.
5. **Encryption**: Encrypting files or entire storage devices with strong encryption algorithms can render the data unreadable without the correct decryption key. Criminals may use encryption to protect sensitive information from unauthorized access.
6. **Data Fragmentation**: Criminals may intentionally fragment files and scatter the fragments across the storage device to make it more challenging to recover the original data. This technique can thwart traditional file recovery methods that rely on contiguous data blocks.
7. **Alternate Data Streams (ADS)**: On NTFS file systems used in Windows, alternate data streams allow additional data to be associated with a file without changing its size or attributes visibly. Criminals may use ADS to hide information within legitimate files.
8. **Unused Disk Space**: Criminals may store data in unused portions of a storage device, such as unallocated disk space or slack space within files. This technique can make it difficult to detect the presence of hidden data without specialized forensic tools.



- A *disk sector is a unit of space of a fixed size (such as 512 bytes). Older hard disks could have some* wasted storage space on the outside tracks because of the way the disks are divided into sectors that contain an equal number of sectors per track.
- The discrepancy in circumference between the inside and outside tracks causes this wasted space.
- It is possible in some cases to hide data in the space between sectors on the larger outside tracks. This space is called the *sector gap*.

Slack

- Another place that data can be hidden is in the *slack space caused by file sizes that don’t exactly* match the size of the clusters in which they are stored.

- Cluster sizes can vary, but anytime a file or portion of a file is smaller than the cluster size, the “leftover” bits in that cluster go unused.

- Clusters are made up of sectors.

- When the file is too small to fill up the last sector in a file, DOS and Windows use random data from the system’s memory buffers to make up the difference.

- This is called *RAM slack and can result in data from the* work session (the time since the computer was last booted) being stored on the disk in this slack space to “pad” the final sector.

- All sorts of data dumped from memory can be lurking in the slack space and could prove useful to the investigator.

- Any kind of disk (diskette, hard disk, and removable disk) is subject to slack. Computer forensic analysis tools can recover data hidden in slack areas.

- *Shadow data is created in magnetic disks because the vertical and horizontal alignments of the mechanical heads* that write to the disk are not exactly the same each time a write operation is performed.

- "Shadow data" refers to residual magnetic fields or remnants of previously written data that may still be faintly detectable on magnetic disks even after the data has been overwritten.

- This means that even when data is overwritten, remnants of the old data could still be there. It is sometimes possible (although very time-consuming and expensive) to reconstruct the data from these remnants.

Detecting Steganographic Data

- Steganalysis and steganography are the two different sides of the same coin. Steganography tries to hide messages in plain sight while steganalysis tries to detect their existence or even more to retrieve the embedded data.

- Steganography software hides files within other files, using empty space or the least significant bit to encode messages.

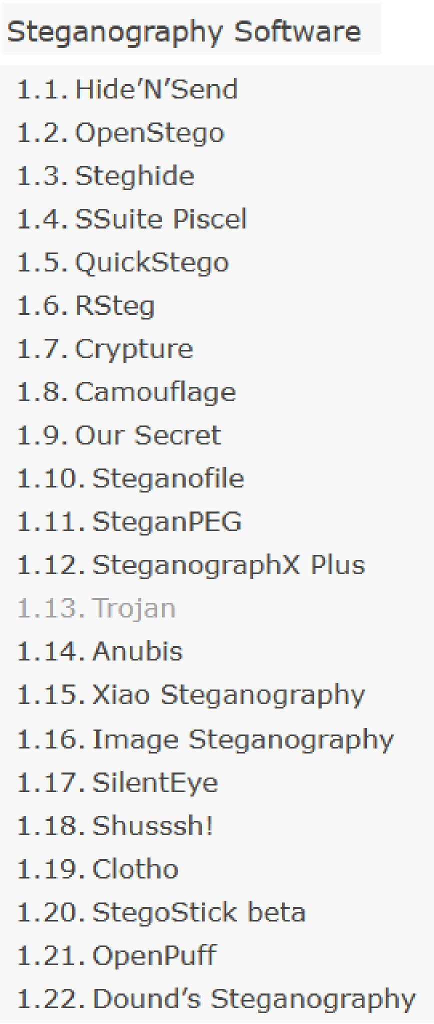
- The entire file that you want to hide is broken up into its binary components, and these are then concealed in different parts of the photo image pixel values.

  For example: data can be hidden within an image file by slightly altering a single bit related to a particular pixel. If one pixel in the photo has a red component, represented by the binary number 10001100, the least significant bit (the last one) can be changed to a 1, making the binary 10001101. This will make that one pixel a tiny bit redder, which will not be noticeable to viewers. This creates one "hidden" bit, a 1. To create a 0, you would leave the least significant bit as it was.

- Determining which pixels contain the hidden bits, and in what order, can be done by a random number generator that uses a key so that only someone who knows the key will be able to reconstruct the hidden message by retrieving the hidden bits in the correct order.

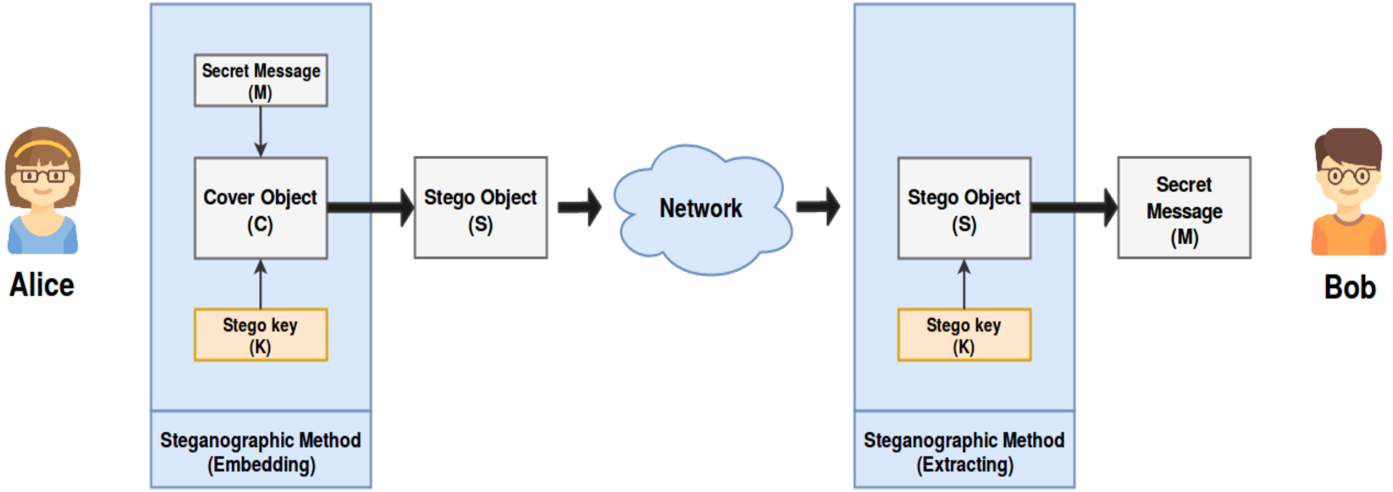
- Several "anti-steganography" tools (such as StegoHunt, StegoCommand, Discover the Hidden, StegoSuite) allow you to detect the presence of stego data that is hidden within other files using steganographic techniques.

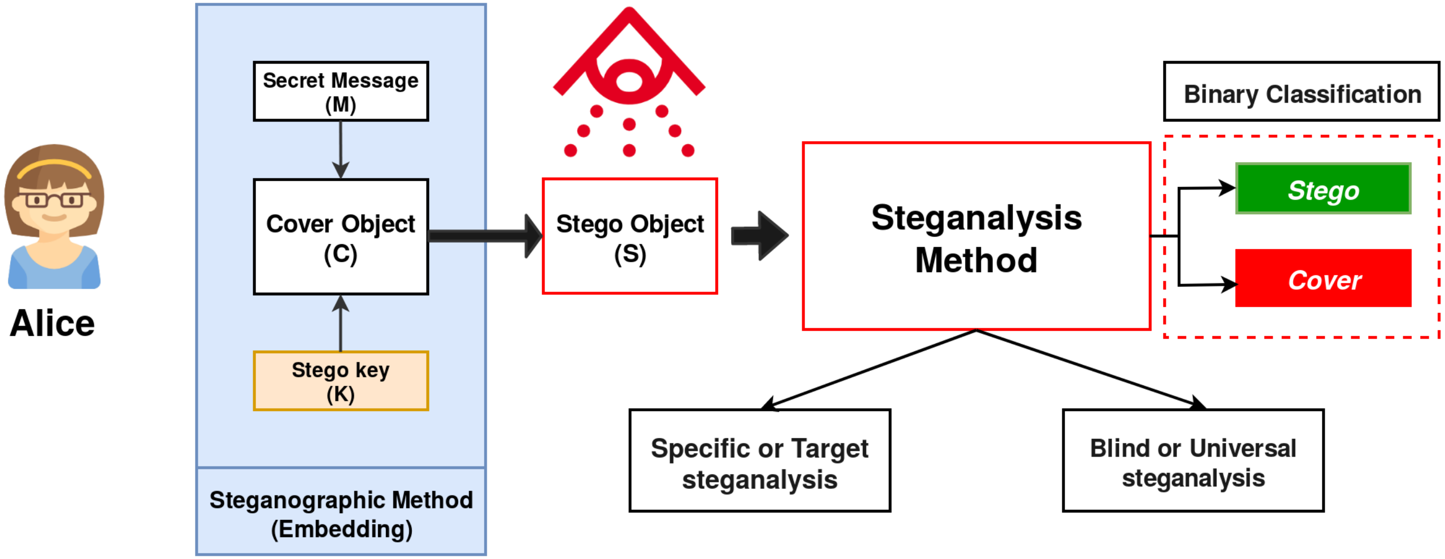
- Detecting the presence of steganographic data is usually done by software that checks the statistical profile of an image and looks for statistical artifacts left by steganographic software.

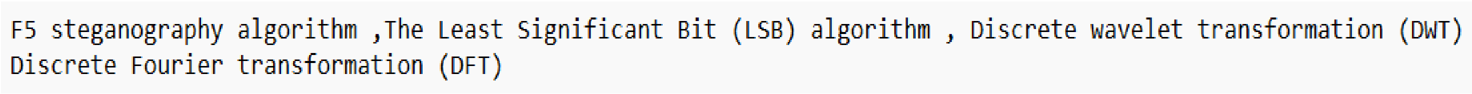


Steganography Software

1.1. Hide’N’Send
1.2. OpenStego
1.3. Steghide
1.4. SSuite Piscel
1.5. QuickStego
1.6. RSteg
1.7. Crypture
1.8. Camouflage
1.9. Our Secret
1.10. Steganofile
1.11. SteganPEG
1.12. SteganographX Plus
1.13. Trojan
1.14. Anubis
1.15. Xiao Steganography
1.16. Image Steganography
1.17. SilentEye
1.18. Shusssh!
1.19. Clotho
1.20. StegoStick beta
1.21. OpenPuff
1.22. Dound’s Steganography





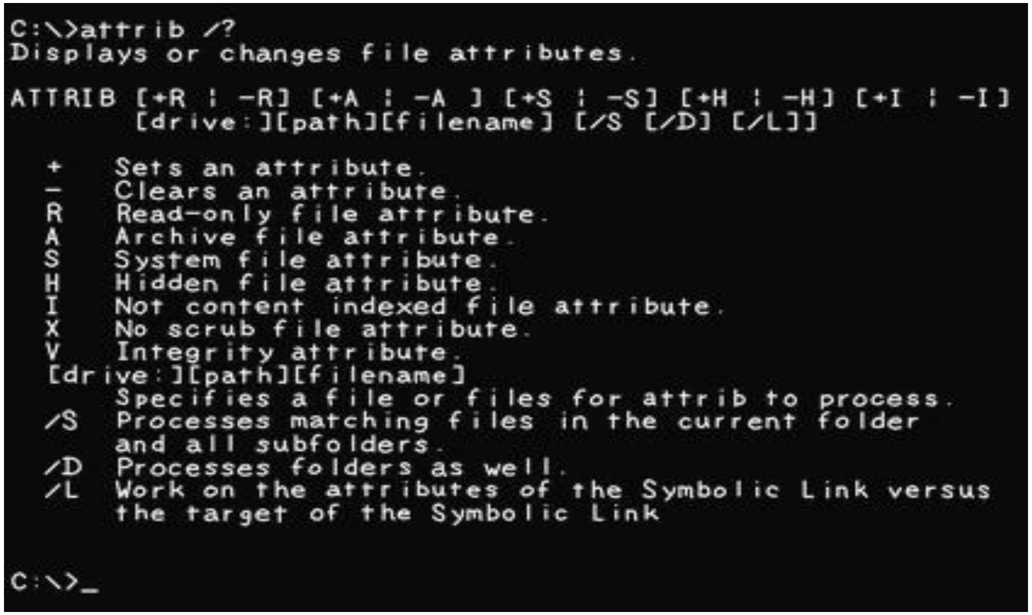


```
F5 steganography algorithm ,The Least Significant Bit (LSB) algorithm , Discrete wavelet transformation (DWT)
Discrete Fourier transformation (DFT)
```

Blind steganalysis techniques detect the existence of secret messages embedded in digital media when the steganography embedding algorithm is unknown.

Methods for Hiding Files

- Files can be hidden on a system in a number of ways.
- On DOS/Windows file systems, setting the hidden attribute (*–h at the command line, or set in the File Properties dialog box in the GUI) will* prevent the file from showing up in response to the *DIR command at the command line or in the* files list in Explorer if the default settings are in place in **Folder Options | View**. However, if the Show Hidden Files and Folders option button is enabled, these hidden files will still be displayed.
- **drive letter : \ >attrib –H –R –S /S /D *.***.



```
C:\>attrib /?
Displays or changes file attributes.

ATTRIB [+R | -R] [+A | -A ] [+S | -S] [+H | -H] [+I | -I]
       [drive:][path][filename] [/S [/D] [/L]]

  +   Sets an attribute.
  -   Clears an attribute.
  R   Read-only file attribute.
  A   Archive file attribute.
  S   System file attribute.
  H   Hidden file attribute.
  I   Not content indexed file attribute.
  X   No scrub file attribute.
  V   Integrity attribute.
  [drive:][path][filename]
      Specifies a file or files for attrib to process.
  /S  Processes matching files in the current folder
      and all subfolders.
  /D  Processes folders as well.
  /L  Work on the attributes of the Symbolic Link versus
      the target of the Symbolic Link

C:\>_
```

- On UNIX systems, files and directories with names that begin with a dot are hidden and are not displayed in response to the *ls command unless you use the –a switch.*

- **Another method** for hiding files is known as *hiding in plain view.* Using this method, a cybercriminal gives a file a name that makes it appear to be something it isn't—and something that the investigator would not be interested in.

  For example, a objectionable graphics file containing could be renamed to something like window.sys and stored in the Windows system directory. To the casual observer, it looks like just another operating system file. When the criminal wants to access it, he merely has to change the file extension back to .jpg or .gif and open it in any graphics viewer program.

- Another way to hide files is to use areas of the hard disk that normally aren’t visible. The Host Protected Area or Hidden Protected Area (HPA) is an area of the hard disk that normally isn’t visible to an operating system.

- An HPA may be used to store utilities, diagnostic tools, or programs used when the computer is first powered up. Many computer manufacturers use this space to store software.

- For example, Computer manufacturers may use the area to contain a preloaded OS for install and recovery purposes (instead of providing DVD or CD media). Dell notebooks hide Dell MediaDirect utility in HPA. IBM ThinkPad and HP, LG notebooks hide system restore software in HPA.

- If this hidden partition of the hard disk exists, and is known to the user of the computer, it may be used to store illegal or sensitive materials that may be relevant to your case.

- Tools such as X-Ways Forensics, OSForensics can detect these protected areas, allowing you to access any data that may be stored there.

Locating Forgotten Evidence

- A great deal of data is stored on computers automatically by application programs and/or the operating system.

- Some users are unaware of this stored data; others know about it but might forget to get rid of it when they are destroying evidence on a system.

- Depending on the nature of the offense, some of this data could be useful to the cybercrime investigator.

- Sources of forgotten evidence include Web caches, temporary (temp) files, swap/page files, and application logs.

Web Caches and URL Histories

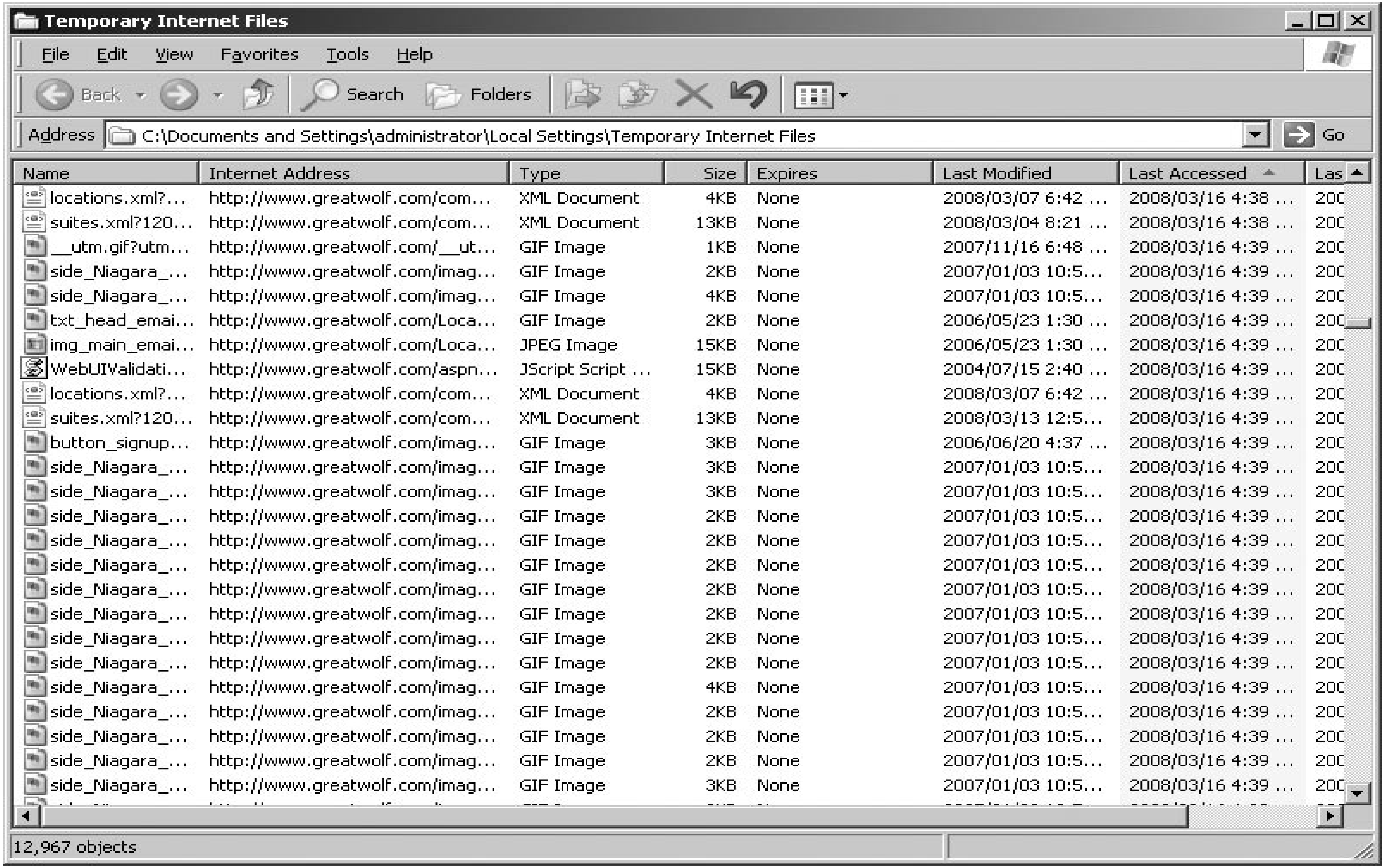
- **Web browsers by default *cache the pages that a user visits,*** *along with related* graphics, sounds, and other embedded files, so that if user visit the same page again, it can be quickly retrieved from the disk.

- These files are usually called *temporary Internet files and are stored in a special folder, usually under the user's profile* name.

  "%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cache"
  "%LOCALAPPDATA%\Mozilla\Firefox\Profiles[profilename].default\Cache"

- This information can be especially useful in cyber stalking , child pornography cases or cases with need of identifying frequently visited or specific Web sites.

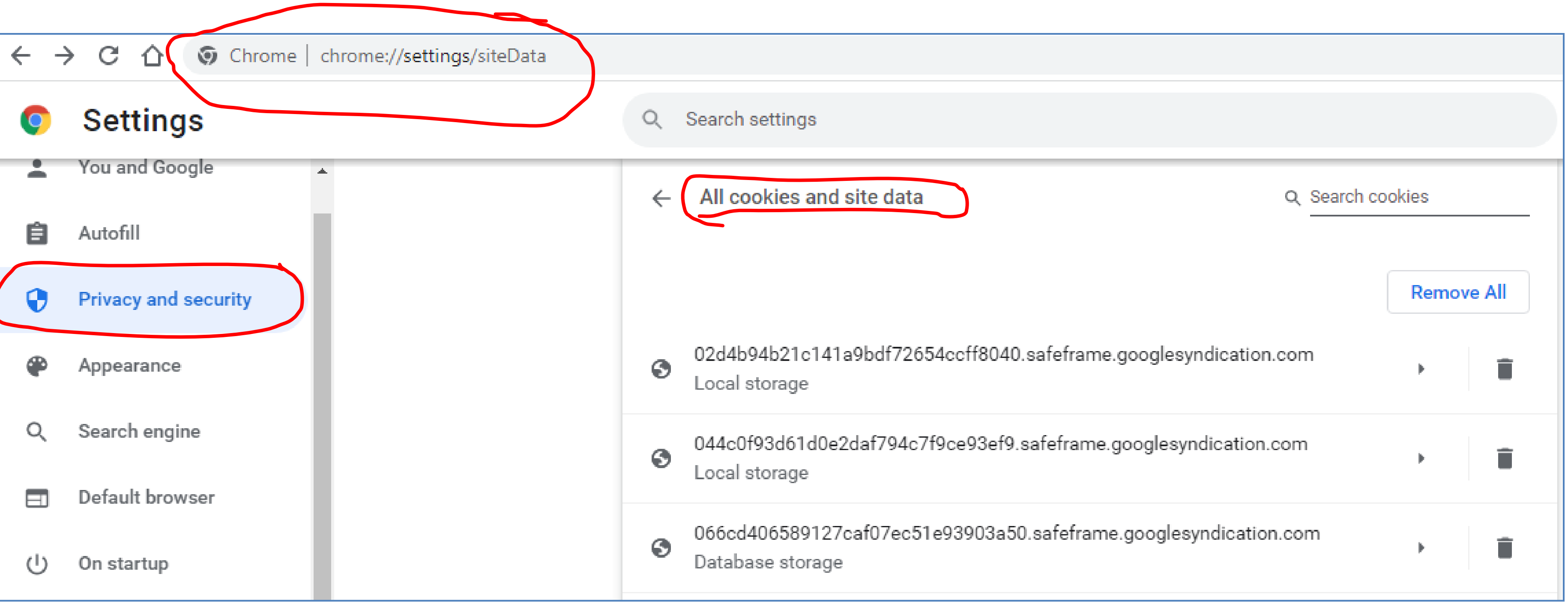
- Temporary Internet Files (the Web Cache), which can provide clues to the web sites a computer user has recently visited .



C:\Documents and Settings\administrator\Local Settings\Temporary Internet Files

Name	Internet Address	Type	Size	Expires	Last Modified	Last Accessed	Las
locations.xml?...	http://www.greatwolf.com/com...	XML Document	4KB	None	2008/03/07 6:42 ...	2008/03/16 4:38 ...	200
suites.xml?120...	http://www.greatwolf.com/com...	XML Document	13KB	None	2008/03/04 8:21 ...	2008/03/16 4:38 ...	200
__utm.gif?utm...	http://www.greatwolf.com/__ut...	GIF Image	1KB	None	2007/11/16 6:48 ...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	4KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
txt_head_emai...	http://www.greatwolf.com/Loca...	GIF Image	2KB	None	2006/05/23 1:30 ...	2008/03/16 4:39 ...	200
img_main_emai...	http://www.greatwolf.com/Loca...	JPEG Image	15KB	None	2006/05/23 1:30 ...	2008/03/16 4:39 ...	200
WebUIValidati...	http://www.greatwolf.com/aspn...	JScript Script ...	15KB	None	2004/07/15 2:40 ...	2008/03/16 4:39 ...	200
locations.xml?...	http://www.greatwolf.com/com...	XML Document	4KB	None	2008/03/07 6:42 ...	2008/03/16 4:39 ...	200
suites.xml?120...	http://www.greatwolf.com/com...	XML Document	13KB	None	2008/03/13 12:5...	2008/03/16 4:39 ...	200
button_signup...	http://www.greatwolf.com/imag...	GIF Image	3KB	None	2006/06/20 4:37 ...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	3KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	3KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	4KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	2KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200
side_Niagara_...	http://www.greatwolf.com/imag...	GIF Image	3KB	None	2007/01/03 10:5...	2008/03/16 4:39 ...	200

12,967 objects



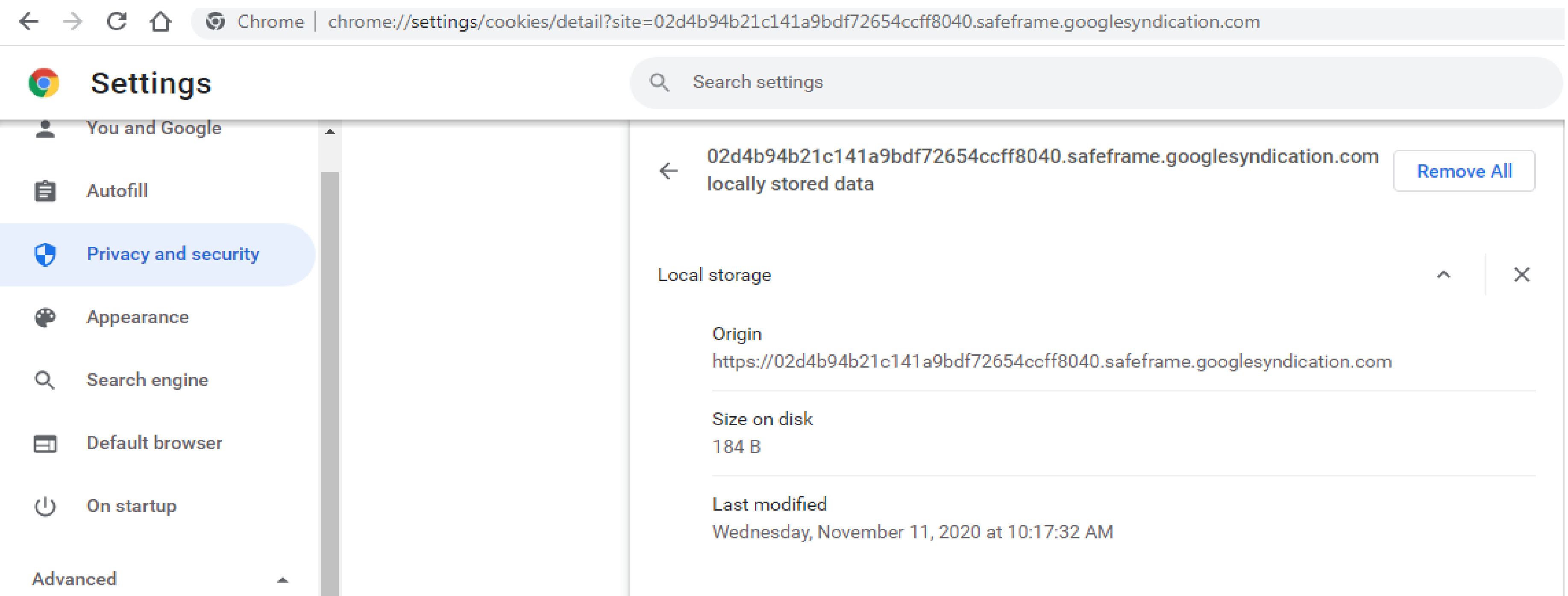
chrome://settings/siteData

All cookies and site data

02d4b94b21c141a9bdf72654ccff8040.safeframe.googlesyndication.com
Local storage

044c0f93d61d0e2daf794c7f9ce93ef9.safeframe.googlesyndication.com
Local storage

066cd406589127caf07ec51e93903a50.safeframe.googlesyndication.com
Database storage



chrome://settings/cookies/detail?site=02d4b94b21c141a9bdf72654ccff8040.safeframe.googlesyndication.com

02d4b94b21c141a9bdf72654ccff8040.safeframe.googlesyndication.com locally stored data

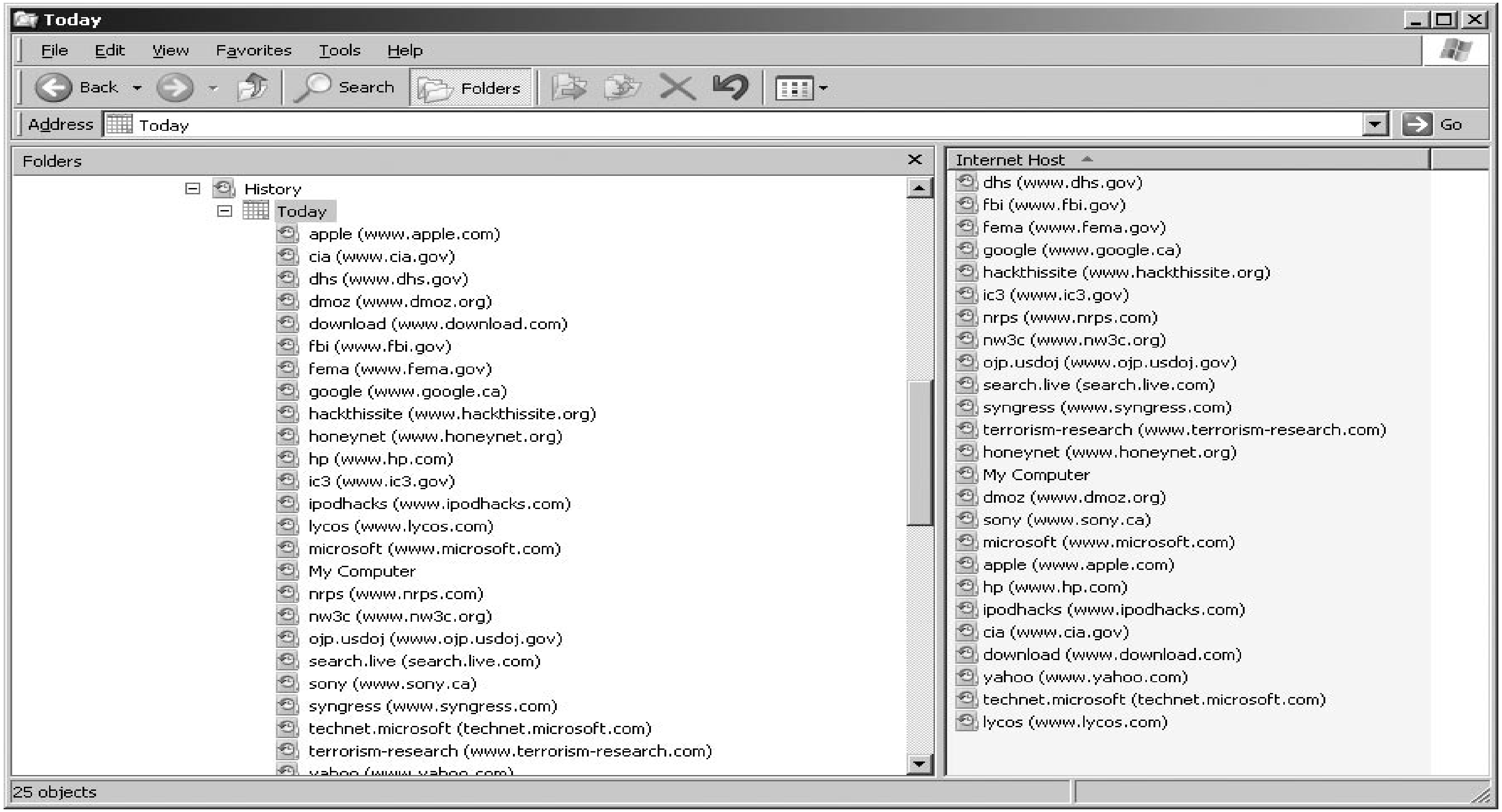
Local storage

Origin
https://02d4b94b21c141a9bdf72654ccff8040.safeframe.googlesyndication.com

Size on disk
184 B

Last modified
Wednesday, November 11, 2020 at 10:17:32 AM

- Another source of information about Web sites that have been visited is the History folder.
- Cybercriminals sometimes delete their temporary Internet files but forget to clear the history records.
- Unlike the Web cache, the History folder doesn't contain actual copies of the Web pages; instead, it contains a list of links (URLs) to those sites.



```
apple (www.apple.com)
cia (www.cia.gov)
dhs (www.dhs.gov)
dmoz (www.dmoz.org)
download (www.download.com)
fbi (www.fbi.gov)
fema (www.fema.gov)
google (www.google.ca)
hackthissite (www.hackthissite.org)
honeynet (www.honeynet.org)
hp (www.hp.com)
ic3 (www.ic3.gov)
ipodhacks (www.ipodhacks.com)
lycos (www.lycos.com)
microsoft (www.microsoft.com)
My Computer
nrps (www.nrps.com)
nw3c (www.nw3c.org)
ojp.usdoj (www.ojp.usdoj.gov)
search.live (search.live.com)
sony (www.sony.ca)
syngress (www.syngress.com)
technet.microsoft (technet.microsoft.com)
terrorism-research (www.terrorism-research.com)
yahoo (www.yahoo.com)
```

```
dhs (www.dhs.gov)
fbi (www.fbi.gov)
fema (www.fema.gov)
google (www.google.ca)
hackthissite (www.hackthissite.org)
ic3 (www.ic3.gov)
nrps (www.nrps.com)
nw3c (www.nw3c.org)
ojp.usdoj (www.ojp.usdoj.gov)
search.live (search.live.com)
syngress (www.syngress.com)
terrorism-research (www.terrorism-research.com)
honeynet (www.honeynet.org)
My Computer
dmoz (www.dmoz.org)
sony (www.sony.ca)
microsoft (www.microsoft.com)
apple (www.apple.com)
hp (www.hp.com)
ipodhacks (www.ipodhacks.com)
cia (www.cia.gov)
download (www.download.com)
yahoo (www.yahoo.com)
technet.microsoft (technet.microsoft.com)
lycos (www.lycos.com)
```

Temp Files

- Applications such as Microsoft Word create temporary (temp) files on a system.

- These files are used for tracking changes made to the original and for recovery if the program crashes.

- Working on a Word document can result in dozens of temp files, usually stored in the same directory as the original .doc file.

- **Other temporary files include** those that are downloaded from the Internet or e-mail attachments that have been opened and saved in a Temp directory, usually located in the system root directory (the directory where the operating system files are located, such as WINDOWS or WINNT).

- In theory, when you close the document or application, these temporary files are deleted, but Even when they are "deleted" by the system, they are still on the disk until overwritten.

- These temporary files can be deleted when the system shuts down or reboots, which is another reason to image the disk *before shutting down the system if at all possible.*

- Like other "deleted" files, these temp files can be recovered using tools designed for that purpose.

Swap and Page Files

- Most modern operating systems utilize a feature called ***virtual memory****, which allows the system to* think as it has more RAM than is actually installed.

- A portion of the hard disk is used to emulate additional memory and data is “swapped” from real physical memory to this holding space on disk as it’s needed by the processor.

- On Windows*, this data is held in a* file called the *swap file. On Windows NT, 2000, XP and Vista onward systems, it is called the page file because* data is swapped in units called *pages.*

- *Linux systems create a swap partition on the disk for this same* purpose. These files are generally created automatically by the operating system.

- These swap files contain all sorts of data in pages, including e-mail, Web pages, word processing documents, and any other work that has been performed on the computer during the work session.

- Some swap files are temporary and others are permanent, depending on the operating system in use and how it is configured.

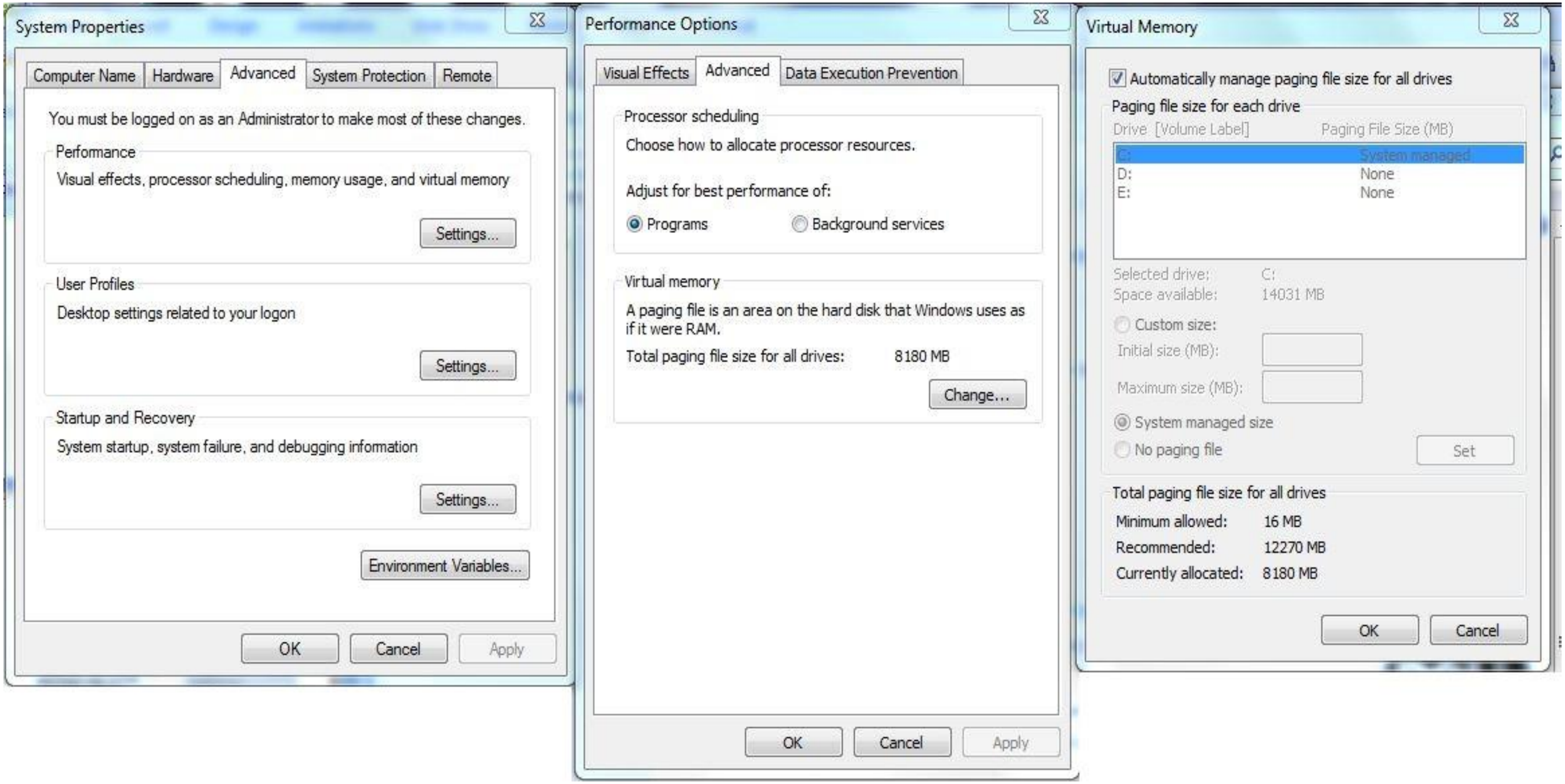
- The files might be marked with the hidden attribute, which makes them invisible in the directory structure under default settings.

- Swap files are created by the operating system in a default location.

- Many computer users are either unaware of the existence of these files or don’t really understand what they are, what they do, and what kind of data they contain.

- A technically savvy user **can change the location of the swap file or create additional swap/page files so that there are multiple virtual memory locations on a system**.

Virtual Memory



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information

Processor scheduling

Choose how to allocate processor resources.

Adjust for best performance of:

● Programs ○ Background services

Virtual memory

A paging file is an area on the hard disk that Windows uses as if it were RAM.

Total paging file size for all drives: 8180 MB

☑ Automatically manage paging file size for all drives

Paging file size for each drive

Drive [Volume Label]	Paging File Size (MB)
C:	System managed
D:	None
E:	None

Selected drive: C:
Space available: 14031 MB

○ Custom size:
Initial size (MB):
Maximum size (MB):
● System managed size
○ No paging file

Total paging file size for all drives

Minimum allowed: 16 MB
Recommended: 12270 MB
Currently allocated: 8180 MB

- You can then navigate to the drive on which the file is stored and locate it there.
- Note, however, that the page file will not be visible unless you have unchecked the ***Hide protected operating system files*** **(recommended) checkbox in the Tools | Folder Options | View advanced** settings in Windows Explorer.
- You can view the swap/page file with a utility such as DiskEdit, but much of the information is binary (0s and 1s) and not very usable.
- Special programs such as NTA Stealth and the Filter I "intelligent forensic editor" are designed to read swap file data and other *ambient computer data.*
- NTA Stealth is an upgrade to the Net Threat Analyzer tool, and is used to evaluate Internet browsing, download activity, and e-mail communications in ambient data for evidence related to illegal activities.
- Filter I uses a type of artificial intelligence (AI) to locate fragments of various types of files, including e-mail, chat conversations, newsgroup posts, and even network passwords and credit card and Security numbers.
- Both of these software packages are marketed by NTI (www.forensics-intl.com).
- The company also makes text search and disk search programs that can search storage devices at the physical level and locate data that is stored between allocated partitions or text strings that are in unallocated space.

Defeating Data Recovery Techniques

- There *are ways to defeat data recovery methods and suspects can use the* techniques to cover their tracks and destroy evidence of their crimes.

- Investigators need to be aware of the ways by which data *can be removed from a disk "once and for all."*

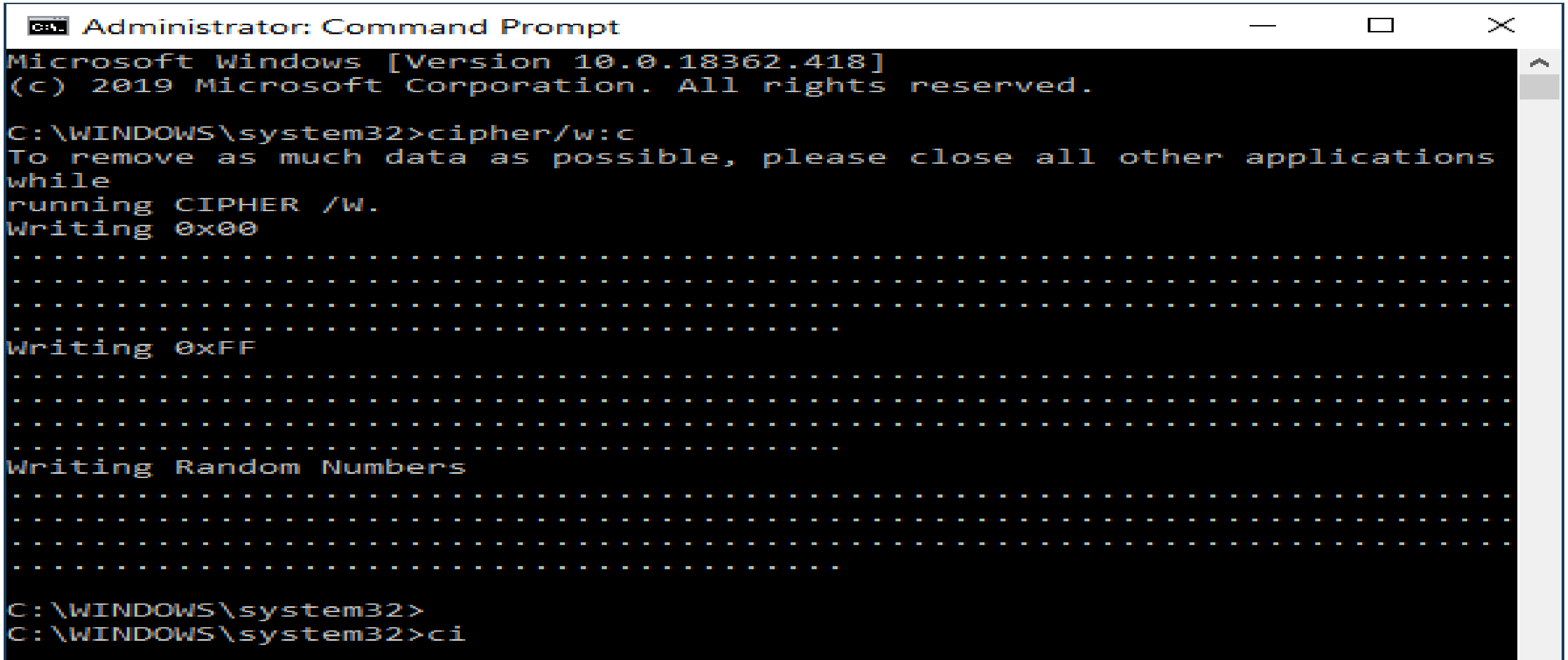
- In general, there are three ways to do this:
  1. Overwriting
  2. Degaussing (demagnetizing)
  3. Physically destroying the disk.

1. Overwriting the Disk

- The term *data remanence refers to the residual physical manifestations of data that have supposedly* been deleted or erased.

- Many "disk-wiping" utilities available commercially and as freeware or shareware on the Internet claim to remove this remanence.
- These utilities work by writing null or random data over the unallocated space on the disk.
- Windows include a command-line utility called CIPHER.EXE that, in addition to encrypting, decrypting, and managing encrypted files using the Encrypting File System (EFS), has a switch (/w) that overwrites data in unallocated clusters.

- **To overwrite deleted data on a volume by using Cipher.exe, use the /w switch with the cipher command:** Type cipher /w: folder, and then press ENTER, where **folder** is any folder in the volume that you want to clean.



```
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cipher/w:c
To remove as much data as possible, please close all other applications
while
running CIPHER /W.
Writing 0x00
........................................................................
........................................................................
........................................................................
........................................
Writing 0xFF
........................................................................
........................................................................
........................................................................
........................................
Writing Random Numbers
........................................................................
........................................................................
........................................................................
........................................

C:\WINDOWS\system32>
C:\WINDOWS\system32>ci
```

- These utilities attempt to fill the unallocated space with random binary values and can overwrite several times .
- To be effective, overwriting must be done many times using alternating patterns.

❖ If you're serious about eliminating data remanence by the overwriting method, use a program that meets or exceeds the standards such as U.S. Department of Defense (DoD) security standards **5220.22-M**.

- Under these standards, the **overwrite process must undergo at least three passes**:
  - ❑ Pass 1: Overwrite all addressable locations with binary zeroes.
  - ❑ Pass 2: Overwrite all addressable locations with binary ones (the compliment of the above).
  - ❑ Pass 3: Overwrite all addressable locations with a random bit pattern.
  - ❑ Verify the final overwrite pass.

- The **Gutmann method** is another algorithm for securely erasing the contents of computer hard disk drives, such as files. An overwrite session consists of a lead-in four random write patterns, followed by patterns 5 to 31 (see rows of table below), executed in a random order, and a lead-out of four more random patterns. Refer link for more info on passes. https://en.wikipedia.org/wiki/Gutmann_method

❖ **Royal Canadian Mounted Police (RCMP)** published the **(RCMP TSSIT OPS-II)**Technical Security Standards for Information Technology document that combines these various methods (writing zeros, ones , random data) and is usually implemented in the following way:

❑ Pass 1: Writes a zero
❑ Pass 2: Writes one
❑ Pass 3: Writes a zero
❑ Pass 4: Writes one
❑ Pass 5: Writes a zero
❑ Pass 6: Writes one
❑ Pass 7: Writes a random character and verifies the write

❖ **CSEC ITSG-06** published by Communication Security Establishment Canada (CSEC). CSEC ITSG-06 replaced **RCMP TSSIT OPS-II** as Canada's data sanitization standard.

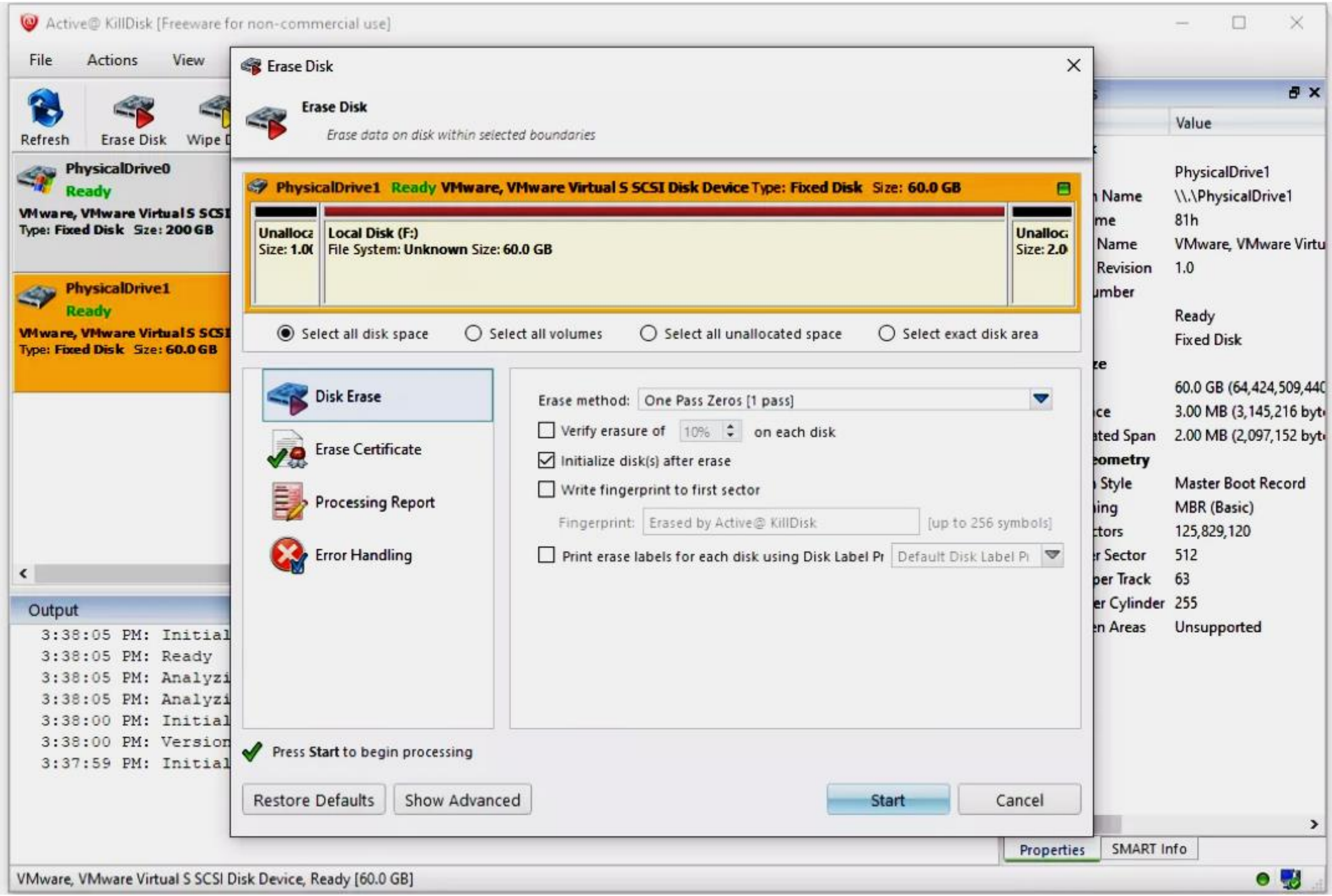
- It's usually implemented in the following way:

  Pass 1: Writes a one or zero
  Pass 2: Writes the complement of the previously written character (e.g. one if Pass 1 was zero)
  Pass 3: Writes a random character and verifies the write
- **(BITERASER)** Data Erasure Standards Supported by BitRaser Software

Internationally Recognized DISK Erasure Standards

Standards Name	Passes
NIST 800-88 Clear	1 pass
NIST 800-88 Purge	1~3 passes
US - DoD 5220.22-M	3 passes
US - DoD 5200.22-M (ECE)	7 passes
US - DoD 5200.28-STD	7 passes
Russian - GOST R 50739-95	2 passes
B. Schneier's Algorithm	7 passes
German Standard VSITR	7 passes
Peter Gutmann	35 passes
US Army AR 380-19	3 passes
NATO standard	7 passes
US Air Force AFSSI 5020	3 passes
Pfitzner Method	33 passes
Canadian CSEC ITSG-06	1-3 passes
NSA 130-1	3 passes
British HMG IS5 (Baseline)	1 pass
British HMG IS5 (Enhanced)	3 passes
Zeroes	1 pass
Pseudo Random	1 pass
NAVSO P-5239-26	3 passes
NCSC-TG-025	3 passes
Pseudo-Random & Zeroes	2 Passes
Random Random Zero	6 Passes
BitRaser Secure & SSD Erasure	1~3 passes

- An example of a disk-wiping program that meets DoD standards is : Active@ KillDisk (www.killdisk.com).
- It is a popular product that companies use to overwrite any data on hard disks and other media, especially those that are being disposed of or resold.
- Other important products that meet DoD standards are DiskScrub and M-Sweep Pro Data Eliminator from NTI.
- It overwrites the ambient data storage areas (file slack, unallocated file space).
- The **sale of these products is restricted to U.S. law enforcement,** medical facilities and hospitals, financial institutions, law ,accounting firms and government agencies.



PhysicalDrive0 Ready
VMware, VMware Virtual S SCSI
Type: Fixed Disk Size: 200 GB

PhysicalDrive1 Ready
VMware, VMware Virtual S SCSI
Type: Fixed Disk Size: 60.0 GB

Erase Disk

Erase Disk

Erase data on disk within selected boundaries

PhysicalDrive1 Ready VMware, VMware Virtual S SCSI Disk Device Type: Fixed Disk Size: 60.0 GB

Unalloca Size: 1.0(| Local Disk (F:) File System: Unknown Size: 60.0 GB | Unalloc Size: 2.0

● Select all disk space ○ Select all volumes ○ Select all unallocated space ○ Select exact disk area

Disk Erase
Erase Certificate
Processing Report
Error Handling

Erase method: One Pass Zeros [1 pass]

□ Verify erasure of 10% on each disk

☑ Initialize disk(s) after erase

□ Write fingerprint to first sector

Fingerprint: Erased by Active@ KillDisk [up to 256 symbols]

□ Print erase labels for each disk using Disk Label Pr Default Disk Label Pr

✓ Press Start to begin processing

Restore Defaults | Show Advanced | Start | Cancel

```
3:38:05 PM: Initial
3:38:05 PM: Ready
3:38:05 PM: Analyzi
3:38:05 PM: Analyzi
3:38:00 PM: Initial
3:38:00 PM: Version
3:37:59 PM: Initial
```

	Value
	PhysicalDrive1
Name	\\.\PhysicalDrive1
me	81h
Name	VMware, VMware Virtu
Revision	1.0
umber	
	Ready
	Fixed Disk
e	
	60.0 GB (64,424,509,440
ce	3.00 MB (3,145,216 byt
ated Span	2.00 MB (2,097,152 byt
eometry	
Style	Master Boot Record
ing	MBR (Basic)
tors	125,829,120
r Sector	512
per Track	63
er Cylinder	255
n Areas	Unsupported

VMware, VMware Virtual S SCSI Disk Device, Ready [60.0 GB]

Permanently Deleting Files

- Drive wiping is a crucial component of all digital forensic examinations.
- Any drive that is not thoroughly wiped has to be considered suspect.

PDWipe

- PDWipe is capable of wiping large hard drives (in excess of 8.4 GB) in just less than 11 minutes.

- PDWipe provides the option of specifying a character code when wiping a drive. It also offers the ability to wipe the drive using a random pattern.

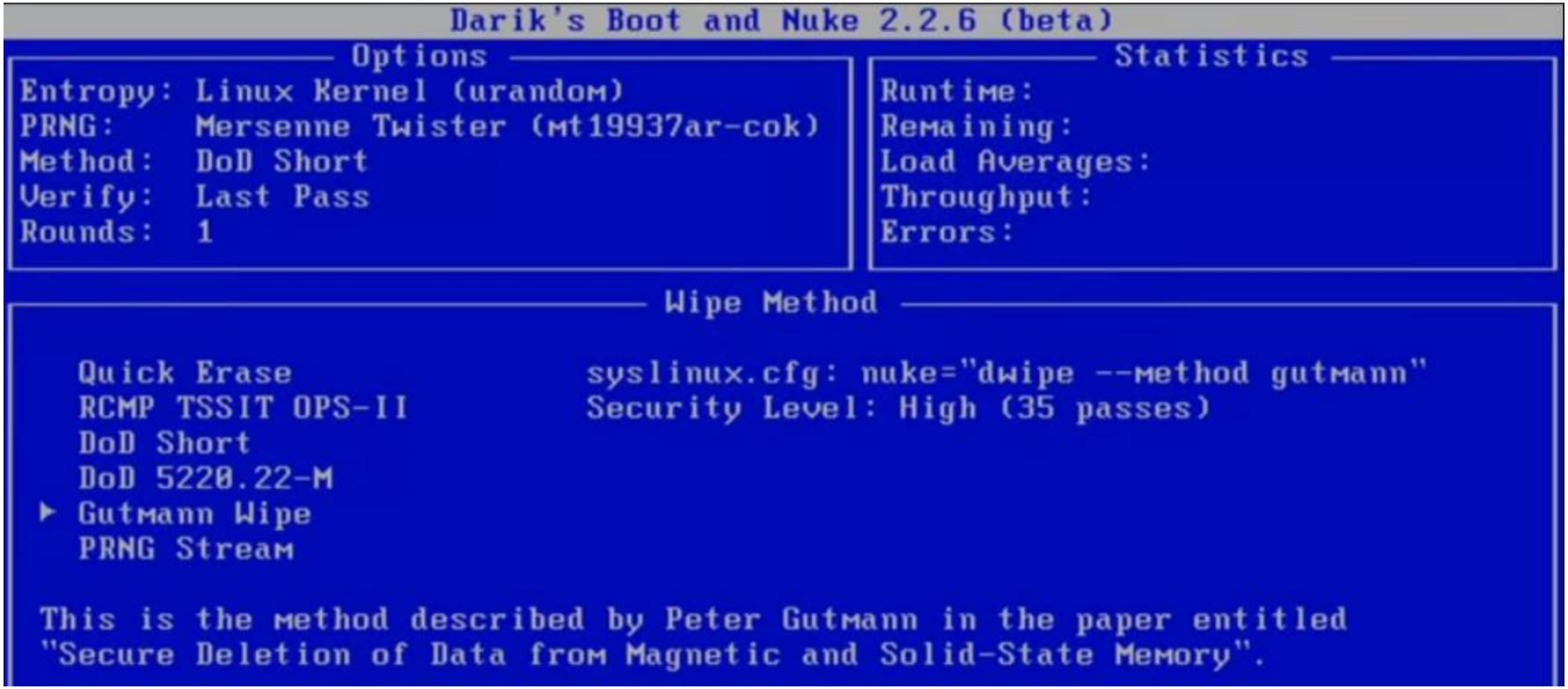
- PDWipe can process all drives in a system such that *all drives can be wiped with a single program* operation. It can generate a report of the wiping activity performed on a system.

- PDWipe can also verify that the contents of a specified number of randomly chosen sectors have been wiped.

- PDWipe will support any drive which is accessible to your system through the Int13h or the Microsoft/IBM Int13 extensions. Basic Input Output Systems (BIOS) typically provide this capability for all attached IDE devices. In addition, most SCSI adapters offer the ability to support attached devices through Int13 as well.
  - INT 13h is shorthand for BIOS interrupt call 13hex, the 20th interrupt vector in an x86-based computer system. The BIOS typically sets up a real mode interrupt handler at this vector that provides sector-based hard disk and floppy disk read and write services using cylinder-head-sector (CHS) addressing.

Darik’s Boot and Nuke (DBAN)

- Darik’s Boot and Nuke (DBAN) is a free tool available from http://dban.sourceforge.net.
- It is a **self-contained boot program** that securely wipes the hard disks of most computers.
- DBAN can be booted from a CD, DVD, USB flash drive or diskless using a Preboot Execution Environment. It is based on Linux and **supports PATA (IDE), SCSI and SATA hard** drives. DBAN can be configured to automatically wipe every hard disk that it sees on a system or entire network of systems, making it very useful for unattended data destruction scenarios.
- DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction.



```
                         Darik's Boot and Nuke 2.2.6 (beta)
 ---------------- Options ------------------------  ------------ Statistics --------
 Entropy:  Linux Kernel (urandom)                     Runtime:
 PRNG:     Mersenne Twister (mt19937ar-cok)           Remaining:
 Method:   DoD Short                                  Load Averages:
 Verify:   Last Pass                                  Throughput:
 Rounds:   1                                          Errors:

 ------------------------------------ Wipe Method ------------------------------------

    Quick Erase                syslinux.cfg: nuke="dwipe --method gutmann"
    RCMP TSSIT OPS-II          Security Level: High (35 passes)
    DoD Short
    DoD 5220.22-M
  ▸ Gutmann Wipe
    PRNG Stream

  This is the method described by Peter Gutmann in the paper entitled
  "Secure Deletion of Data from Magnetic and Solid-State Memory".
```

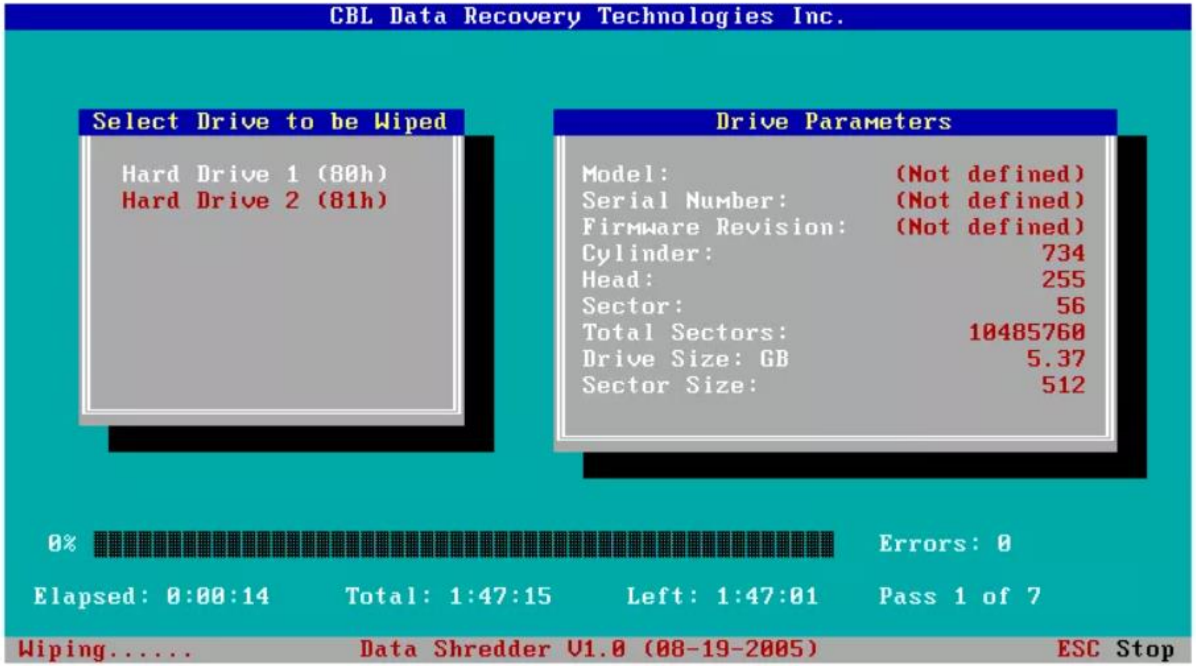
- **CBL Data Shredder** comes in two forms: you can either boot from it via a disc or USB stick (like with DBAN) or use it from within Windows like a regular program.

- To erase the hard drive that's running an operating system, you're required to boot to the program, whereas deleting another internal or external drive can be done with the Windows version.

- **Data Sanitization Methods:** DoD 5220.22-M, Gutmann, RMCP DSX, Schneier, VSITR

- In addition to the above, you can create your own custom method to include 1s, 0s, random data, or custom text with a custom number of passes.

- The Windows version of CBL Data Shredder works with Windows XP through Windows 11.



```
                    CBL Data Recovery Technologies Inc.

   Select Drive to be Wiped            Drive Parameters

     Hard Drive 1 (80h)          Model:                 (Not defined)
     Hard Drive 2 (81h)          Serial Number:         (Not defined)
                                 Firmware Revision:     (Not defined)
                                 Cylinder:                        734
                                 Head:                            255
                                 Sector:                           56
                                 Total Sectors:              10485760
                                 Drive Size: GB                  5.37
                                 Sector Size:                     512

  0% ████████████████████████████████████████████       Errors: 0

 Elapsed: 0:00:14     Total: 1:47:15     Left: 1:47:01     Pass 1 of 7
Wiping......           Data Shredder V1.0 (08-19-2005)            ESC Stop
```

2. Degaussing or Demagnetizing

- Another way to get rid of the data remaining on a disk is to create a very strong magnetic field that is capable of reducing the magnetic state of the media to zero.

- This process is called *degaussing, and the* device that generates the magnetic field is called a *degausser.*

- *Degaussers work either by applying an* alternating magnetic field using AC power or by applying a unidirectional field using DC power.

- Handheld permanent magnets can also be used to degauss some types of magnetic media (diskettes and hard disk platters; they are not usually used to degauss magnetic tapes).

- There are different types of magnetic devices, based on the coercivity of the media.

- It is important to have the proper type of degausser that matches the tape type, to purge all the data.

- For example, hard disk drives typically have higher coercivity compared to floppy disks or magnetic tapes. Therefore, a degausser with a higher magnetic field strength would be required to effectively erase data from hard drives compared to other media types.

3. Physically Destroying the Disk

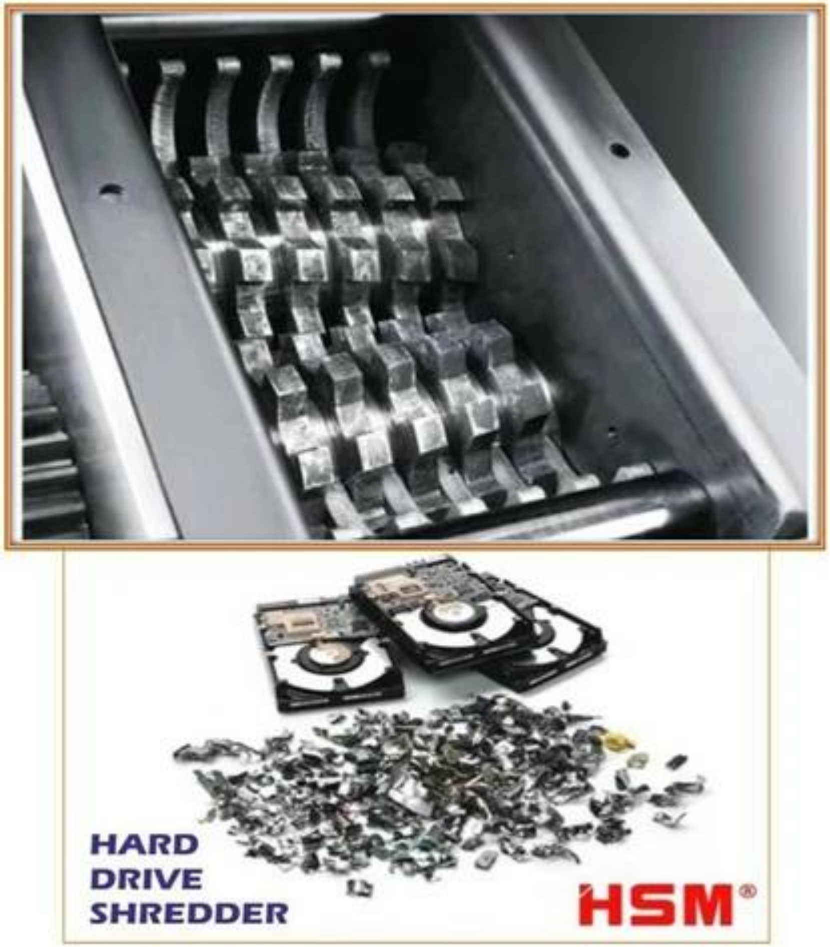
- In cases, where it is extremely important that there be no possibility that data remaining on a disk could ever be reconstructed—for example, in a national security situation in which classified data was stored on the disk—it might be preferable to physically destroy the disk.

This can be done in several ways:

- Pulverization (completely crushing or grinding the disk down to powder)
- Incineration (burning the disk to ashes)
- Abrasion (using a sander or emery wheel to completely remove the surface of the disk)
- Acid (submerging the disk in a strong acid solution, such as hydrochloric acid or sulfuric acid, which corrodes the metal components of the disk and destroys the magnetic surface where the data is stored)

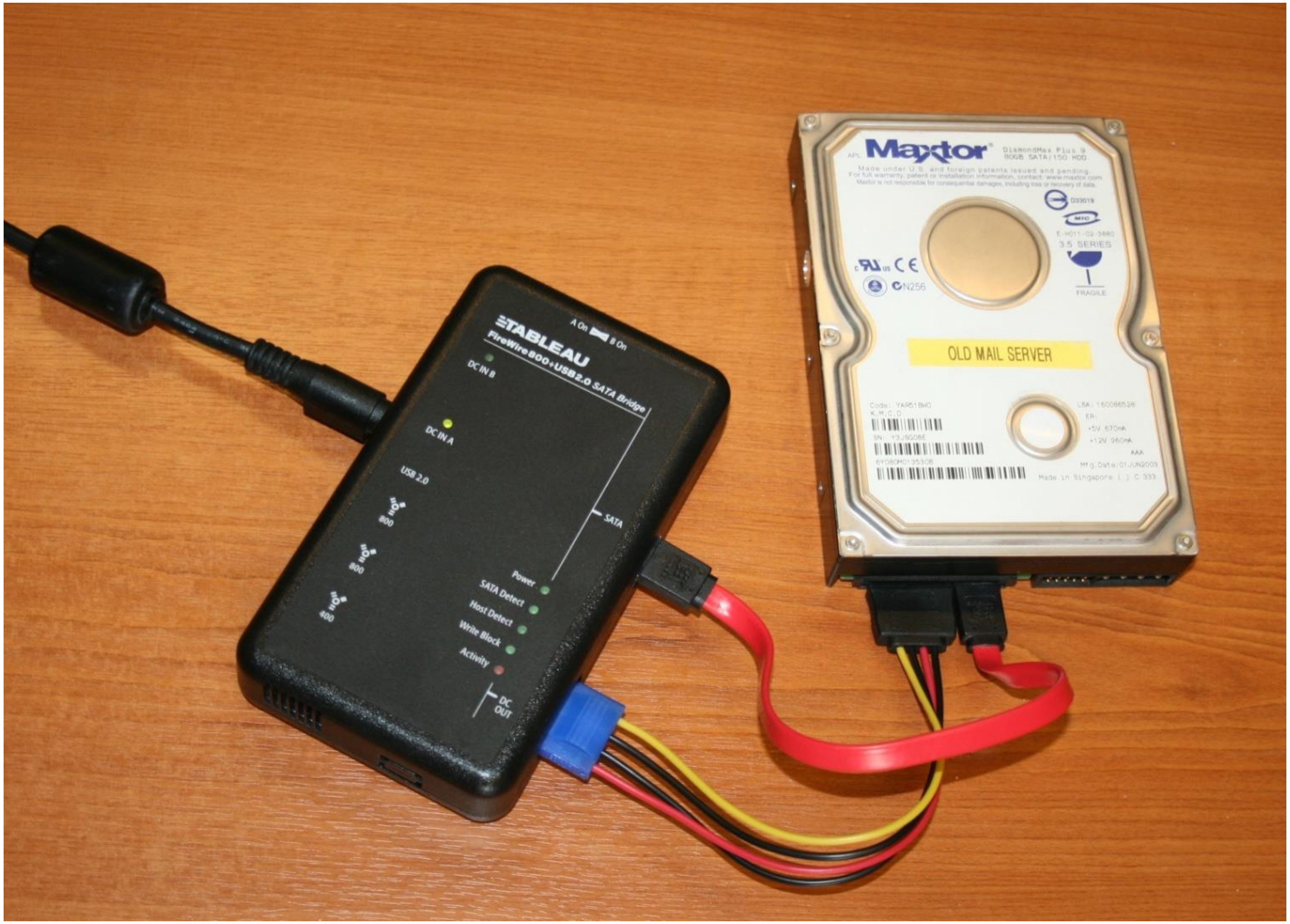
3. Destroying CDs and DVDs and magnetic disks

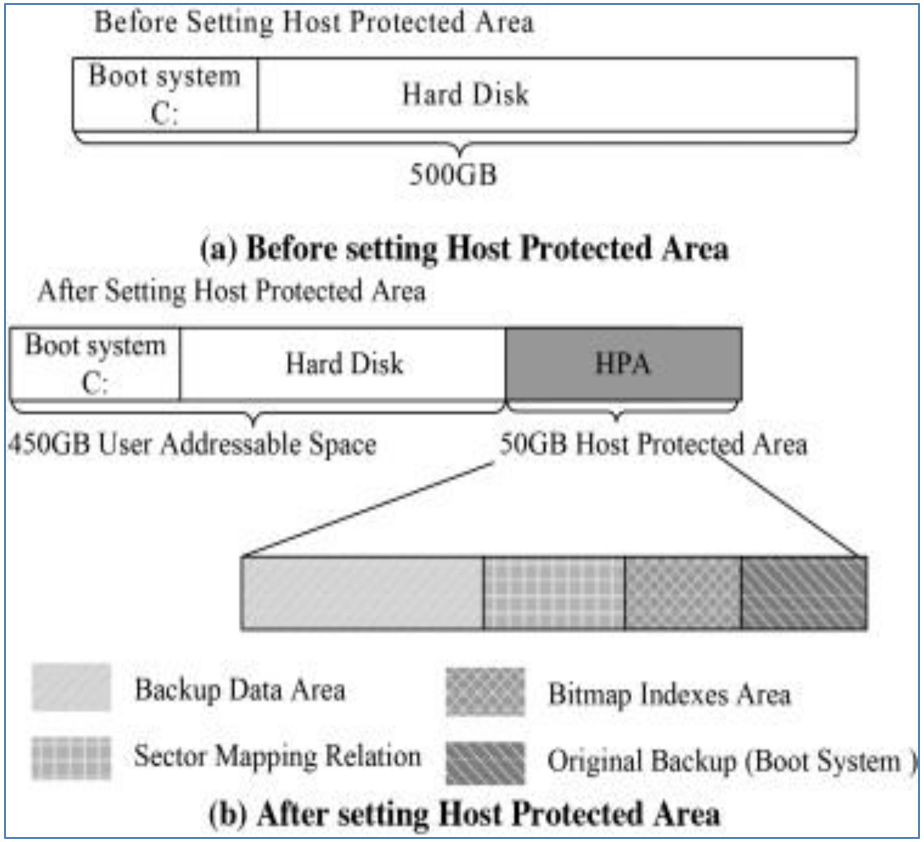
- To prevent others from gaining access to programs, financial information, or other data stored on disks, **shredders** can be used to destroy the disks.



Thank you

Hardware write blocker



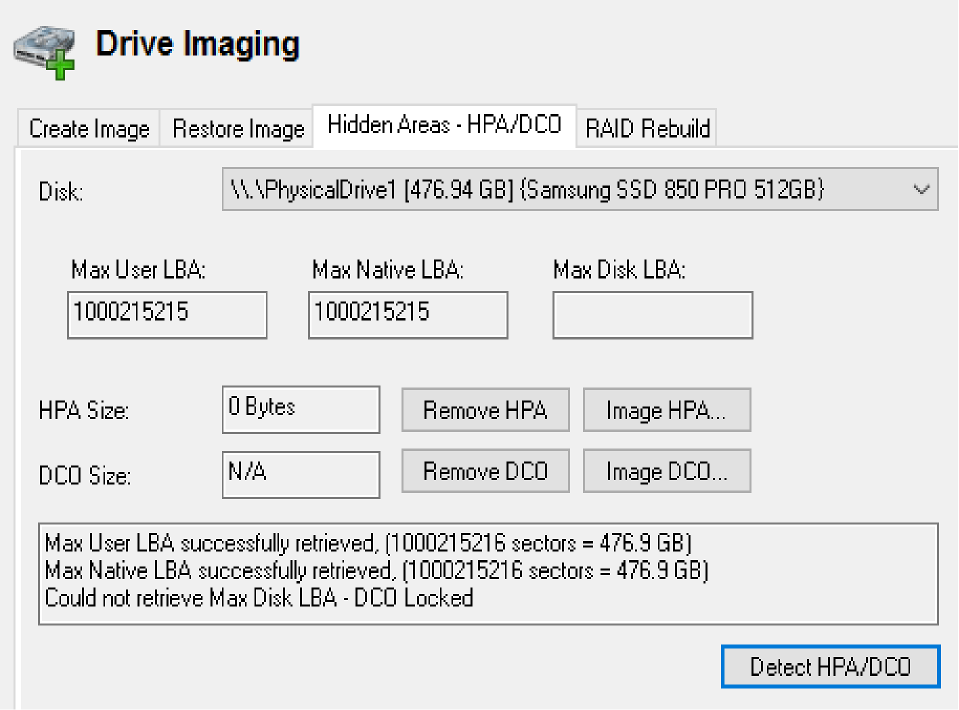

Before Setting Host Protected Area
Boot system C:
Hard Disk
500GB
After Setting Host Protected Area
Boot system C:
Hard Disk
HPA
450GB User Addressable Space
50GB Host Protected Area
▨ Backup Data Area
▨ Bitmap Indexes Area
▨ Sector Mapping Relation
▨ Original Backup (Boot System)

(a) Before setting Host Protected Area

(b) After setting Host Protected Area

Source: https://www.sciencedirect.com/science/article/pii/S0030402614012455

OSForensics includes built-in support for accessing HPA



Disk: \\.\PhysicalDrive1 [476.94 GB] (Samsung SSD 850 PRO 512GB)

Max User LBA:	Max Native LBA:	Max Disk LBA:
1000215215	1000215215	

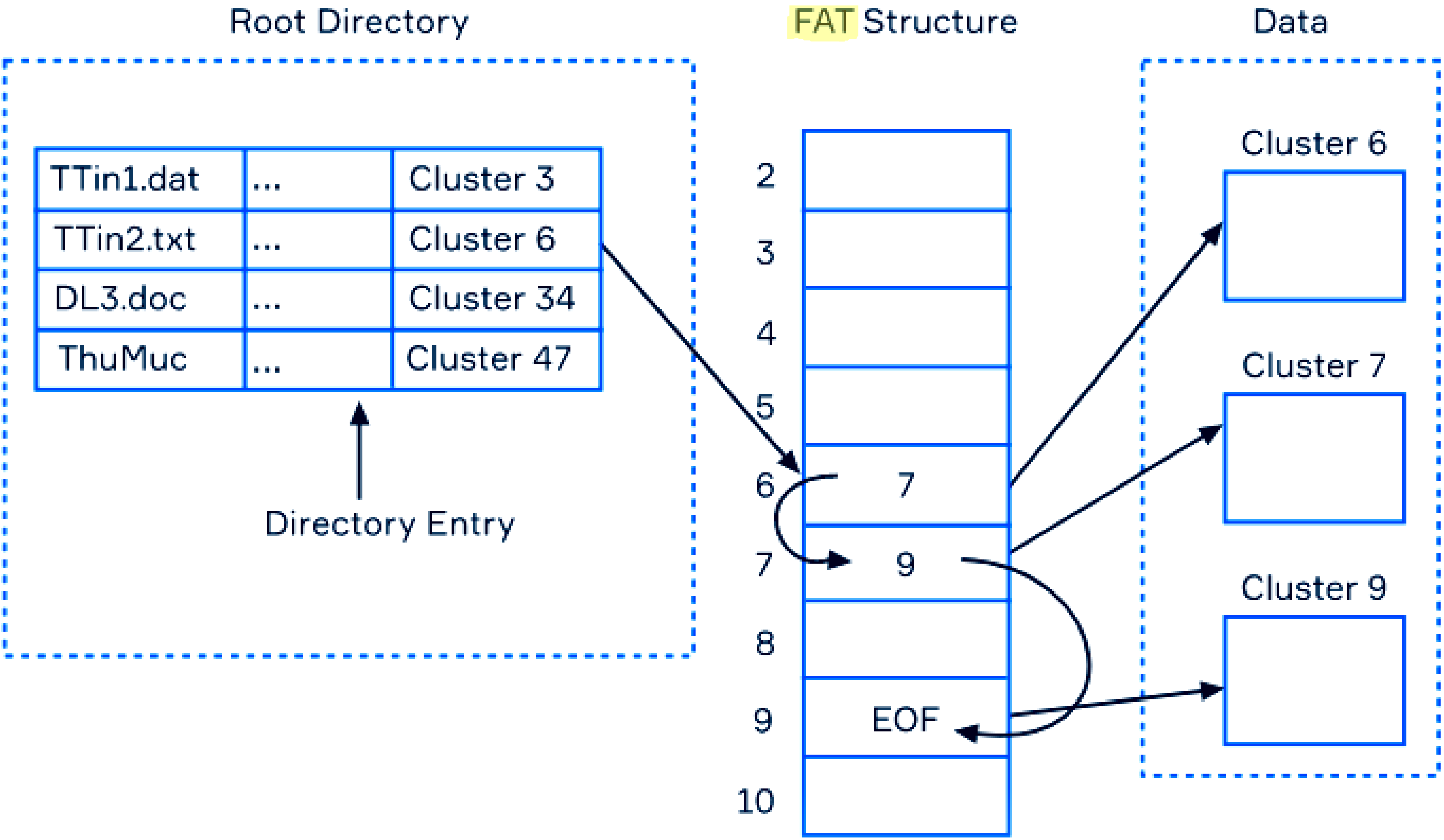
HPA Size: 0 Bytes

DCO Size: N/A

```
Max User LBA successfully retrieved. (1000215216 sectors = 476.9 GB)
Max Native LBA successfully retrieved. (1000215216 sectors = 476.9 GB)
Could not retrieve Max Disk LBA - DCO Locked
```

Source: https://www.osforensics.com/hidden-areas-hpa-dco.html

- HPA is also used by various theft recovery and monitoring service vendors. For example, the laptop security firm CompuTrace use the HPA to load software that reports to their servers whenever the machine is booted on a network. HPA is useful to them because even when a stolen laptop has its hard drive formatted the HPA remains untouched.
- Some rootkits hide in the HPA to avoid being detected by anti-rootkit and antivirus software.
- The DCO allows system vendors to purchase HDDs from different manufacturers with potentially different sizes, and then configure all HDDs to have the same number of sectors. For example, using DCO to make an 80 Gigabyte HDD appear as a 60 Gigabyte HDD to both the OS and the BIOS.



Root Directory

TTin1.dat	...	Cluster 3
TTin2.txt	...	Cluster 6
DL3.doc	...	Cluster 34
ThuMuc	...	Cluster 47

Directory Entry

FAT Structure

2	
3	
4	
5	
6	7
7	9
8	
9	EOF
10	

Data

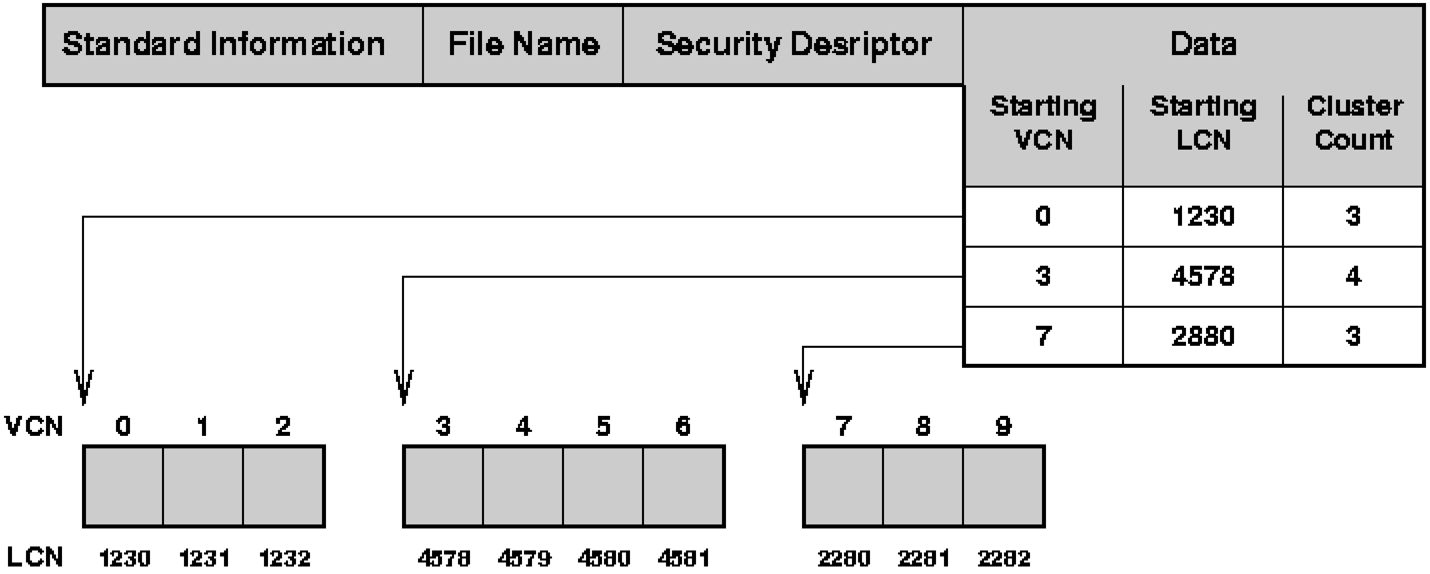
NTFS and the Master File Table

MFT Entry (Simplified)

Standard Information	File Name	Security Desriptor	Data

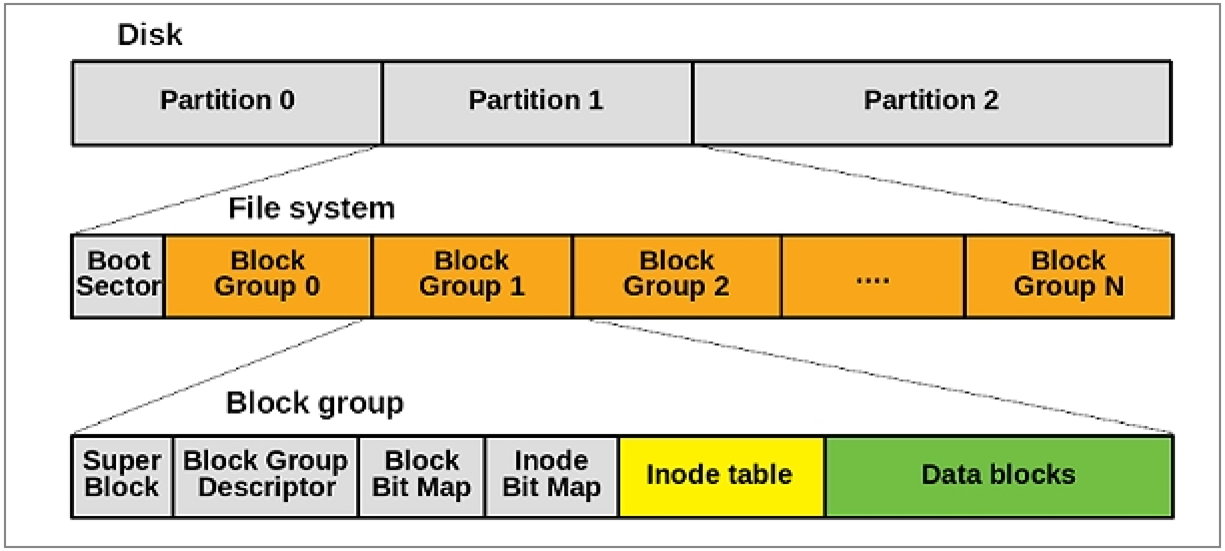
- *Standard information:* This attribute includes the information :
  - read/write permissions,
  - creation time,
  - last modification time,
  - count of how many directories point to this this file (hard link count.
- *File Name:* This attribute describes the file's name in the Unicode character set.
- *Security Descriptor:* This attribute lists which user owns the file and which users can access it (and how they can access it).
- *Data:* This attribute either contains the actual file data in the case of a small file or points to the data (or points to the objects that point to the data) in the case of larger files.

MFT Entry

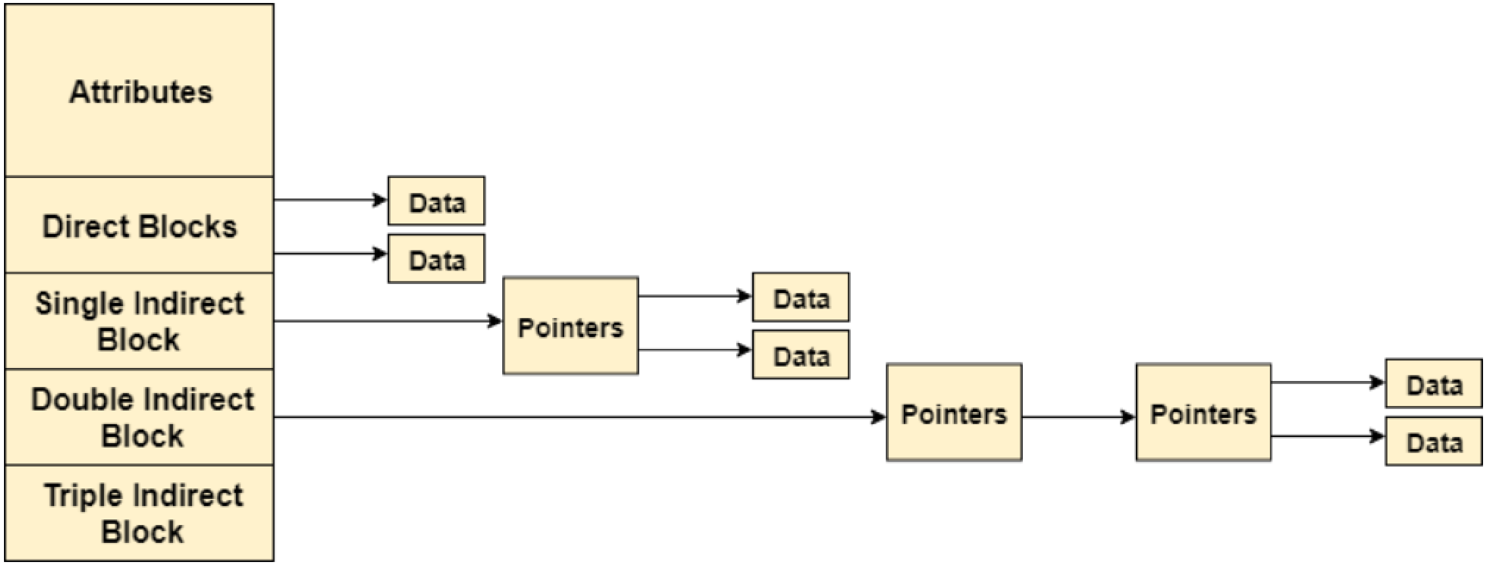


Starting VCN	Starting LCN	Cluster Count
0	1230	3
3	4578	4
7	2880	3

Ext



An inode is an index node. It serves as a unique identifier for a specific piece of metadata on a given filesystem. Each piece of metadata describes what we think of as a file.


Attributes
Direct Blocks
Single Indirect Block
Double Indirect Block
Triple Indirect Block
Data
Data
Pointers
Data
Data
Pointers
Pointers
Data
Data