File Encryption and Deletion 101

Randi Ellias, Butler Rubin Saltarelli & Boyd LLP

Ronald S. Gass, The Gass Company, Inc.

With thanks to Daniel B. Garrie, JAMS

ARIAS U.S.

Current State

- Regulations issued by New York Department of Financial Security effective March 1, 2017, phased in over a two-year period

- NAIC Insurance Data Security Model Law. Compliance with NY regulations deemed compliance with the Model Law. Chair for the Working Group expects the final document to pass through the Innovation and Technology Task Force and be sent to the Executive Committee for final approval "at the next available opportunity"

- NY regs require insurance companies to ensure that third-party service providers have adequate policies and procedures in place for security of sensitive data

This means arbitrators

- Specifically includes the requirement that third-party service providers have policies and procedures in place for encryption of non-public information, both "in transit and at rest"

- Clients increasingly expect arbitrators to have policies and procedures in place

- Law firms have instituted policies and procedures and also expect arbitrators to have policies and procedures in place

Tech Talk
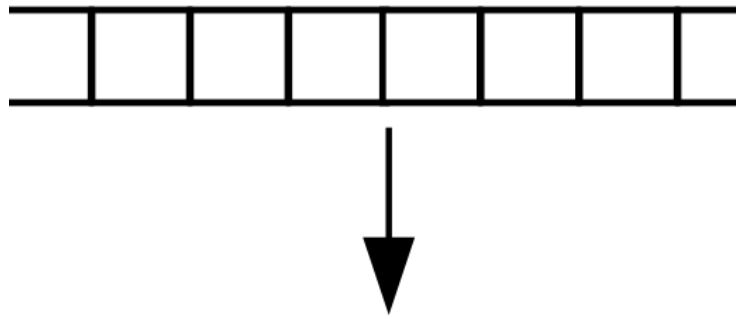
File Encryption

- Sometimes just need to encrypt attachments (e.g., Cover e-mail does not contain confidential information)

- Most versions of Microsoft Office and Apple OS allow for file encryption

- Could also use an FTP site, such as sync.com, pCloud, SpiderOak and HighTail.

- **Don't send the password for the encrypted file in the same communication as the encrypted file itself.**
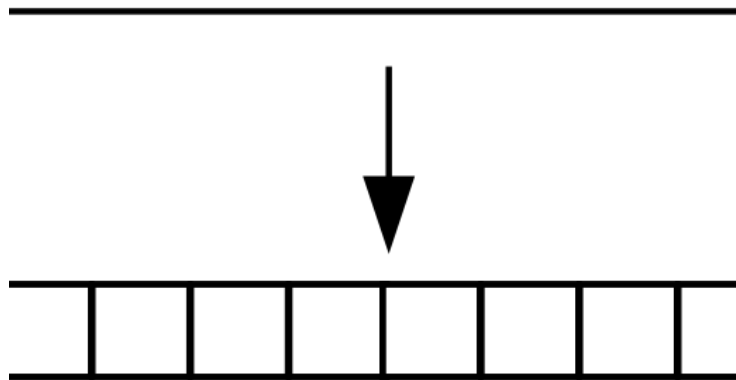
The following standalone products encrypt files or folders on your PC or Mac.

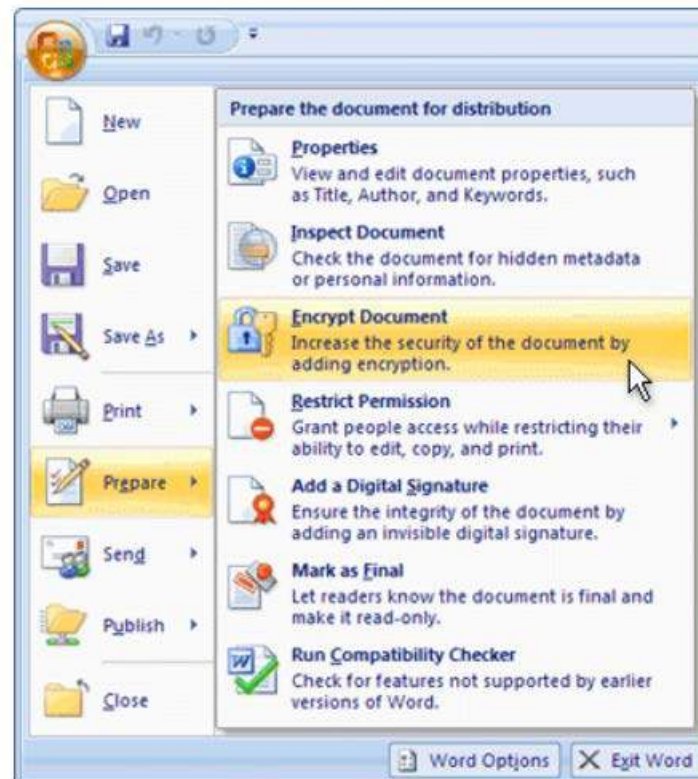|		
Veracrypt (Windows and Mac)	AxCrypt (Windows)	DiskCryptor (Windows)
GNU Privacy Guard (Windows and Mac)	7-Zip (Windows)	WinZip (Windows) or WinZip5 Mac (Mac)
	iZip (Mac)	

1. Click the **Microsoft Office Button** 🔘 , point to **Prepare**, and then click **Encrypt Document**.

2. In the **Encrypt Document** dialog box, in the **Password** box, type a password, and then click **OK**.

> CAUTION: Keep your password in a safe place. If you lose or forget the password, it can't be recovered.

You can type up to 255 characters. By default, this feature uses AES 128-bit advanced encryption. Encryption is a standard method used to help make your file more secure.

3. In the **Confirm Password** dialog box, in the **Reenter password** box, type the password again, and then click **OK**.

4. To save the password, save the file.

Microsoft

Step 1

Open the PDF and click on "Advanced "Security" on the main menu, click on "Password Encryption" from the pull-out menu and then Click "Yes" to the security change prompt screen.

Step 2

Click the check box next to "Require a Password to Open the Document" and enter your password in the "Document Open Password" text box. Click "OK" to accept and then enter your password again to confirm and then click "OK." Save your file for the change to take place.

Step 3

Click the "Required Password to Change Permissions or Password" to have the user enter a password to make any changes to the security of the file; type in a password that is different from the "Password to Open the Document."

Step 4

Click the "Printing Allowed" pull-down menu and choose "Low Resolution" (150 dpi) to allow users to print bitmap images or choose the "High Resolution" option to allow users to print high-quality vector outputs.

Step 5

Remove a password by opening the PDF and entering the password when prompted, then hit "OK." Click on "Advanced," "Remove Security," "Password Encryption" and then "OK" on the "Are you sure you want to remove security from this document?" prompt screen. Save your file for the change to take place.
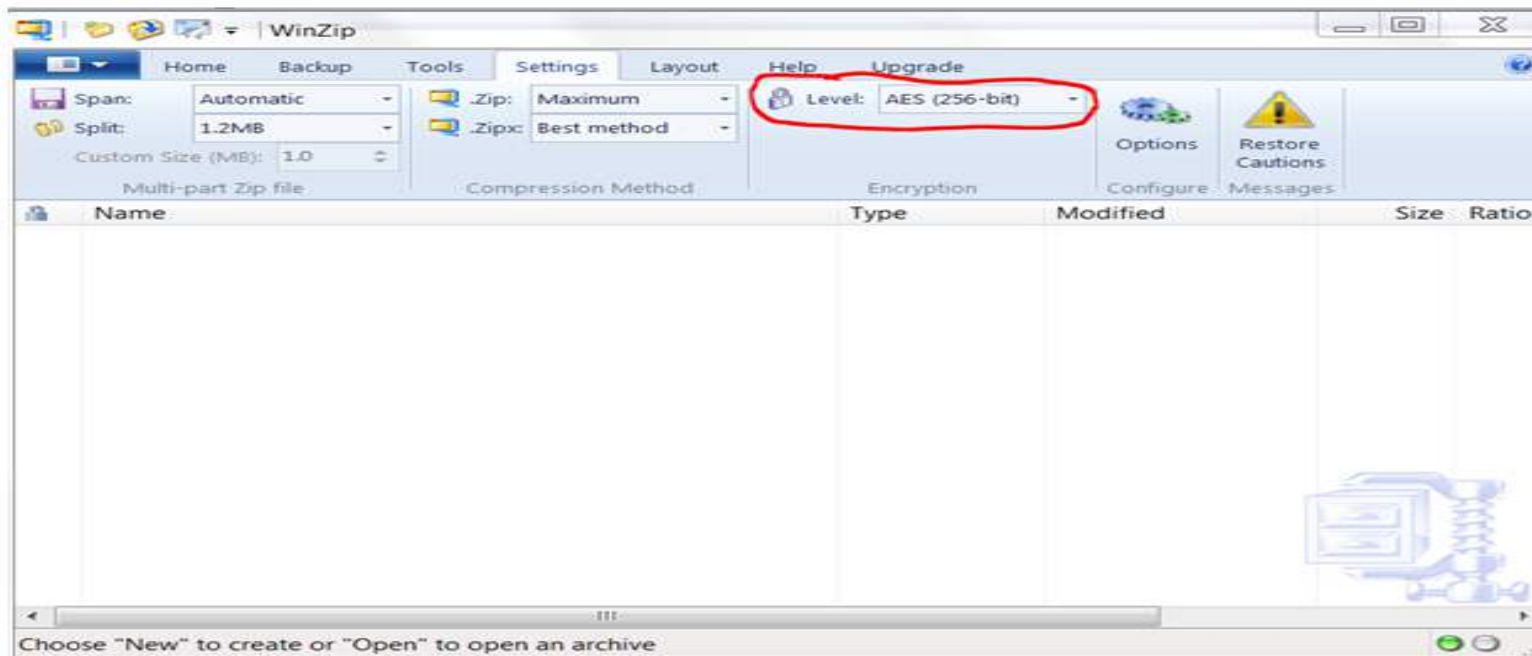
File Encryption – Adobe PDF for Apple OS X

1. Open a .pdf document in Preview
2. Choose File -> Save as
3. Choose a name
4. Click "Encrypt"
5. Choose a password

## Setting Up Encryption Level (older versions of WinZip)

1. Open Win Zip
2. Go to Settings Tab
3. Change the Encryption Level to AES (256-bit)

4. From this point forward your WinZip will be set to AES (256-bit) encryption.

1. If you are zipping one file right click on it, if you are zipping multiple files, move them into a folder and click on the folder.

2. Then highlight WinZip and an additional menu will appear and choose Add to Zip File..

3. In the window that opens, under Options, put a check mark next to Encrypt Added Files
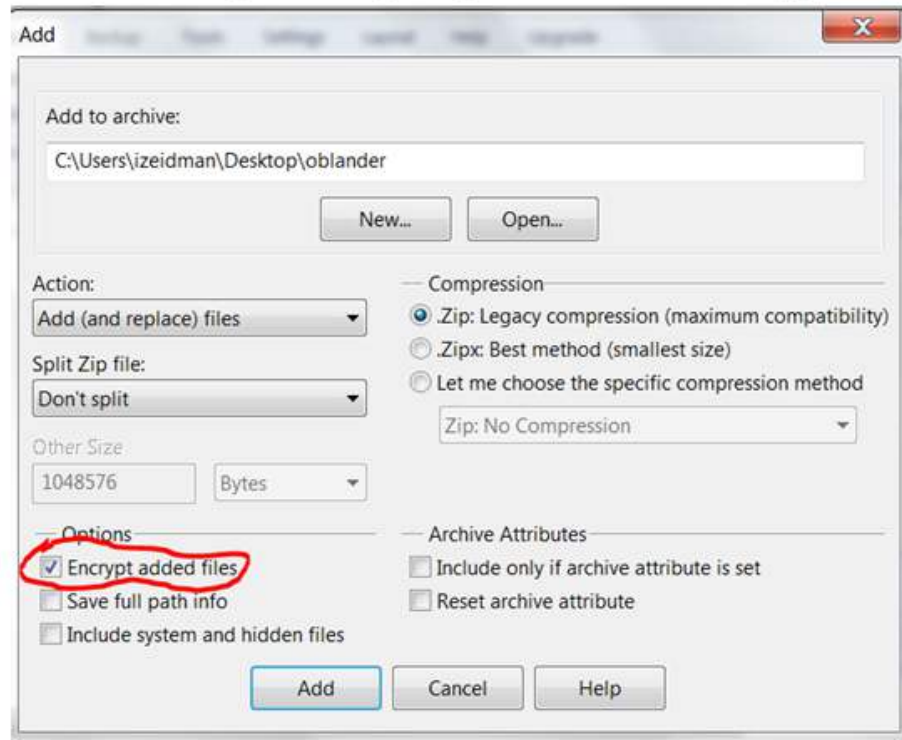
File Encryption – Creating Encrypted .zip Files (older versions of WinZip)
Adding a Password

4. Then click on Add and a password window will open.

5. Enter a complex password (must be at least 8 characters long) with a combination of upper and lower case letters and numbers and symbols. You can uncheck Hide the password if you'd like to see what you are typing, this will not affect the strength of the password.

6. Then click on OK and the Zip file will be created on your desktop.

7. You must then delete the non-zipped file or folder from your desktop and then open up the Recycle Bin and delete the file from there as well.

8. The Zip file can either stay on your desktop or you can move it to a flash drive or write it to a CD/DVD

9. The password should be sent to the client either through telephone communication or by a separate e-mail. Never place a copy of the password on the flash drive on CD/DVD.

Creating an Encrypted Zip File (newer versions of WinZip)

1. If you are zipping one file right click on it, if you are zipping multiple files, move them into a folder and click on the folder.

2. Then highlight WinZip and an additional menu will appear and choose Add to Zip File…
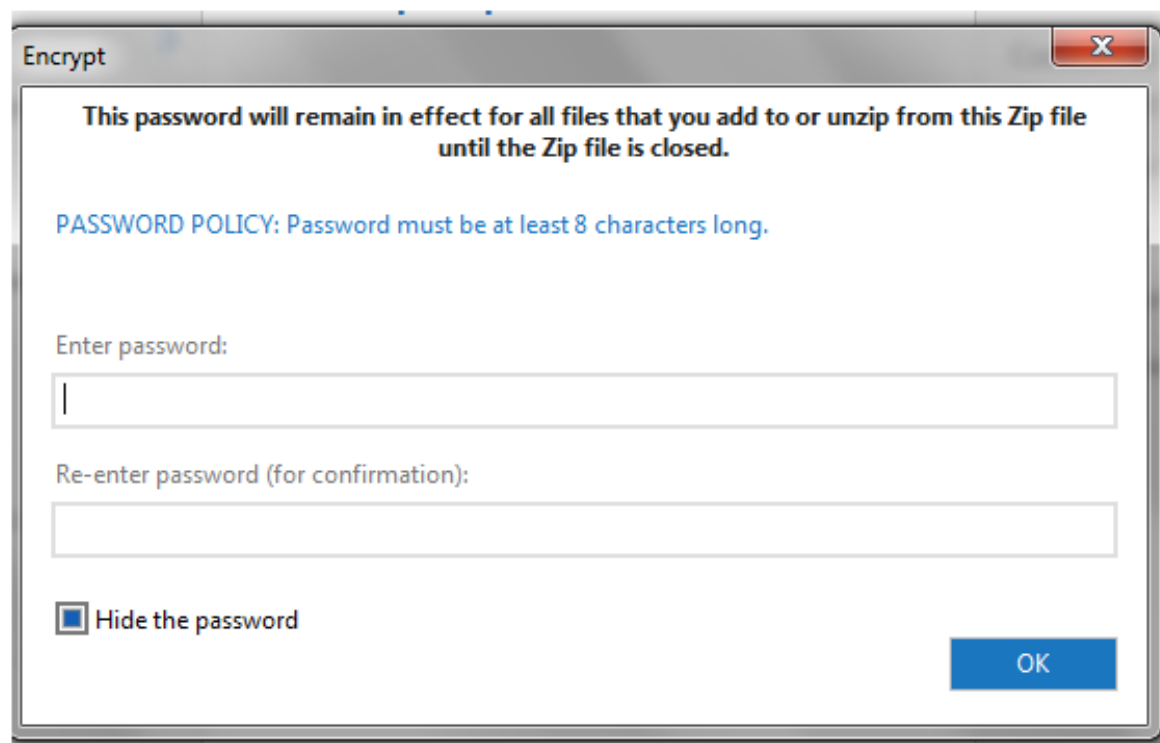
3. In the window that opens, click on Encrypt files
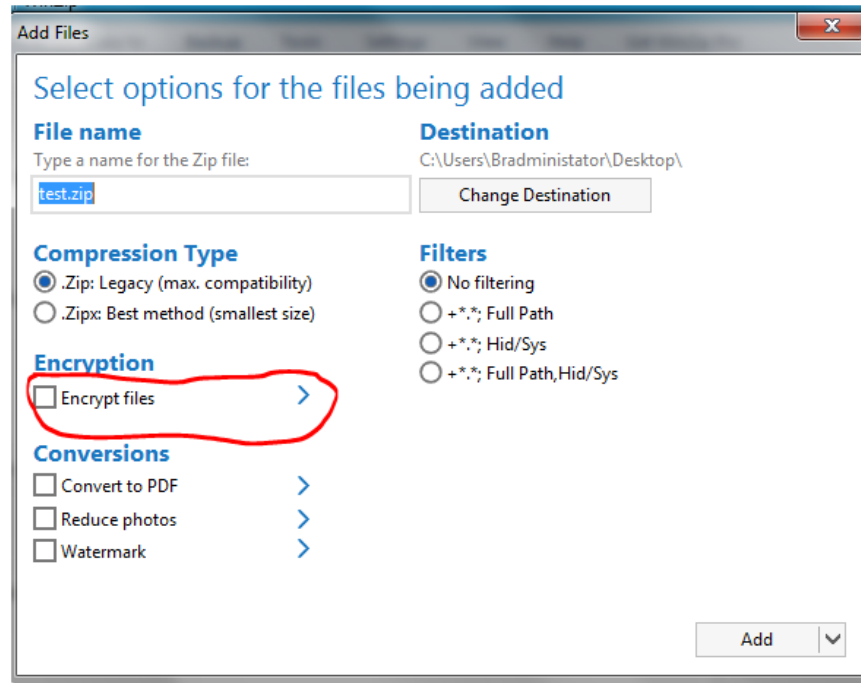
File Encryption – Creating Encrypted .zip Files (newer versions of WinZip)
Setting Destination

4. Now make sure the destination is properly set. The Desktop is the easiest place to find the file. If you need to change the location, click on Change Destination.
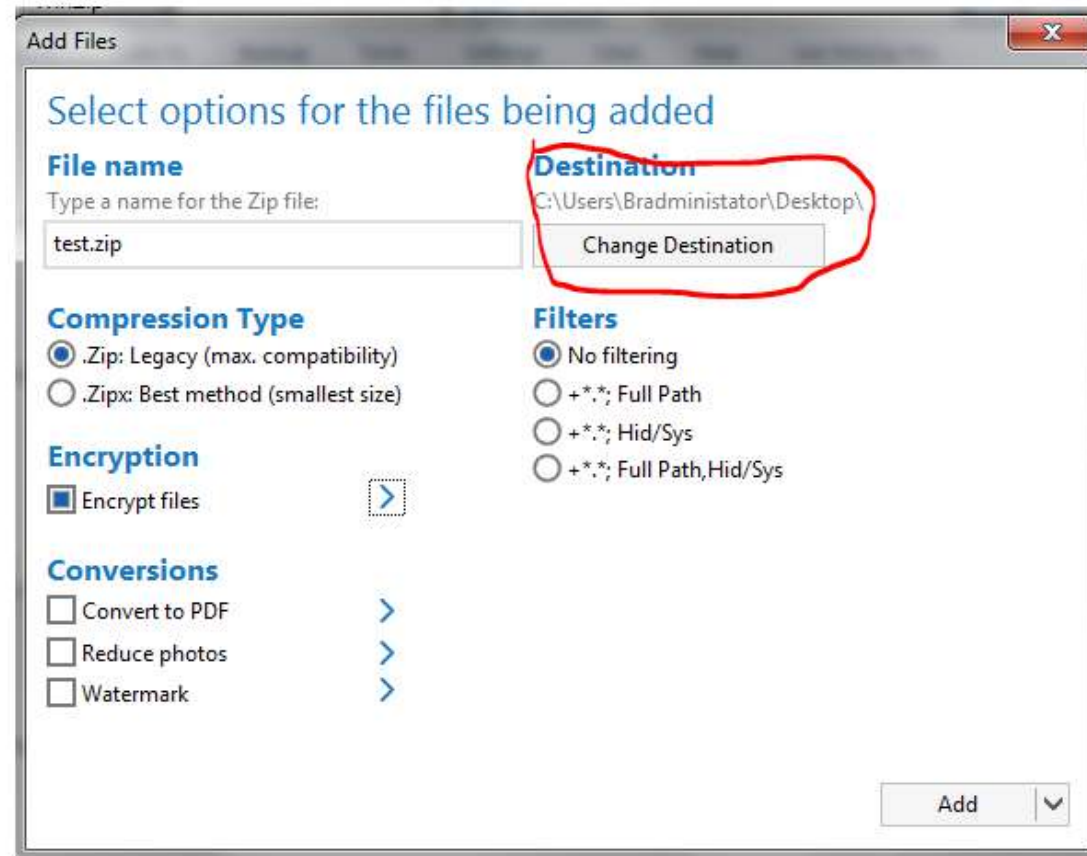
5. Then click on Add and the following window will appear:

Encrypt

This password will remain in effect for all files that you add to or unzip from this Zip file until the Zip file is closed.

PASSWORD POLICY: Password must be at least 8 characters long.

Enter password:

Re-enter password (for confirmation):

☒ Hide the password

OK

6. Enter a complex password (must be at least 8 characters long) with a combination of upper and lower case letters and numbers and symbols. You can uncheck Hide the password if you'd like to see what you are typing, this will not affect the strength of the password.

7. Then click on OK and the Zip file will be created on your desktop.

8. You must then delete the non-zipped file or folder from your desktop and then open up the Recycle Bin and delete the file from there as well.

9. The Zip file can either stay on your desktop or you can move it to a flash drive or write it to a CD/DVD

10. The password should be sent to the client either through telephone communication or by a separate e-mail. Never place a copy of the password on the flash drive on CD/DVD.

Deletion of Files

01

Deletion of files does not mean those files are gone.

02

It means that the files are not readily accessible, and probably would need to be forensically restored

03

Failure to delete files properly can damage your reputation and your desirability as a vendor

Things to Consider when Deleting Files

- Check everywhere – Word files, Excel files, e-mail files, .pdf files, etc.

- Any computer backup system may contain files that you wish to delete.
  - If at a company or firm, be aware of the document retention policy

- Consider whether you have an old computer that may contain files

- Don't donate computers without making sure your files are wiped

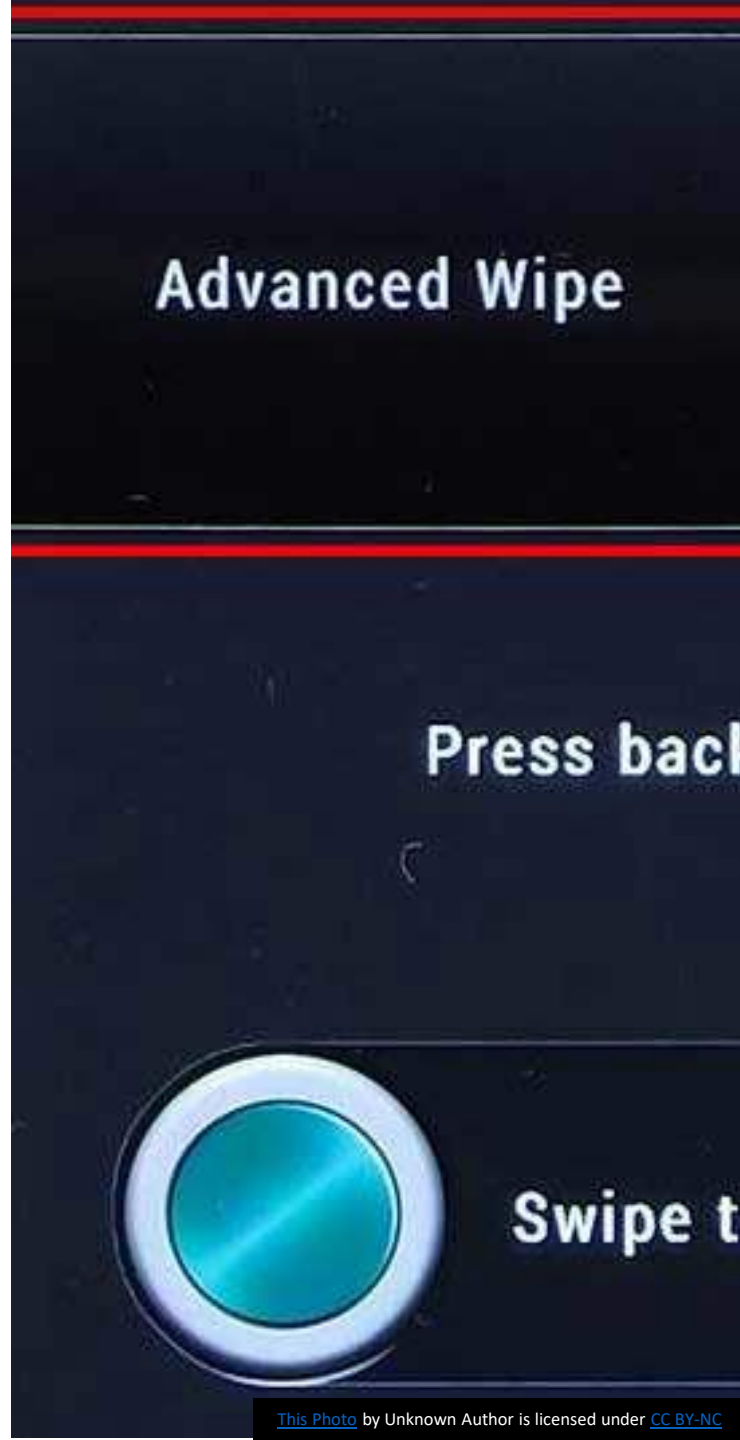- Terry Pratchett – when in doubt, use a steamroller

Mechanics of Deletion

- Right-click on file or folder and select "Delete" from drop-down menu

- This will send the file or folder to the Recycle Bin (PC) or Trash (Mac)

- Also need to empty the Recycle Bin or Trash to delete file or folder entirely

- The above applies for Word, Excel, or e-mail systems

Software for deletion

- For wiping a hard drive, there are various software solutions

- https://www.lifewire.com/free-data-destruction-software-programs-2626174
  - Identifies free programs that will wipe hard drive