Computer Workshop Series

How to Fully Delete Data from a Disk Drive

April 2013

Dennis Martin

Demartek

This presentation is available at http://www.demartek.com/Demartek_Presents_Data_Destruction_Methods.html

Agenda

- Introduction
- Reasons to fully delete data
- How disk drives and SSDs work
- “Leftover Data” and the Delete command
- ~ Short Break ~
- Security vs. Convenience
- Data Sanitization Methods

Introduction

- If you plan to sell or donate a computer, it is important to insure that any personal data is removed from the disk drives in that computer before it leaves your control.

- In this context, “disk drive” means any storage device such as hard disk drive (HDD) or solid state drive (SDD) that is installed in the computer or external drive that is bundled with the computer.

Reasons to Fully Delete Data

Identity Theft Prevention

- It’s a good idea to keep your personal information, passwords and financial information private
- Identity thieves are looking for ways to steal your money and old computer disk drives are one way to accomplish this
  - Attend the “Identity Theft Prevention Tips” workshop on May 19

Reasons to Fully Delete Data

Legal Requirements

- Several Federal and State laws and regulations in the USA, Canada, Europe and elsewhere require data security practices, especially for certain industries or types of personal information
  - HIPAA, Gramm-Leach-Bliley, Sarbanes Oxley, FACTA, California SB 1386
- There can be fines, prison time and civil action for violations

Examples of Drives

- Show and Tell time
  - Examples of 3.5-inch and 2.5-inch hard disk drives and SSDs

How Disk Drives Work

- Drives read and write data to blocks on the media

Normal Data Blocks

ABC	DEF	GHI	JKL
MNO	PQR	STU	VWX

How Disk Drives Work

- Sometimes, blocks go “bad”
  - Operating System marks the block as bad and no longer uses it
  - Normal user commands can’t touch the bad blocks
  - Deleting the data blocks does not delete any usable bits in the bad block
  - Potentially leaves data on the drive

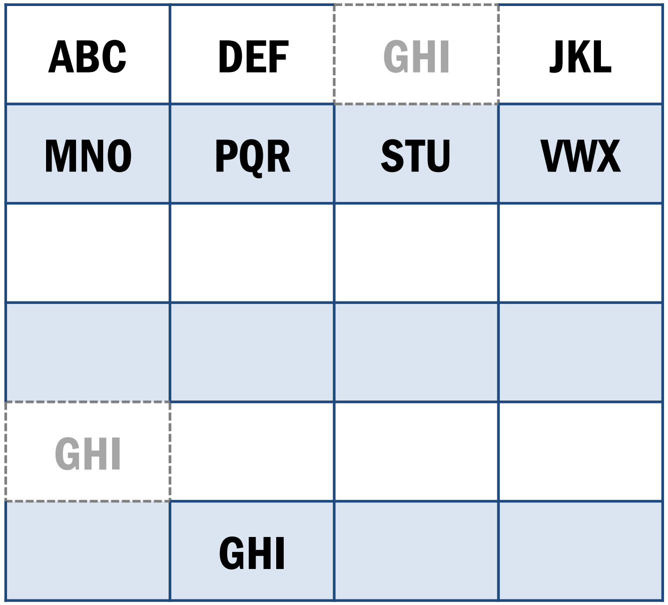
Normal Data and One Bad Block

ABC	DEF	GHI	JKL
MNO	PQR	STU	VWX

How SSDs Work

- SSDs use a technique called “wear leveling” that reassigns blocks periodically to prolong the life of the NAND flash
  - Old blocks are unavailable to user commands
  - Leaves data on the drive

Normal Data Blocks



ABC	DEF	GHI	JKL
MNO	PQR	STU	VWX
GHI			
	GHI		

Delete File Process

- When you delete a file, generally only the table of contents (TOC) entry is deleted, not the data blocks

T.O.C.
(Filenames)

Data
Blocks

A	B	C	D				
A1	A2	A3	B1	B2	B3	B4	B5
C1	C2	C3	C4	C5	D1	D2	D3
D4	D5	D6	D7				

Delete File Process

- Delete file “C”
  - Data blocks associated with file “C” can used for new data

T.O.C. (Filenames)

Data Blocks

A	B		D				
A1	A2	A3	B1	B2	B3	B4	B5
C1	C2	C3	C4	C5	D1	D2	D3
D4	D5	D6	D7				

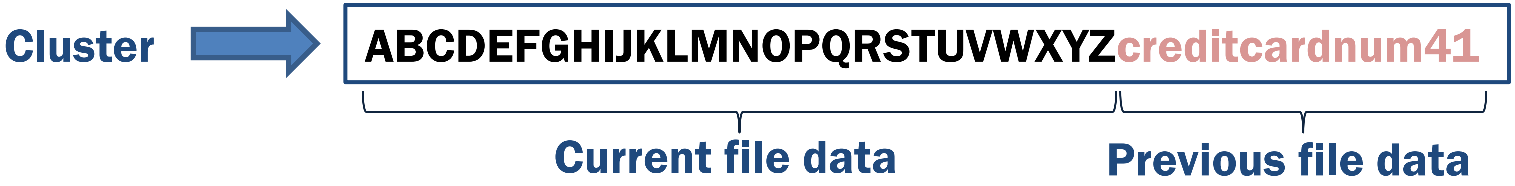
Delete File Process

- Create new file “E”
  - New data is written to any available blocks

T.O.C. (Filenames)	A	B	E	D				
Data Blocks	A1	A2	A3	B1	B2	B3	B4	B5
	E1	E2	E3	C4	C5	D1	D2	D3
	D4	D5	D6	D7				

Slack Space

- File space is frequently allocated in clusters
  - Clusters are groups of blocks
- When applications write data to files, they may not use the entire cluster
- The space remaining towards the end of the cluster after the end of the file is called “slack space”
  - The contents of the slack space are undefined, meaning that it could contain old data



Other Places Data is Kept

- Recycle Bin
  - Used to prevent accidental erasure
- Recovery copies
  - Microsoft Office and other applications allow you to specify a recovery file location
- Operating System Paging File
  - Copy of in-memory data

Break Time

Upcoming Workshops

- May 19 – Identity Theft Prevention Tips
  - Identity theft, also known as ID theft and identity fraud, is a widespread and fast-growing crime. Although potentially anyone can be targeted, there are a number of practical steps that can be taken to reduce the risk of becoming an identity theft victim.
- June 2 – How to Build a Computer
  - We will explain the major components of a computer and build a computer during the workshop. No experience is necessary.

Security vs. Convenience

- Security and Convenience are inversely related
  - Higher security results in less convenience
  - Higher convenience results in less security

Security Principles

- Security focuses on risk management
  - What are the threats?
  - Which threats are the most likely to occur?
  - What can be done to mitigate these threats?
  - How much time, money and effort are you willing to devote to mitigating specific threats?
- Discuss the above when selling or donating a computer
  - What data is on your storage devices?
  - Who is likely to be the new owner of your computer?

Data Sanitization

- Data Sanitization means removing data from computer storage devices
- Two basic types of data sanitization
  - Logical – uses software techniques
  - Physical – uses physical hardware techniques
- US Government standards
  - NIST 800-88
  - NSA/CSS Storage Declassification Manual 9-12

NIST 800-88

- A revision 1 draft was published in September 2012
- Describes three levels of sanitization
  - **Clear**: logical sanitization of user-addressable areas
  - **Purge**: physical or logical sanitization that renders data recovery infeasible
  - **Destroy**: renders data recovery infeasible and the device unusable for data storage

Logical Data Sanitization

- Weak erase – deleting files
- Block erase – overwrite
- Normal secure erase
- Enhanced secure erase

Weak Erase

- Deleting files – we discussed the problems already
- Quick Format
  - Only the volume T.O.C. but not the data blocks in that partition
  - Can take seconds or minutes

Block Erase

- Full format: all the blocks in that partition are erased
  - Can take hours
- Overwrite utilities
  - Various utilities can overwrite files, partitions or entire drives with data patterns
  - Some reference DoD 5220.22, but this now considered obsolete and does not provide enough security for certain government security levels
  - Can take hours or days
  - May not erase bad blocks or certain unallocated areas

Normal Secure Erase

- Approved by NIST 800-88 up to “Confidential” security level
- Available in recent SATA disk drives
- Requires special program to execute
- Takes minutes or up to about an hour

Enhanced Secure Erase

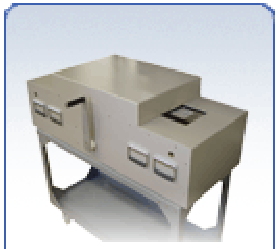
- Uses cryptographic techniques
- Only works with self-encrypting hard disk drives or many types of SSDs that perform encrypted writes
- Removes the cryptographic key, effectively rendering the data as useless
- Takes seconds

Physical Data Sanitization

- Degaussing – magnetic fields that erase data (hard disk drives only)
- Disintegration – physical destruction that meets specific government standards
- Incineration/smelting – physical destruction that requires “hazmat” protection

Degaussing

- Uses a magnetic force to erase magnetic data
  - Degaussers are rated by “coercivity” in units of Oe (Oersteds)
  - Applies to HDDs and some also work with magnetic tape
  - Two categories: Longitudinal and Perpendicular
- Frequently requires cover of disk drive to be removed, rendering the device unusable
- NSA/CSS maintains a current Degausser “Evaluated Products List”



HPM-4E Degausser
energy efficient,
large chamber,
multi-directional
magnetic field

Disintegrators

- Machines that bend, shatter, puncture or crush hard disk drives
- SSD disintegrators destroy solid-state media into particles 2mm or less in size
- Some units perform degaussing followed by disintegration

DB-6000 Destruction Device
heavy duty, portable, energy efficient

Incineration/Smelting

- Incineration and Smelting techniques can be used
- These involve use of hazardous materials and require a controlled environment
  - By-product of burning magnetic tapes and disk is cyanide gas
  - Disk coatings contain carcinogens
- Disk platters can be sanded, removing the oxide
  - The oxide can then be treated with acid
- SSDs can be melted at very high temperatures

Conclusion

- Questions to ask yourself
  - What type of data is on your storage devices?
  - How much time, money and effort do you want to devote to this process?
- Recommendations
  - A good overwrite of the entire drive will be good enough for most personal data
  - If you have business data on your personal device, consult your company policy

Thank You!

Dennis Martin, President
dennis@demartek.com
www.linkedin.com/in/dennismartin

Demartek

(303) 940-7575
www.demartek.com
http://twitter.com/Demartek
www.youtube.com/Demartek
Skype: Demartek

To learn more about Demartek:

- ◆ Download the Aurasma App (Android/iPhone)
- ◆ Search and follow “Demartek”
- ◆ View image below with viewfinder.

*also on the back of Dennis’ business card

Powered by: AURASMA