Zipping Evidence Files: The Good, the Bad and the Ugly

What is a ZIP file?

File compression is an important part of the digital workspace. ZIP files use compression to send more data at faster speeds than unzipped files which is why ZIP files are such a popular tool for businesses across the world. But what exactly is a ZIP file? ZIP is a common file format that is used to compress one or more files together into a single location, reducing file size and makes it easier to transport or store. A recipient can unzip (or extract) a ZIP file after transport and use the file in the original format.

ZIP files work in much the same way as a standard folder on your computer. They contain data and files together in one place. However, with zipped files, the contents are compressed, which reduces the amount of data used by your computer. Another way to describe ZIP files is as an archive. The archive contains all the compressed files in one location. So, the ZIP file format is one option to use if you need to make a single file or group of files smaller.

How can you identify a ZIP archive file? Whenever you see the extensions .ZIP or .zip at the end of a file name, you're looking at a ZIP file. The icon that represents the file would also change. Say you have a photo named Evidence1.jpg. After you zip this photo, it would now read Evidence1.zip and have a new icon.

3rd Party tools: Is ZIP different from 7-ZIP or RAR?

When you're researching ZIP files, you may come across the term "7z file" or "7-ZIP." This is an archiving format that uses a higher compression ratio for fewer megabytes. While this smaller size is a positive, it also takes longer to process and is less convenient in to download and install a software application to use. This is also the case for RAR and TAR files as well as WinRAR, ZIPx, PeaZip and other third-party software apps.

How do ZIP files work?

ZIP files encode information into fewer bits by removing redundant data. This "lossless data compression" ensures all the original data is intact. Let's look at a quick example to explain how this works.

Imagine a file that contains the following sentences:

- The best sharing and storage solution for your business
- Your business solution for the best sharing and storage

Each word in this file appears twice. Now, if each letter and space in the sentence equals one unit of memory, then the entire file size would be 110 units. But you can create a numbered code to express the data in a different way:

- The best sharing and storage solution for your business
- 123456789

Or to put it a different way, both sentences would now read: 123456789896712345. This means that the initial file size of 110 units is reduced to 18 units, which is a massive savings. The ZIP file format uses lossless compression algorithms to express the same information in a more efficient way by removing the redundant data from the file. This also means it is faster to send a ZIP file.

When to use ZIP files at work

There are a broad range of potential uses for zipped files in a business setting. Being able to send large numbers of files over email is imperative. Say you need to send a big batch of files to a colleague or client. If you try to send all the files at once in an email attachment, you will get an error message because of file size. You could try to send each file in separate emails, but this is time consuming, labor intensive, and could lead to duplicate files. Instead, you can zip the files and attach the now single ZIP file to your email and send. Your recipient can then unzip the file by downloading and clicking.

You should also consider any potential storage saving. Zipping your files can help to reduce the amount of space they use on your computer's hard drive.

What are the advantages, disadvantages, and facts of dealing with evidence files in a ZIP file format?

The Advantages (The Good)

Zipped files save storage space and increase the efficiency of your computer. It is also an effective way to improve file transfers to send emails faster with smaller files. Furthermore, the ZIP file format will encrypt your data to maintain your privacy when sending files over the internet. In short, it's a simple way to maximize the efficiency of your file handling. It also a somewhat easy process to make a ZIP file on a Mac or PC. Windows and Mac OS have different methods, but they both begin with a right click. For the recipients, it is simple to unzip files; all it takes is a download and a click, regardless of their computer's operating system.

The Disadvantages (The Bad)

There are a range of disadvantages associated with ZIP files. Some of these issues include:

- File size limits
- File type limits
- Corruption
- Mobility issues
- Creation time and space
- Security

ZIP archive files have compression limits. Some files cannot be compressed much more than they already are. This is especially true for video files, MP3 files and JPG files. So, if you frequently work with video and image files, the ZIP format will not help you save very much storage space.

When using ZIP, you also need to think about the security aspect of zipped files. Completed zipped files are encrypted, but you don't know what happens to your file if you upload a third-party app. ZIP file extensions can also get corrupted. In some cases, corrupted data can affect the entire ZIP folder. ZIP files are also difficult to use if you are on the go. If you're using a phone or tablet, you would need to use a file saved on your phone and a third-party app. This method would create problems with both file storage space as well as security.

Another disadvantage of creating Zip files, is the time it takes to create them and the space it requires. ZIP files take 3 times the amount of storage for the creation process. First, you need to place all the files into one folder (staging) to create the Zip file. (Imagine taking files from a thumb drive, a USB HDD, a DVD, an SD card, and a network storage device and having to copy all the files to a single location on your PC/MAC.) That staging just doubled your storage and you now run the risk of corrupting the files in the copy/paste process. This process will also take a long period of time based on the size of each file; a 1GB file can take 24 seconds or longer to copy and paste. Next you run the Zip tool and it essentially makes a third copy, with the

completed Zip file; this has now tripled your storage. Finally, you go back and delete the temporary staging folder, adding more time to the overall process.

Zipping up Evidence (The Ugly)

Digital Media Evidence (DME) can be extremely effective in legal proceedings. Potential evidence is readily available due to the abundance of surveillance cameras, smartphones, and mobile devices. These devises are now mainstream, readily available, and more affordable than ever, making DME a part of nearly every legal claim. But is DME by default always admissible in court? No. It very much depends on how it is captured, secured, authenticated, and stored.

For DME to be admissible in court it must meet two basic requirements: relevance and authenticity. For evidence to be relevant it must have probative value. In other words, it must either support or undermine the truth of any point at issue in the legal proceedings. For evidence to be authenticated, it must accurately represent its subject as related to the legal claim, deemed the original and can be authenticated. Demonstrative evidence such as a video cannot come from anywhere. It must be brought forth by someone who can testify in court to the legitimacy of the video. Many people assume that social media videos online can be used as evidence in a trial to support their case. But for such footage to be admissible, your attorney must recover the **original video evidence**.

While photos and videos may seem like concrete, immutable representations of reality, the fact is that this evidence can be manipulated to skew that reality. Lighting, position, perception, filters, and editing can be strategically used to misrepresent the facts. Attorneys know this and will use objection tactics to claim that the evidence should be inadmissible. The following are some of the most common objections to Digital Media Evidence:

- **Undue Prejudice:** An attorney can argue that the photo or video evidence is not a reasonable representation of its subject and may result in undue prejudice.
- **Hearsay:** If there is no witness present who can be cross-examined, an attorney can argue that the substance of the photo or video evidence is hearsay.
- **The Best Evidence Rule:** If the photo or video is secondary evidence (a copy or facsimile), an attorney can argue that the **original copy** is superior evidence.
- **Lack of Foundation:** When visibility, the time of day, the weather or some other factor is an issue in the litigation, an attorney can question a substantial similarity between the occurrence in question and the photo or video evidence.
- **Chain of Custody:** The chain of custody is the most critical process of evidence documentation. It is a must to assure the court of law that the evidence is authentic, i.e., it is the **same evidence seized and secured** at the crime scene.

DME in the form of video and audio is the most difficult to process as evidence. Many forms of video files are proprietary and are wrapped up with their software players, CODECS, and supporting files. These players and supporting files need to be kept in their specific file order or the video will not play and therefore will not be authenticated.

Many Law Enforcement Agencies just simply Zip up proprietary media files because they have no other way to keep all the DME and related software in one location for investigation and distribution to the legal process with their IT infrastructure and Evidence Management Solutions. Many manufactures of Digital Evidence Management or Case Management Systems require or recommend to simply Zip the files up and submit them to their software. The issues and concerns regarding Zipping up evidence now become abundant and obvious. These glaring drawbacks of ZIP files introduce more reasons the defense can get the evidence thrown out of court. Once this has been done, precedence has been set. The following questions are just some of many, that are now being asked by legal teams…

Are these still the original files?

How can you prove it after being Zipped-up?

Was each evidence file hashed prior to Zipping it up or did the Zipped-up file get hashed?

How do I know the files didn't get corrupted in the copy/paste via a computer process?

How do I know the files didn't get corrupted in the compression process?

Any of these questions would be valid points for the defense to bring up if they discover the workflow process includes a Zip process in the Chain of Custody. If this was the OJ Simpson trial and the prosecutors presented the Dream Team (Robert Shapiro, Johnnie Cochran, Robert Kardashian) with a condemning video, this would be in their list of questions for the courts.

What is an alternative to a ZIP file?

Case-Paks from **Dynamic Workflow Solutions**. The **Case-Pak** is an extension of the **Data-Central (DC)** workflow. It empowers users to create an evidence package that includes the database and all its files, including proprietary first instance, "original" DME, and MP4 video work product. The files can also be placed in a specific order regardless of their file name, allowing a synced copy with the investigator / prosecutor case timeline and report to display in court. The **Case-Pak** can then be transferred ANY way the user/s require, including, but not limited to:

Cloud

On Premise Servers

USB Drives

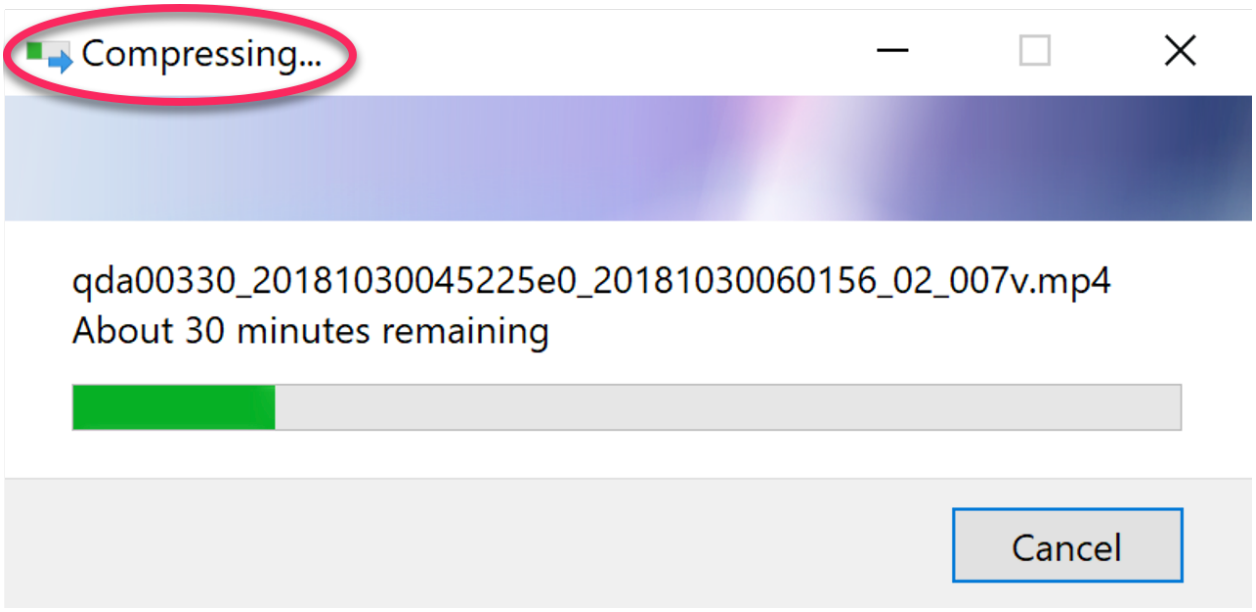
Automated Disk Burning with Labels via Rimage

Case-Paks create a SHA-256 Hash and a unique ID for every file, while maintaining the original file folder structure and the parent/child relationship, between the original first instance and the newly created work product/s. **Case-Paks** are encrypted using AES256 encryption and can only be decrypted by **DC** and the password that the original creator used. When a user creates or decrypts a **Case-Pak**, they are given the option to include the Case #, Case information (i.e., meta-data), and the file notes, allowing specific information to be shared or kept private upon decrypting the **Case-Pak**.

The original evidence files are always kept whole and complete and are authenticated during the **Case-Pak** creation/encryption and during the decryption process via the SHA-256 Hash. There is never a question regarding the authenticity of each file in the **Case-Pak** process. **Case-Paks** are not compressed. Through the **(FREE) Case-Pak Viewer**, files can be kept in the order they were intended for the courts and to maintain/show the case timeline.

Unlike Zip files, the user doesn't need to copy/paste the files into a staging folder first to create a **Case-Pak**. The files, (spread-out through DVDs, thumb drives, USB HDD, network drives, SD cards and more), can be streamed directly into the **Case-Pak,** saving time and the risk of a corrupted copy/paste process. It also eliminates the need to triple the storage in the process.

Looking at a real-world example, we will use a case that is made up of 163 files and is 6.46 GB in size. These files are comprised of audio files, photos, proprietary video files, standard video files, and documents, and then placed in a specific case timeline order. Using the built in Windows Zip function, it took minutes to create a Zip file. This does not even take into account the copy/paste process to get all the files into a single staging folder prior to the Zip process.



Using **Data-Central** to create the **Case-Pak,** only took 85 seconds, and the files were pulled directly from the secondary devices. The **Case-Pak** creation includes the AES-256 encryption and the DB containing all the metadata related to the files and the case. The Zip files' size is 6.33GB and the **Case-Paks'** size is 6.46GB. To unzip the file through Windows, it took over 2

minutes and the file order is not the same as the original case timeline; it's in a Windows default order. To decrypt the **Case-Pak**, it took 46 seconds, which included the SHA-256 Hash validating and setting up the file index/case timeline along with the DB.

Clearly based on the information above, **Case-Paks** save the user valuable time and ensure the evidence is admissible in court. **Case-Paks** are also inexpensive. For example, a 10 GB **Case-Pak** with proprietary video conversion would cost less than a bottle of water. A 100 GB **Case-Pak** with proprietary video conversion would cost less than a lunch. A 256 GB Cell Phone Dump without conversion would be less expensive than a dinner.

Once the **Case-Pak** has been created there are no additional fees. In fact, the **Case-Pak** can be shared with whomever you choose, and a **FREE Case-Pak Viewer** is used to decrypt, search, and view all the files. The **FREE Case-Pak Viewer** comes with a wildcard search and a nested filter feature, capable of complex sorts to go through 1000s of files and display only the key important files.

For more information or a demo: CLICK HERE

dynamicworkflowsolutions.com