

ACTIVISTS'



WITNESS
SEE IT
FILM IT
CHANGE IT

GUIDEto

ARCHIVING

VIDEO



archiveguide.witness.org

TABLE OF CONTENTS

START HERE PG. 3

Who is this Guide for?	pg. 3
Why Archive?	pg. 3
What is Archiving?	pg. 4
How to Use this Guide.....	pg. 5

THE WORKFLOW PG. 8

Create	pg. 8
Transfer	pg. 18
Acquire	pg. 29
Organize	pg. 37
Store	pg. 48
Catalog	pg. 57
Preserve	pg. 68
Share	pg. 75

VIDEO AS EVIDENCE PG. 86

KEY CONCEPTS PG. 88

GLOSSARY PG. 92

PLEASE NOTE

Words highlighted in **orange** are internal links to Glossary and Key Concepts terms, or to other sections in the Guide. Click on the links or look up the terms, which are alphabetized in the back of the Guide.

Words highlighted in grey and underlined are links to external resources. Click on the links or look up the URL in the footnotes.

START HERE

WHO IS THIS GUIDE FOR?

- You are a human rights activist, a small or grassroots human rights organization, or media collective;
- You are creating or collecting **digital video** to document human rights abuses or issues, and;
- You want to make sure that the video documentation you have created or collected can be used for advocacy, as **evidence**, for education or historical memory - not just now but into the future....
- But you are not sure where to begin, or you are stuck on a particular problem.

If this is you, then this Guide is for you.



WHY ARCHIVE?

With everything else you need to think about and do - why archive?

Ask yourself:

- Do you want your videos to be available in the future?
- Do you want your videos to serve as **evidence** of crimes or human rights abuses?
- Do you want your videos to raise awareness and educate future generations?

If the answer is yes, it is important to begin thinking about **archiving** before it is too late.



One reason to archive your videos.

Still not sure? Here is what might happen if you do not take steps to archive.

- Your videos may be accidentally or deliberately deleted and lost forever.
- Your videos may exist somewhere, but no one can find them.
- Someone may find your videos, but no one can understand what they are about.
- Your videos cannot be sufficiently **authenticated** or corroborated as evidence.
- Your videos' quality may become so degraded that no one can use them.
- Your videos may be in a **format** that eventually no one can play.

WHAT IS ARCHIVING?

ARCHIVING IS... a general term for the range of practices and decisions that support the long-term **preservation**, use, and accessibility of content with enduring value. In this Guide, our focus is on your **digital videos**.

ARCHIVING IS ... an ongoing process that begins when a video is created and continues infinitely into the future.

ARCHIVING IS...a process that can be incorporated into your existing video **workflows**.

ARCHIVING IS ... a way to ensure your videos remain **authentic** and intact, so you can use them as **evidence**.

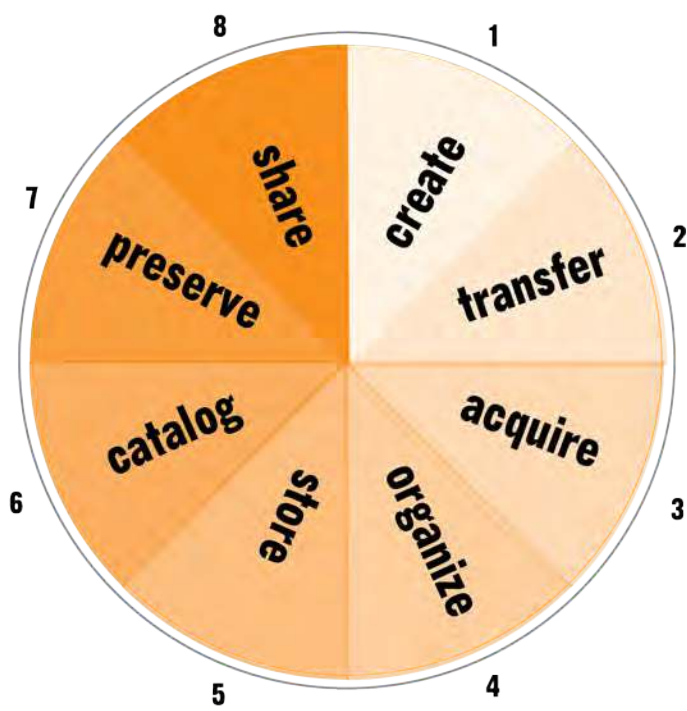
ARCHIVING IS ... a way to ensure your videos are available, findable and playable long into the future.

ARCHIVING IS NOT... a one-time action.

ARCHIVING IS NOT... putting your videos on a hard drive and leaving it on a shelf.

HOW TO USE THIS GUIDE

This Guide is organized into 8 sections focused on stages in a video **archiving workflow**:



Stages in a video archiving workflow.

Are you looking for information about a specific topic or stage of archiving, such as **metadata**, storage devices, or **cataloging**? Jump in via any of the Workflow topics or look at the “**Key Concepts**” page.

NOT SURE WHERE TO BEGIN?

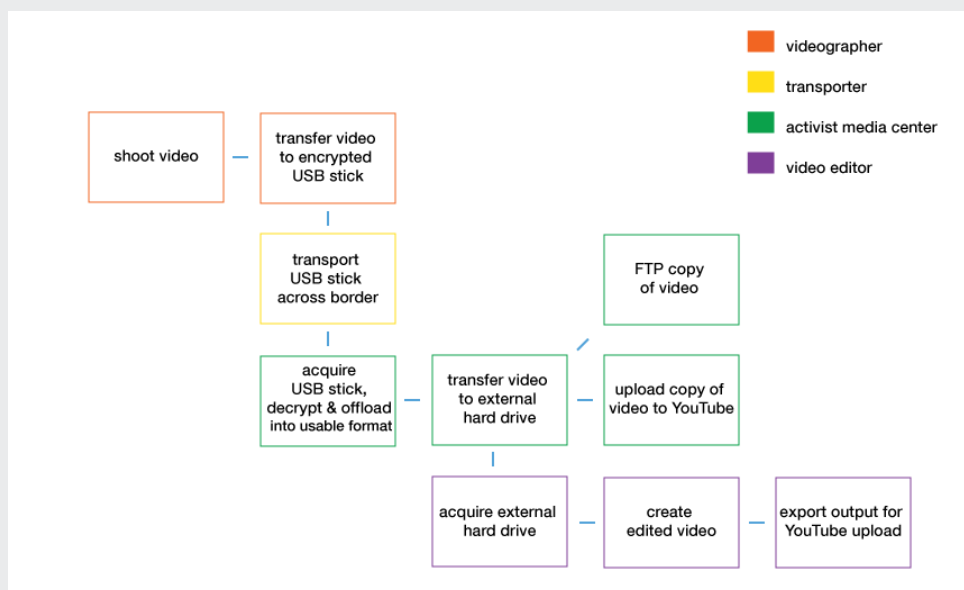
If you are unsure how to incorporate the video archiving stages above into your current situation, one place to start is to chart your current video workflow. A workflow is a map of processes and roles for activities that require multiple actions and usually more than one person. Visualizing how you or your organization works can help you build and improve on the way you get things done. See the scenario below for an example of a workflow.

Once you map your existing workflow, it will be easier to see where the archiving stages can fit in. In some cases, it might just mean making slight changes to something you are already doing. In other cases, it might mean introducing entirely new steps in your workflow. Everyone's workflows are different, and everyone will incorporate these archiving stages in different ways.

As you read through this Guide, you will be able to determine what you can easily incorporate and what might take more planning. Do not become discouraged! Building an archiving workflow takes time, but every small step you take along the way contributes to the survival of your videos and increases their ability to be used in the future.

A SCENARIO AN ACTIVIST MEDIA CENTER

The Activist Media Center has an efficient workflow for getting newsworthy videos online in a timely manner, but has not given much thought to the videos' long-term usability up to now.

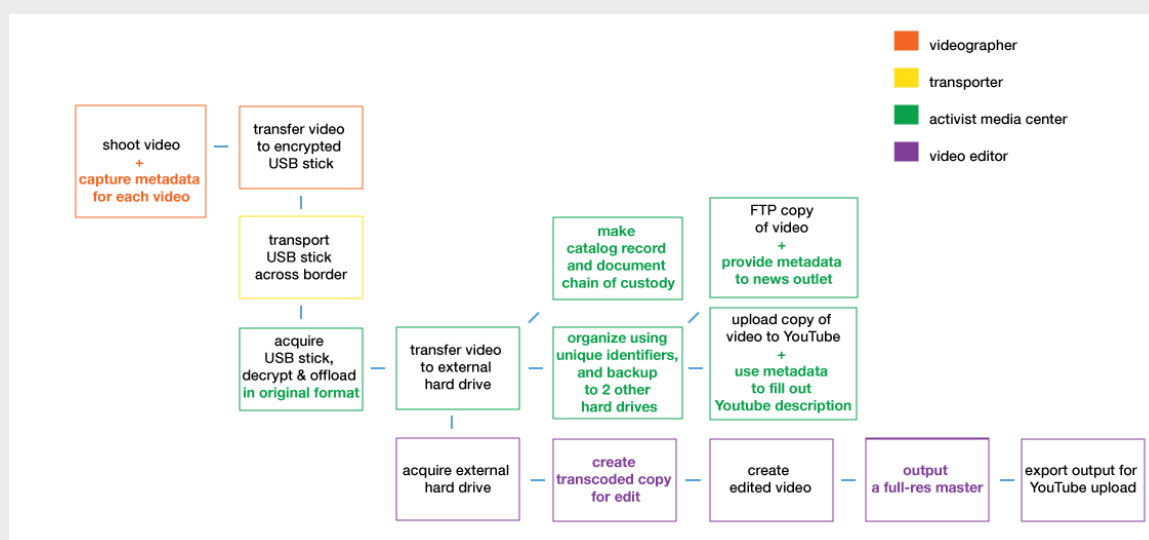


An efficient workflow for getting videos online, but not for long-term usability.

As they collect more and more videos, the Media Center starts to see the potential value of the collection to future legal cases, and as a historical record of events. However, the way they have organized their videos is not consistent, and only one person really knows how to find the older videos. They also realize that media outlets are having a hard time verifying their videos, and that it would be hard for the Media Center to prove that its videos are **authentic**. Then, one day, someone accidentally drops a cup of coffee onto one of the hard drives and it immediately stops working. Because the Media Center does not have a **backup** copy, the videos on that drive are permanently lost.

In an effort to improve their practices, the Media Center adds some archive-minded steps to their workflow.

- The Videographer notes important **metadata** for each video, such as date, location, **hash value** and her name, in a document that she includes with her videos on the **encrypted** USB stick.
- After receiving and decrypting the USB stick, the Media Center offloads the **original files** to its primary storage.
- The Media Center organizes the videos and makes backup copies on 2 additional hard drives.
- The Media Center makes a **catalog** record for each video in a database, expanding on the metadata provided by the videographer, to make the videos findable.
- The Media Center adds detailed titles and descriptions to its YouTube videos, and provides descriptions along with videos to news outlets.
- Instead of **transcoding** videos during **offload**, the Video Editor makes transcoded copies from the offloaded original files.
- The Video Editor outputs a full quality **master** of her edited video in addition to the lower quality output she uploads to YouTube.



A few steps are added to the video workflow to improve the long-term usability of the videos.

READY TO START?

In the menu, look under “The Workflow” to find out more about the stages in the video archiving process. Start with “**Create**” and follow along, or jump to any particular stage you want to learn more about.

THE WORKFLOW: CREATE

CREATE: INTRODUCTION

Archiving begins from the moment of creation, when you record raw video footage on a camera. At this key stage, there is important information about the video that must be captured to enable identification, authentication and use of the video later on.

This information is known as **metadata**. You can create video metadata in an automated or manual fashion. You can do it in the camera and **embed** it in the video file, or record it separately in a spreadsheet, text file, email, or handwritten note. You should also collect any documents related to your videos, such as consent forms or production notes.

Archiving also begins when you create new edited videos using editing software. The choices you make about what to output and keep from your editing project can affect a video's usability later on.

A SCENARIO A VIDEO IN CONTEXT



<http://youtu.be/03P83yQhjd8> This video was recorded on April 9, 2012 in Homs, Syria, showing that an upsurge of violence occurred in the lead-up to a UN-brokered ceasefire agreement that called for a withdrawal of heavy weapons from built-up areas and a complete cessation of hostilities on April 12, 2012.

Note how the videographers state the date and location in which the video was recorded in the video's audio. This basic metadata is central to the video's significance, and allows it to be verified, understood and contextualized in relation to external information, like the date of the ceasefire agreement.

CAUTION!

PROTECT SENSITIVE INFORMATION

Video metadata can contain private or sensitive information like names or locations that can put you or other people at risk. If you have sensitive data, choose methods of capturing metadata that allow you to either **encrypt** the data, separate it from other data, or keep it in a safe location. Be aware of what metadata your camera embeds automatically (case in point [here](#))¹.

GET INFORMED CONSENT

You cannot be sure that sensitive information will never be compromised. Consider the risks to yourself, and inform the people you are filming about the risks and get their consent to be filmed. See WITNESS's [Informed Consent](#)² tips for more information.

BE SAFE WHEN RECORDING

See WITNESS's [Safety and Security](#) tips for more information.



CREATE: WHAT METADATA TO CAPTURE

Key contextual information about your video needs to be captured at the time it is created. This **metadata** is critical to the video's **authenticity**, and to the ability to find, use, and understand the video.

The key pieces of information to capture at the point of creation are:

WHEN The date and time recorded / created.

WHERE The geographic location of recording.

WHAT AND WHY A basic description - the important details about the event recorded that would be difficult to identify later (e.g. people's names, the purpose for recording) or that make the event significant (e.g. shelling during a ceasefire, violence against civilians).

WHO The video's source. The full name (or pseudonym, if not safe) and contact information (if safe to provide) of the video's creator.

VIDEO AS EVIDENCE TIP

Hash values are another type of metadata that are particularly important for evidentiary video.

They can be used to show whether your files have been tampered with over time, so it is valuable to capture them as early as possible in the video lifecycle.

Some recording devices may be able to embed hashes in the video file at the point of creation. Otherwise, you can compute hashes after you offload them to a computer (see ["Transfer"](#) for more information on how to do this).

¹ <http://cbsn.ws/1vZTKVd>

² <http://library.witness.org/product/obtaining-informed-consent/>

SECURITY REQUIREMENTS Whether or not the identities of the video’s subjects or creator need to be protected.

Other information, such as detailed descriptions or keywords, will be important to making your video more findable and understandable but are not critical at this stage. Additional information can be added later at different stages of the workflow (see “[Catalog](#)”).

CREATE: HOW TO CAPTURE METADATA AND DOCUMENTATION

There are many ways to capture **metadata** about your video at the point of creation. Information can be captured in an automated or manual fashion, and can be **embedded** in the video file or recorded in a separate document. Different methods have different safety and security risks and logistical requirements.

The basic ways to capture information about your video are:

CAMERA SETTINGS

Depending on your camera, you may be able to embed the date, time, geolocation, creator’s name, and other metadata in the video file. Check your settings to see if these features are turned on and if they are correct. Also, if you have options for recording format, select the highest quality ones that your camera allows.

- **Advantage** Embedding information in the file metadata means that the information stays with the file, as long as the file is unaltered.
- **Disadvantage** You cannot hide this information without encrypting the video. If you do not want your location known, for example, geolocation metadata is a security risk.



You can enable and embed metadata with your camera settings.

	/958_0167.MOV
Format	MPEG-4
Format profile	QuickTime
Codec ID	qt
File size	63.5 MiB
Duration	47s 948ms
Overall bit rate mode	Variable
Overall bit rate	11.1 Mbps
Movie name/More	KODAK Zi8 Pocket Video Camera
Encoded date	UTC 2009-01-02 01:12:31
Tagged date	UTC 2009-01-02 01:12:31
Origin	Digital Camera
AMBA	
▼ Video	
ID	1
Format	AVC
Format/Info	Advanced Video Codec
Format profile	Main@L4.2
Format settings, CABAC	Yes
Format settings, ReFrames	4 frames
Format settings, GOP	M=3, N=15
Codec ID	avc1
Codec ID/Info	Advanced Video Coding
Duration	47s 948ms
Bit rate mode	Variable
Bit rate	11.0 Mbps
Maximum bit rate	17.7 Mbps
Width	1 920 pixels
Height	1 080 pixels
Display aspect ratio	16:9
Frame rate mode	Constant
Frame rate	29.970 fps
Color space	YUV
Chroma subsampling	4:2:0

Just some of the metadata captured by your camera.

Try This BASIC

To see what metadata your camera has embedded in your video files, use [MediaInfo](#)³ (\$0.99, **GUI** version) to display the metadata.

Try This ADVANCED

The free version of [MediaInfo](#)⁴ displays metadata embedded in video and audio files in the **command-line**.

Try This ADVANCED

[Exiftool](#)⁵ is another command-line tool that displays metadata embedded in photo and video files, and allows you to add metadata to photo files.

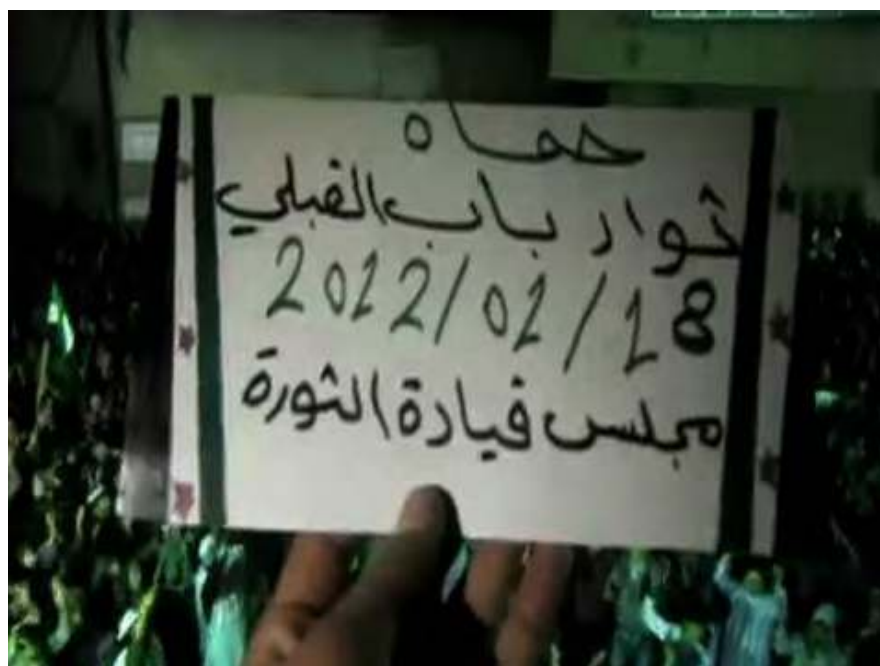
³ <https://itunes.apple.com/app/mediainfo/id510620098>

⁴ <http://mediaarea.net/en/MediaInfo>

⁵ <http://www.sno.phy.queensu.ca/~phil/exiftool/>

RECORD ON-CAMERA

While recording a video, speak into the camera; hold a sign in front of it (similar to the idea of using a slate or clapboard in a film); or film things (like signposts, clocks, recognizable landmarks) to capture key contextual information in the video itself. If you have a choice of recording formats, film in the highest quality that your camera allows.



You can record important metadata in the video itself.

- **Advantage:** The information stays with the video, even if the file is **transcoded** and loses the metadata embedded in the file.
- **Disadvantage:** Someone needs to actually view the video to find this information; the information is not searchable unless someone transcribes it. You may also need to edit the video before sharing it if the information has security restrictions.

RECORD ON-CAMERA, IN A SEPARATE FILE

Similar to the method above, except you record the information in a separate file by stopping and starting the camera, or using a different feature (e.g. a Voice Note on your mobile phone).

- **Advantage:** Almost as easy as the method above, and eliminates the need to edit the video before sharing if the information has security restrictions.
- **Disadvantage:** You will need to make sure the two files remain associated with each other later on; and someone still needs to view or listen to the additional file to get the information.

ENTER IN A PRE-FORMATTED TEMPLATE

Create a template using a spreadsheet or other application with columns or fields for each piece of metadata. Fill it out electronically (e.g. using a computer or tablet), or print it out and fill it out by hand.

Media Summary		
Camera Person / Interviewer Name		
Filming Date		
Title		
Name(s) of Interviewees / People Depicted (unless there are security issues)		
Location (unless there are security issues)		
Language(s) Spoken		
Security	Use of Face Allowed?	
	Use of Full Name Allowed?	
	Use of Location Allowed?	
Summary / Description Provide a description of the events, people, and places depicted in the footage, including relevant background information.		

You can create and enter metadata into a preformatted template.

- **Advantage:** Prompts you to enter key information. If entered electronically, the information can be easily searched or brought into other applications later on.
- **Disadvantage:** It can be cumbersome to have and fill out the template in some recording situations; you also have to make sure the document remains associated with the video. If entering electronically, your device needs to have the appropriate software and template loaded.

ENTER IN AN ELECTRONIC TEXT DOCUMENT

Enter metadata using any text editor available on your computer, tablet, or smartphone.

The screenshot shows a text editor window with the title '2012_01_28_MilesArrest'. The text inside the document is as follows:

```
When: 2013-01-28 12:24am
Where: Cass Ave and Martin Luther King Jr Blvd, Detroit, MI, USA
What and why: Arrest of Davis Miles, excessive police force
Recorded by: Shira Fennesz, SFenn@email.com
Security: Do not share contact information
```

You can enter data in a text document.

- **Advantage:** Uses available tools at hand. Choose an application that allows you to save/export your document as plain-text (.txt) from your device.
- **Disadvantage:** A device is required; as with using a template, it can be cumbersome to fill out; and you have to make sure the document remains associated with the video.

ENTER IN AN EMAIL OR ONLINE DOCUMENT

Similar to the two methods above, except you fill out the metadata online or send it to someone (potentially with the video file).

- **Advantage:** Metadata can be sent to a safe location.
- **Disadvantage:** The video needs to be matched with and remain associated with the document.

HAND-WRITE ON PAPER

You can simply write down information on paper (use a printed, pre-formatted template if possible). Metadata in any form is better than none at all.



You can write down metadata by hand.

- **Advantage:** It does not require a computer or other device.
- **Disadvantage:** Your notes need to be physically transported or scanned to be shared with anyone, and may subsequently need to be transcribed.

COLLECT RELATED DOCUMENTS

In addition to capturing metadata in the ways above, collect any existing documents that relate to the video, such as production notes, consent forms, or logs.

- **Advantage:** These documents can contain valuable information about the video and the context of its creation.
- **Disadvantage:** You need to make sure the documents remain associated with the video. See the “**Transfer**” section on information packages.

CREATE: OUTPUTTING EDITED VIDEOS

New videos are created when you edit raw footage together or add new components to raw video footage like titles or graphics, and **output** or export them from editing software.

OUTPUT AT FULL RESOLUTION

Always output or export a full-quality **master** video (i.e. in the **format** in which the video was edited), even if you do not have an immediate use for it. This is especially important if you will not have access to the raw footage later on. You can export additional copies in other formats as needed.

Name	Size
Ken02_SinaiAnne_Master.mov	588.9 MB
Ken02_SinaiAnne_WebUpload.mov	33.9 MB

NAMING OUTPUTTED FILES

You will need to provide filenames for your outputted videos. Create a filenames convention so that you name all of the files you create consistently. If you use unique identifiers, you can include the unique identifier for the video in the filename. For example, you can name your outputted files according to a template like this:

ID_Title_Version_DateOutput

Name
P0112_TahrirSquareProtest_Arabic_20110201.flv
P0112_TahrirSquareProtest_English_20110201.flv

Name your edited video files consistently, following a template.

KEEP PROJECT FILES

Save your project files (e.g. the .fcp file), as it shows how you made your video. It is also useful in case you ever need to re-edit the video. You may need to re-edit, for example, if you find an error, if the situation changes and you need to update information, or if you want to make a new version of the video. For the same reason, it is a good idea to keep graphics or any other elements that were created for the video.

Since this project file can usually only be opened in the application that created it, you should also export the project information in an **edit decision list (EDL)** or other interchange format (e.g. Final Cut Pro XML Interchange Format).

INCLUDE METADATA IN YOUR EDITED VIDEOS

An easy way to ensure that **metadata** stays with your video is to include it in the video itself. With edited videos, you can add slates, title cards, lower thirds, subtitles, logos or credit rolls to display key information about your video.



You can include important metadata in the edited video itself.

CREATE: TAKEAWAYS

- The most important **metadata** to capture when recording a video are: date and time, geographic location, basic description, safety and security requirements, and who shot the video.
- Other information can be added later to aid understandability and findability of the video.
- There are many ways to capture information, including using camera settings to automatically embed data, or using a separate pre-formatted template like a spreadsheet.
- Different ways of capturing information have different safety and security risks and logistical requirements.
- When creating edited videos, output at full resolution, name your video files consistently, and keep your project files.

KEY CONCEPTS IN THIS SECTION

Authenticity:

The concept of authenticity is based on the creator and the context of creation. This information must therefore be documented in order for authentication/verification to happen.

[Read More...](#)

Metadata:

Capturing metadata at this stage – before it is lost or forgotten – is critical for the identification, authentication, and use of the video.

[Read More...](#)

THE WORKFLOW: TRANSFER

TRANSFER: INTRODUCTION

Transfer refers to the electronic or physical movement of video, **metadata**, and related documentation from one device or location to another. Transferring can occur at any point in a workflow, and often happens at multiple points.

Transferring includes any kind of copying, **uploading**, or **downloading** of files between local or remote devices (e.g. camera to computer, camera to cloud service, hard drive to local server, etc.) and the physical transportation or shipment of storage devices, such as USB sticks or hard drives.

Ideally, the result of a transfer is a file that is **complete**, unaltered, and in its original **format**. Videos can be easily lost, altered, corrupted, or disassociated from each other and their metadata and documentation when transfers are not done properly. Transferring media can also be a very time consuming process, so it is important to transfer efficiently.

A SCENARIO

GETTING VIDEO TO ITS DESTINATION

The Citizen Journalists Network aims to get credible, high-quality video footage to major news outlets to highlight growing unrest in a remote area of their country. The Network needs to get video from this remote location to their contacts at BBC, CNN, and Al Jazeera without losing the metadata needed for verification, and without degrading the image/audio quality. The Network also needs to make sure that information with security restrictions is not released. What do they do?

- After recording, Saira offloads the unaltered **original files** from her camera onto two **encrypted** portable hard drives. She also puts a text file with metadata on the hard drives.
- Yaser physically carries one of the hard drives to the network's safe central location, while Saira holds on to the other copy for safekeeping.
- At the central location, Ahmed performs a virus check, then decrypts and copies the original files and additional metadata from the portable hard drive to their primary storage device, which is backed up.
- Hala looks at the footage, and checks whether there is sensitive information that needs to be restricted in the videos or its metadata before it is shared outside of the network.
- Hala selects and sends some original files with descriptions to her contacts in the news media via **FTP**.

CAUTION!

ENCRYPT FILES WHEN NECESSARY

If your videos or documentation contain confidential information and your transfer is at risk of interception, **encryption** can be used to prevent the information from being revealed. The interceptor cannot decrypt and read your files without a secret key. Note that encryption does not prevent your files from being intercepted. Also be aware that possession of encrypted information can be incriminating in some cases.

CHECK FOR VIRUSES

Malware like viruses and Trojans can spread through the Internet or on portable devices. Protect yourself from inadvertently acquiring malware by running virus check software on your computer and on portable devices before you transfer. If viruses are detected, clean your devices before transfer, and clean again after transfer. Also, only download or open attachments from known and trusted sources.

Try This BASIC

There are many commercially available virus scanners. Some free virus scanners include [ClamXAV](http://www.clamxav.com/index.php)⁶, [Immunet](http://www.immunet.com/main/index.html)⁷, and [ClamWin](http://www.clamwin.com)⁸.

Try This ADVANCED

[ClamAV](http://www.clamav.net/index.html)⁹ is an open source anti-virus engine for detecting Trojans, malware, viruses, and other malicious threats.

TRANSFER: OFFLOADING FROM CAMERAS

Unless you are **uploading** directly to the Internet from your camera, the first transfer you usually make after recording video footage is **offloading** from the camera to a computer. As with any kind of transfer, the aim is to obtain a copy of the video files that is **complete**, unaltered, and in its original **format**.



⁶ <http://www.clamxav.com/index.php>

⁷ <http://www.immunet.com/main/index.html>

⁸ <http://www.clamwin.com>

⁹ <http://www.clamav.net/index.html>

OFFLOADING IN THE FIELD

Transferring video in the field can be tricky; challenges include chaotic or unsafe surroundings, weather, or dirty environments. Bear in mind:

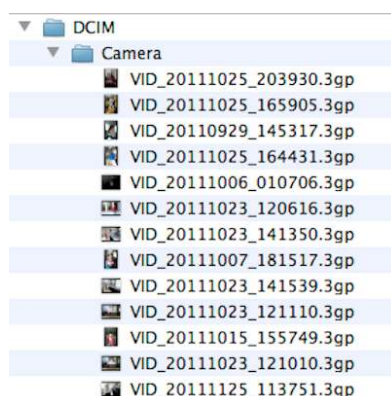
- If there is dirt and debris around, it is best to offload by plugging the camera into the computer rather than ejecting the card. SD cards are fragile, and can be easily damaged or lost.
- When offloading in the field, it is best to offload your footage twice and save it to two separate devices, before deleting the footage from the camera/card.

OFFLOADING FILES

To transfer video files from your camera or card to your computer in a way that preserves their **authenticity** and usability:

OFFLOAD THE ORIGINAL FILE

The **original file** is the most authentic and highest quality copy of your video, and contains valuable **embedded metadata**. Copy raw video files directly to your storage devices without altering them in any way. Avoid using the “import” function on video/photo software if possible, as some software may transcode (i.e. change the encoding format of) your video. In some cases, due to proprietary technology, it may be impossible for you to access your camera files directly in Windows Explorer or Finder (e.g. iPhone), or without using specific software to offload. With whatever software you use, try to copy the original file.



Offload your original files.

Try This ADVANCED

`rsync`¹⁰ is a **command-line** tool for transferring files that includes many options. Typically used for backup systems, but can be used for simple copying.

ALTERNATIVES TO THE ORIGINAL FILE

If it is not possible to obtain a copy of the original file, try to obtain a high quality copy in a current and widely used **format**. Note that important embedded metadata such as date and time recorded can be lost in transcoded copies. Changing the encoding format of your video can also result in files that are much larger than the originals (but not better quality), so ensure that you have sufficient storage capacity to handle these files.

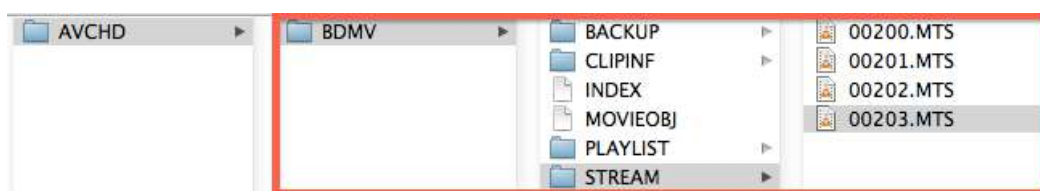
¹⁰ <http://rsync.samba.org/documentation.html>

Original Files			Transcoded Files		
Name	Size	Kind	Name	Size	Kind
00071.MTS	9.6 MB	MPEG-2 Transport Stream	00071.mov	164.3 MB	QuickTime Movie
00072.MTS	8.5 MB	MPEG-2 Transport Stream	00072.mov	160.9 MB	QuickTime Movie
00073.MTS	9.2 MB	MPEG-2 Transport Stream	00073.mov	159.5 MB	QuickTime Movie
00074.MTS	15.6 MB	MPEG-2 Transport Stream	00074.mov	183.4 MB	QuickTime Movie
00075.MTS	11.5 MB	MPEG-2 Transport Stream	00075.mov	152.9 MB	QuickTime Movie
00076.MTS	16.9 MB	MPEG-2 Transport Stream	00076.mov	305.4 MB	QuickTime Movie
00077.MTS	11.2 MB	MPEG-2 Transport Stream	00077.mov	198.6 MB	QuickTime Movie

Changing formats can result in lost metadata and larger files.

DO NOT RE-ORDER FILES OR CHANGE FILENAMES

Some video formats have directory structures that organize video streams, clip info, and other data in particular ways (e.g. AVCHD, XDCAM). This structure is important to the function of the video. When offloading, copy the entire directory tree without altering the structure or filenames.



Some video formats have complex structures that should not be altered.

MAKE TWO COPIES

Transfer your footage to two devices before deleting from the camera/card.

CHECK YOUR TRANSFER

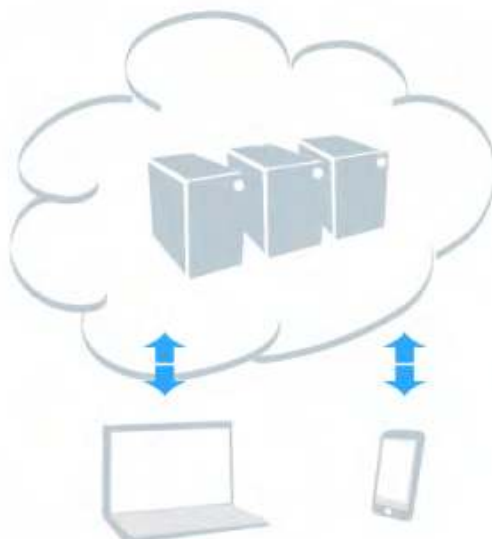
Do not delete the footage from the card or camera until you have confirmed that the files have copied properly. A simple, but not foolproof, way to check is to see if the file sizes and number of files match, and to play a sampling of the videos. To be more certain, compute and verify hashes before and after the files have copied. See the section on “[Keeping Files Intact \(and Proving It\)](#)” for more on how to do this.

TRANSFER: UPLOADING AND DOWNLOADING VIDEO

Video can be **uploaded** from a camera or from a computer to a remote system in order to allow someone in another location to view or **download** the video. The remote system could be one that you own and control, owned by an entity that you pay a subscription fee to use (e.g. Amazon, Dropbox), or owned by an entity that lets you upload for free (e.g. YouTube, Internet Archive).

VIDEO AS EVIDENCE TIP

Hash values can show whether your files have been tampered with, so it is valuable to compute and capture hashes early in the video lifecycle. Compute and keep a record of hashes as soon as you offload files from your camera.



TRANSFERRING VIDEO FILES

No matter how or where you upload and download, transfer video files in a way that preserves their **authenticity** and usability:

TRANSFER THE ORIGINAL FILE

For raw video footage, the **original file** is the most authentic and highest quality copy of your video, and contains valuable **embedded metadata**. Upload your original files to a location that will maintain their **integrity** and that will allow you to download without altering or **transcoding** the files. Always download original files if they are available.



Download original files if they are available.

ALTERNATIVES TO THE ORIGINAL FILE

If it is not possible to download the original file (e.g. if you are downloading from YouTube), obtain the highest quality copy available in a current and widely used format. Note that important embedded metadata (e.g. date and time recorded) can be lost in transcoded copies, so document and upload important metadata in a separate form (e.g. in your YouTube title and description).

Original File	
Format	MPEG-4
Format profile	QuickTime
Codec ID	qt
File size	965 KiB
Duration	11s 872ms
Overall bit rate	666 Kbps
Recorded date	2012-10-26T17:24:33-0400
Encoded date	UTC 2012-10-26 21:25:30
Tagged date	UTC 2012-10-26 21:25:35
Writing application	6.0
Writing library	Apple QuickTime
Make	Apple
©xyz	+40.6851-073.9742+040.776/
Model	iPhone 4S
com.apple.quicktime.make	Apple
com.apple.quicktime.creationdate	2012-10-26T17:24:33-0400
com.apple.quicktime.location.ISO6709	+40.6851-073.9742+040.776/
com.apple.quicktime.software	6.0
com.apple.quicktime.model	iPhone 4S
Transcoded File	
Format	Flash Video
File size	672 KiB
Duration	11s 867ms
Overall bit rate	458 Kbps
httpstheader	o-o---preferred---sn-a5m7zne1---v9---lscache6.c.youtube.com

Some metadata may be lost if you download transcoded files.

Try This ADVANCED

[YouTube Data API](#)¹¹ allows you to access some metadata from your original file that is not present in copies downloaded from YouTube, which are transcoded.

CHECK YOUR TRANSFER

Transfers can be interrupted, so check your files to make sure they have transferred completely and intact. A simple way to check is to see that the file sizes and number of files match, and to play a sampling of the videos. If **hash values** are available for the files, verify against the hashes. See the section on **“Keeping Files Intact (and Proving It)”** for more on how to do this.

CHOOSING A SYSTEM/SERVICE FOR SHARING FILES

Whether you own and control your own remote server, or use a free online file sharing service to transfer your videos to others, there are a few key factors to keep in mind:

PERMANENCE

Since you may need to download the file at some point after you have uploaded it, the system should not remove or delete your videos without your authorization, or at least without adequate advance notice.

DATA INTEGRITY

The system should enable you to download an exact copy of what you uploaded, without alteration, data loss, or corruption.

SECURITY

The system should not be vulnerable to unauthorized access. In cases where you have restricted information, choose a system that allows you to **encrypt** or limit access to selected files.

¹¹ <https://developers.google.com/youtube/v3/>

CUSTODY

The system should monitor and log activities that affect the video (e.g. who uploaded and when, who accessed and when, who edited and when, etc).

DOCUMENTATION

If you have accompanying documentation, like consent forms or shotlists, choose a system that allows you to keep this documentation associated with the video.

ACCESSIBILITY

The system should enable you to access and download your videos in the manner and at the frequency you need.

EFFICIENCY

The system's method for uploading and downloading needs to suit your time and resources.

COST

You must be able to afford the system's cost to upload and download videos in the volume and frequency that you need.

COMPARISON OF POPULAR SYSTEMS/SERVICES

File sharing services all handle uploaded files differently, potentially affecting their authenticity, integrity, and usability. See the WITNESS tipsheet on [“Transferring Human Rights Video Online”](http://library.witness.org/product/transferring-human-rights-video-online/)¹² for a comparison of a few popular commercial services. Be aware that technologies and terms of use change frequently, so check for the most current information before making a decision.

TRANSFER: KEEPING FILES INTACT (AND PROVING IT)

It is important to make sure your files stay intact and unaltered when you transfer. It can also be important to **show** that your files are intact and unaltered, especially if you are using video for **evidence**.

Hashes, also known as checksums, are a way to check if your files have transferred intact. Hashes are also valuable **metadata** for evidentiary video, because they can be used to show whether your files are tampered with over time. It is therefore a good idea to capture hashes as early as possible in the video lifecycle, such as when you first **offload** videos from your camera.

A hash is an alphanumeric string of characters that is created by running a **hash function** algorithm (such as MD5 or SHA-1) on a file. The resulting hash value will be the same every time you run the algorithm on the file, so long as the file is unchanged. If the file is altered in any way, the resulting hash value will be different.

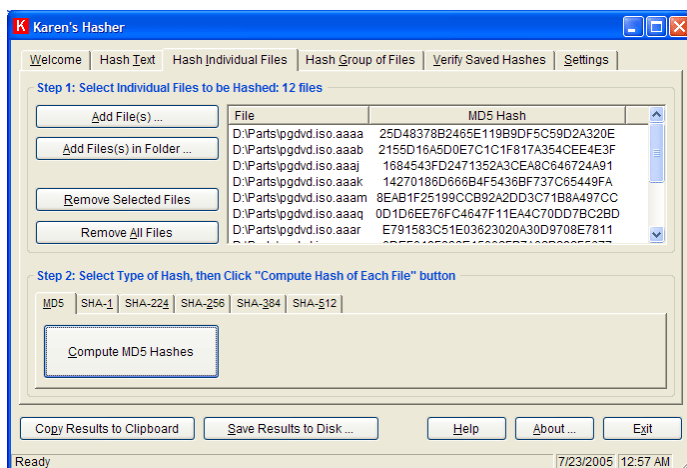


Example: “Myfile.doc.” The MD5 hash for myfile.doc = 887b7bc46f18a8df7457727e4ec3a253. The SHA1 hash for myfile.doc = 281dcb8aed030fc28c87b572ec0294ce17392af

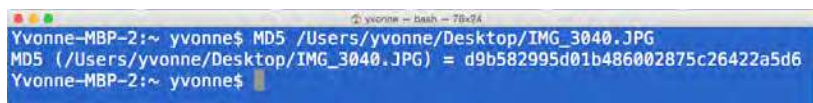
¹² <http://library.witness.org/product/transferring-human-rights-video-online/>

Run a hash algorithm on a file as soon as you acquire it, and again whenever you want to check that it is intact. You may want to check a file, for example, after you have transferred it from one location to another, if your file has been stored for a long time, or if you want to know whether someone has altered it.

There are many free and commercially available software applications you can use to compute hashes (see “Try This” below). In the near future, some cameras will allow you to compute and embed hashes in the video file at the point of creation.



Karen's Hasher is a free Windows application for computing hashes.



There is a built-in MD5 tool for Macs. To use this MD5 tool, open a Terminal window, type “md5,” followed by a space, and then the file (with filepath) you want to hash. Type “man md5” for the full MD5 tool manual.

Try This BASIC

Karen's Hasher¹³ is a Windows **GUI** tool for computing and verifying hashes.

Try This ADVANCED

MD5¹⁴ is a **command-line** tool for computing MD5 checksums that comes pre-installed on

Try This ADVANCED

Microsoft File Checksum Integrity Verifier¹⁵ is a Windows command-line tool for computing MD5 and SHA1 hashes.

Try This ADVANCED

md5deep¹⁶ and hashdeep are command-line tools for computing and comparing multiple checksums for entire directories of files.

Try This ADVANCED

shasum¹⁷ is a command-line tool for computing and checking SHA-1 checksums that is part of the GNU Core Utilities.

¹³ <http://www.karenware.com/powertools/pthasher.asp>

¹⁴ <http://www.fourmilab.ch/md5/>

¹⁵ <http://www.microsoft.com/en-us/download/details.aspx?id=11533>

¹⁶ <http://md5deep.sourceforge.net/#md5>

¹⁷ <http://www.gnu.org/software/coreutils/>

TRANSFER: PHYSICAL TRANSPORT

Video files can be physically transported on portable storage devices, such as SD cards or external hard drives. Storage devices, especially portable storage devices, are unreliable and particularly vulnerable in transport. You should always make at least one other copy of video and documentation that is going to be physically transported on another device.

SD CARDS



SD cards are particularly fragile and easily damaged. Only take an SD card out of a camera when you are in a clean environment. If transporting an SD card, always carry in a protective case.

PORTABLE HARD DRIVES / FLASH DRIVES



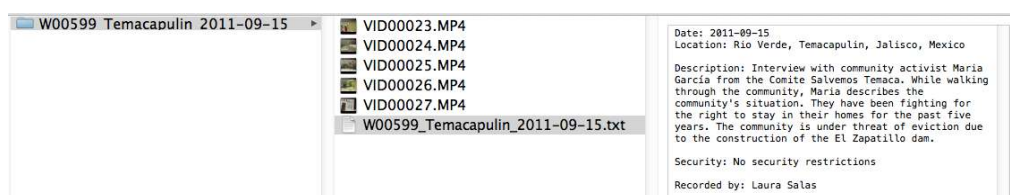
Hard drives and USB flash drives are formatted according to a particular file system, such as NTFS, HFS Plus, or FAT32. There are a few constraints to be aware of when using these devices to transfer video files between people in your network, especially if you have a mixed environment (i.e. Windows and Mac).

- NTFS is a Windows file system, and NTFS-formatted drives are normally read-only on Macs. If you want to be able to write to an NTFS drive using a Mac, you need extra software/drivers (NTFS-3G is a free one, but we have not tested it). Some hard drives (e.g. SeaGate GoFlex) include the software.
- HFS and HFS Plus are Mac OS file systems, and HFS-formatted drives cannot normally be read or written to on Windows computers. There are some commercial softwares available that allow you to read a HFS-formatted drive on Windows, but none that allow you to write.

- FAT32 is an older Windows file system that is used on most USB flash drives. FAT-formatted drives have the advantage of being readable and writable by both Macs and Windows computers. However, the maximum file size on a FAT-formatted drive is 4 GB, which may be too small for some video files.
- You can reformat a drive, but it will erase all the data on the disk.

TRANSFER: TRANSFERRING VIDEOS AND METADATA TOGETHER

Whether you are physically transporting video files on a hard drive or **uploading** to a hosted service, it is important to keep your video, **metadata** and related documents together in transit. One way to do this is to make **information packages**. “Information package” is a term borrowed from the archiving world that simply refers to a container, such as a folder, that holds an object -- your video file -- and information about the object -- your metadata and/or related documentation.



A simple information package, ready to be compressed into a .ZIP file for transfer.

An information package can be as simple as a folder containing a video file and a text file, although information packages can also include multiple video files and multiple documents. To send an information package, you can simply compress the folder into a .ZIP file so it can be moved in one piece.

See the “Organize” section in the workflow for more on information packages.

TRANSFER: TAKEAWAYS

- When **offloading** videos from your camera to your computer, make sure you transfer the files completely and without alteration.
- Always make sure to include your **metadata** and documentation with your video—or make sure they can be matched together after transfer.
- If using the Internet to transfer files, choose a file sharing service that meets your needs for permanence, data **integrity**, security, **chain of custody**, documentation, accessibility, efficiency, and cost.
- Use **hashes** to check that your files have transferred intact, and to show that your files have not been altered over time.
- If physically transporting drives, make sure to have another copy and be aware of cross-platform constraints.
- Organize your videos in “**information packages**,” or folders with your video and metadata, for transfer.

KEY CONCEPTS IN THIS SECTION

Chain of Custody:

Transfers are key events in the chain of custody.

[Read More...](#)

Information Package

Use an information package to transfer videos with their metadata and documentation in one piece.

[Read More...](#)

Metadata:

Capturing metadata at this stage - before it is lost or forgotten - is critical for the identification, authentication, and use of the video.

[Read More...](#)

Original File:

The ideal result of a transfer is to receive the original file.

[Read More...](#)

Authenticity:

A proper transfer maintains the authenticity of the video file.

[Read More...](#)

Fixity:

Files should remain unchanged even over multiple transfers over time.

[Read More...](#)

Integrity:

Transferred files should be complete, intact, and unaltered.

[Read More...](#)

THE WORKFLOW: ACQUIRE

ACQUIRE: INTRODUCTION

Acquisition refers to the process of receiving video and **metadata** from a source and adding it to your collection. Your aim at this stage is to acquire your materials in a **complete** and intact form. Actions you take at this stage are critical to the later usability and preservation of your video.

A SCENARIO INUNDATED WITH VIDEOS

The Elections Monitoring Center wants to collect reliable videos that document the aftermath of recent elections in its country in order to report to the international community, and to retain for the historical record. Fortunately, the days following the election were widely documented on video by news outlets, ordinary citizens, and the Center's own staff. There are so many videos, in fact, that the Center is overwhelmed by the quantity.

Rather than try to collect every single video about the election, the Center decides to prioritize videos that best meet its purposes. It decides to acquire only videos whose source they can confirm; that they have the rights to re-use; and that emerged from electoral districts in which news media were not present.

Some of the most important video documentation was shot by ordinary citizens. In order to ensure the **authenticity** and reliability of these videos, the Center asks citizens to submit their **original files** if they can, and to fill out a metadata form with their names, district, and other information.

CAUTION!

CHECK FOR VIRUSES

Malware like viruses and Trojans can spread through the Internet or on portable devices. Protect yourself from inadvertently acquiring malware by using virus detection software, and only downloading or opening attachments from known and trusted sources.

Try This BASIC

There are many commercially available virus scanners. Some free virus scanners include ClamXAV¹⁸, Immunet¹⁹, and ClamWin²⁰.

¹⁸ <http://www.clamxav.com/index.php>

¹⁹ <http://www.immunet.com/main/index.html>

²⁰ <http://www.clamwin.com>

ClamAV²¹ is an open source anti-virus engine for detecting Trojans, malware, viruses, and other malicious threats.

PROTECT SENSITIVE INFORMATION

Find out from your sources if there is any sensitive information in your video and metadata that needs to be kept confidential (e.g. names, locations). You should acquire and retain this information but restrict access and store securely as needed.

ACQUIRE: DECIDING WHAT TO KEEP

You may not need to keep everything you create or receive. Archives use a basic tool called a **selection** policy to identify what to save or acquire; it is a simple exercise that can make a big difference.

With a selection policy or statement, you can:

- Focus your limited resources on what is most important.
- Provide clarity for your acquisitions team in their day-to-day work.
- Provide guidance for discarding videos you do not need to keep.
- Give potential users of your collection a sense of whether you might have what they are looking for.
- Avoid wasted effort or resources in collecting video that you cannot use, or that is being archived elsewhere.

In the long run, a selection policy helps ensure that the content you preserve has significance and enduring value.

WITNESS Media Archive Collection Policy

The Media Archive collects video related to human rights for the purposes of preservation and access, and in particular, original and master recordings created by or about WITNESS partner organizations and WITNESS. The scope is global, with no geographic limitations. Human rights are broadly conceived to include civil, political, economic, cultural and social rights.

WITNESS and WITNESS Partner footage

Original, raw video created by WITNESS and WITNESS partners during the course of a partnership or collaboration.

Edited productions

Documentaries created by WITNESS, and by or in collaboration with WITNESS partners.

Third-party video

News programs, documentaries, and other recordings depicting WITNESS, about WITNESS or its partners, or used in WITNESS video productions.

Related materials

Documentation related to the video collection, such as logs, scripts, production notes, background information, photographs, consents and licenses forms, etc.

A sample collection selection policy.

IDENTIFY YOUR COLLECTING GOALS

To develop a selection policy, first identify the goals and priorities of your collection:

- What is the overall goal or purpose of your collection?

²¹ <http://www.clamav.net/index.html>

- Who are the target audiences or users of your collection?
- What is the content scope of your collection?
- What types of materials or formats do you collect?
- What is not included in your collection?

OTHER SELECTION CRITERIA

Other potentially important criteria for selecting videos are:

SUFFICIENT METADATA

Is there enough contextual information available so that the video can be used and understood?

UNIQUENESS

Is the video at risk of being lost? Do you have the only copy, or is the video already being properly archived elsewhere that you can access if needed?

RIGHTS

Do you have the legal right to use or distribute the video?

BEST FIT

Do you have the capacity to maintain the video over time, or is there someone who is better suited to do so?

CONDITION

Is the video intact and playable? Is this the better quality copy of the video available?

ACQUIRE: ACQUIRING RAW VIDEO AND METADATA

ALWAYS ACQUIRE ORIGINAL FILES IF YOU CAN

Whether you are acquiring video directly from a camera, mobile phone, hard drive, or **downloading** from the web, always collect the **original file** (i.e. an exact copy) when possible. Besides being the **authentic** object, the original file contains important metadata about the video source, such as the date recorded or geographic location. This information is often lost if the file is altered or **transcoded**.

Metadata from Original Raw Video File		Metadata from MP4 Copy Downloaded from YouTube	
Format	Original Video/MOV_2176.MOV	Derivative Videos/MG_2176_2x360p8_8.m4	MPEG-4
Format profile	QuickTime	Format profile	Base Media / Version 2
Codec ID	Q	Codec ID	mp42
File size	965 KiB	File size	520 KiB
Duration	1:11.872min	Duration	1:11.900min
Overall bit rate	866 Kbps	Overall bit rate mode	Variable
Recorded date	2012-10-26T17:24:33-0400	Overall bit rate	318 Kbps
Encoded date	UTC 2012-10-26 21:25:30	Encoded date	UTC 2012-10-29 14:18:38
Tagged date	UTC 2012-10-26 21:25:35	Tagged date	UTC 2012-10-29 14:18:38
Writing application	iOS	gslv	0
Writing library	Apple QuickTime	gslv	11200
Make	Apple	gslv	10A700601MM135160828763171
Model	+40.68511-073.9742+040.7751	gslv	0
com.apple.quicktime.make	Apple	gslv	71-----sm-p545u7x6.yousize.com
com.apple.quicktime.creationdate	2012-10-26T17:24:33-0400		
com.apple.quicktime.location.ISO6709	+40.68511-073.9742+040.7751		
com.apple.quicktime.software	6.0		
com.apple.quicktime.model	iPhone4,1		

When video is altered or transcoded, metadata from the original file may be lost.

In situations where the original file is not available (e.g. when downloading from YouTube), your only option may be to download a transcoded **derivative**. If you have a choice between non-original files, select one that was derived from the original (i.e. as opposed to a derivative of a derivative). Secondly, select the highest quality copy that is available in a widely used and current **format**.

Try This BASIC

WAIL²² (Web Archiving Integration Layer) is a one-click tool for acquiring web pages, including ones with video.

**Try This
ADVANCED**

YouTube-dl²³ is a **command-line** tool to downloading videos from video sharing sites.

GET THE METADATA

Along with the video, make sure you acquire any metadata or documentation that comes with it. Metadata can be **embedded** in the video file, delivered with the video files in another format (e.g. a text document), sent or displayed separately from the video file (e.g. in an email, on a YouTube page). Metadata can also be communicated to you orally or in person. Record this information in some form, such as a text document, spreadsheet, or database.



Metadata can come in various forms.

Try This BASIC

TubeKit²⁴ is a YouTube crawler that allows you to extract YouTube video data (author, keywords, genre, number of views, ratings, comments, etc.), collect text comments for YouTube videos, and extract a YouTube users' profile data.

**Try This
ADVANCED**

YouTube Data API²⁵ allows you to obtain detailed metadata about a video, including metadata from the original video file (which itself is not available).

Try This BASIC

MediaInfo²⁶ (\$0.99, GUI version) displays metadata embedded in video and audio files.

Try This
ADVANCED

The free version of MediaInfo²⁷ displays metadata embedded in video and audio files in the command-line.

²² <http://matkelly.com/wail/>

²⁴ <http://www.tubekit.org>

²⁶ <http://mediaarea.net/en/MediaInfo>

²³ <http://rg3.github.io/youtube-dl/>

²⁵ https://developers.google.com/youtube/getting_started#data_api

²⁷ <http://mediaarea.net/en/MediaInfo>

Remember that not all metadata is correct, complete, or reliable. Even metadata embedded in a file can be incorrect (e.g. if the camera is set to the wrong date and time). Try to fill in missing information by contacting the creator or source, or through research. When acquiring from untrusted or unknown sources, take steps to verify information, such as by examining the sources or corroborating the videos with other known information. You can still acquire unverified videos, but take note what information is missing or may be unreliable.

00033.MTS	Feb 6, 2040 1:28 AM	Apr 14, 2011 3:03 PM
00034.MTS	Oct 5, 1974 11:21 PM	Apr 14, 2011 3:03 PM
00035.MTS	Apr 24, 1976 9:02 PM	Apr 14, 2011 3:04 PM
00036.MTS	May 17, 1979 1:25 PM	Apr 14, 2011 3:04 PM
00037.MTS	Oct 30, 1979 3:05 PM	Apr 14, 2011 5:51 PM
00038.MTS	Oct 7, 1980 5:26 PM	Apr 14, 2011 5:51 PM
00039.MTS	Oct 10, 1982 6:48 PM	Apr 14, 2011 5:51 PM
00040.MTS	Jan 18, 1983 1:08 AM	Apr 14, 2011 5:51 PM
00041.MTS	Nov 24, 1983 2:29 PM	Apr 14, 2011 5:51 PM
00042.MTS	May 14, 1984 4:09 AM	Apr 14, 2011 5:51 PM
00043.MTS	Jun 6, 1986 2:11 AM	Apr 14, 2011 5:51 PM
00044.MTS	Jul 17, 1987 8:12 AM	Apr 14, 2011 5:51 PM
00045.MTS	Nov 13, 1988 11:54 PM	Apr 14, 2011 5:52 PM
00046.MTS	Jul 15, 1992 6:17 PM	Apr 14, 2011 5:52 PM
00047.MTS	Feb 6, 1997 6:01 AM	Apr 14, 2011 5:52 PM

Metadata can be incorrect and unreliable.

CHECK YOUR FILES

After you have copied, moved, or downloaded the video and any metadata or documentation, check to make sure you have acquired the files completely and intact:

SIMPLE METHOD

Attempt to play back or open the files. If collecting original files, verify that the number of files and file sizes match the source.

MORE FOOLPROOF METHOD

If collecting original files, check hashes (i.e. checksums) of acquired files against **hashes** computed on the source. See “**Keeping Files Intact (and Proving It)**” for more information on how to do this.

Try This BASIC

Karen’s Hasher²⁸ is a Windows GUI tool for computing and verifying hashes.

Try This ADVANCED

MD5²⁹ is a free command-line utility for computing MD5 hashes (aka checksums).

Try This ADVANCED

md5deep³⁰ and hashdeep are a free command-line tools for computing and comparing multiple checksums for entire directories of files.

Try This ADVANCED

shasum³¹ is a free command-line utility for computing and checking SHA-1 checksums that is part of the GNU Core Utilities.

VIDEO AS EVIDENCE TIP

Compute hashes of your videos when you acquire them, and check against hashes from the source if available. As part of **chain of custody**, keep a record of the hashes to demonstrate that your files have not been tampered with or altered over time. Provide the hash value when you share the video with others, so that they can verify that they received the video intact.

²⁸ <http://www.karenware.com/powertools/pthasher.asp>

²⁹ <http://www.fourmilab.ch/md5/>

³⁰ <http://md5deep.sourceforge.net/#md5>

³¹ <http://www.gnu.org/software/coreutils/>

DO NOT RE-NAME RAW VIDEOS FILES

There is no need to rename the acquired video files, unless the filename uses “illegal” characters (e.g. ? [] / \ = + < > ; , . “ , | *), is excessively long, or contains spaces. If your video file still has the original filename from the camera, you should not rename the file. The original filename is important for retaining the **original order** or sequence of raw video files, and is sometimes even essential for the full functionality of the video (e.g. AVCHD format). See the “**Organize**” section in the workflow for more information on naming files.

VIDEO AS EVIDENCE TIP

Maintaining an unbroken chain of custody is especially important for evidentiary materials.

MAINTAIN CHAIN OF CUSTODY

To maintain an unbroken **chain of custody**, you need to document your acquisition. You can create a registry or log of acquisitions to note the time and date that videos were added to your collection. This step is often integrated and automated in **cataloging** and **media management** systems. You can also save documents such as submission forms, emails, download/transfer logs that indicate when you gained custody of a video.

E008761	04/13/2011 4:59:10 PM	AVC	mp4	Master	Yvonne Ng
E008762	04/13/2011 5:00:12 PM	XviD	AVI	Camera Original	Yvonne Ng
E008763	04/13/2011 5:07:12 PM	XviD	AVI	Camera Original	Yvonne Ng
E008764	04/13/2011 5:31:16 PM	WMV3	mov	Master	Yvonne Ng
E008765	04/13/2011 5:37:11 PM	WMV3	mov	Master	Yvonne Ng
E008766	04/14/2011 10:24:41 AM	DV	txt,	Master	Yvonne Ng
E008767	04/14/2011 10:27:24 AM	DV	txt,	Master	Yvonne Ng
E008768	04/14/2011 10:30:39 AM	DV	mov	Master	Yvonne Ng
E008769	04/14/2011 10:31:15 AM	DV	mov	Master	Yvonne Ng
E008770	04/14/2011 10:31:47 AM	DV	mov	Master	Yvonne Ng
E008771	04/14/2011 10:34:35 AM	DV	mov	Master	Yvonne Ng
E008772	04/14/2011 10:41:33 AM	DV	mov	Master	Yvonne Ng
E008773	04/14/2011 11:12:47 AM	DV	mov	Master	Yvonne Ng
E008774	04/14/2011 11:16:12 AM	DV	mov,	Master	Yvonne Ng
E008775	04/18/2011 11:36:06 AM	AVC	mp4	Use/Web Upload	Yvonne Ng

A sample acquisition log from a media management system.

ACQUIRE: ACQUIRING EDITED VIDEO AND ELEMENTS

Edited videos are videos that are created using other videos as sources. They can range from complex productions to the simple addition of logos or title cards to raw video footage.



Acquiring edited videos involves a slightly different approach from acquiring raw video footage. First of all, the “original” file is not relevant since the video is **outputted** from an editing system and there is no direct connection to a recorded event. Second, the creation of edited videos can generate a variety of other files that may need to be acquired depending on the intended future use of the edited video.

MAKE SURE YOU HAVE A MASTER

Always acquire a “**master**” copy -- the highest quality copy of an edited video -- when possible. If you are outputting the video from editing software, export a high-quality video as your master, even if you do not have an immediate use for it. You can export additional copies in other formats as needed.

Remember that once a video is outputted, there is no way to improve its visual or audio quality. Having a high-quality master is therefore especially important if you will not have access to the raw footage or the editing project file later on.

KEEP (SOME) PRODUCTION ELEMENTS

Editing a video usually involves creating a variety of additional files, such as project files, graphics, render files, and transcoded source files. It can be difficult to determine what to keep.

In general, it is a good idea to collect the project files (e.g. the .fcp file) and **edit decision lists (EDL)**, in case you ever need to re-edit the video. You may need to re-edit, for example, if you find an error, if the situation changes and you need to update information, or if you want to make a new version of the video. For the same reason, it is a good idea to collect graphics or any other elements that were created for the video.

It is not necessary to acquire temporary files (i.e. render files) from an editing project, as these can be re-rendered if needed.

Editing software sometimes requires videomakers to **transcode** source video files to a format that is easier for the software to work with. At the end of the project, you may wish to acquire these transcoded copies so that you can easily re-edit the project in the future. However, transcoded copies require extra storage space -- they are often significantly larger than the original source files. To conserve disk space, you may delete the transcoded copies and just keep the original source files. As long as you have not changed any filenames, it is possible to re-create the transcoded copies from the original source files and re-connect them to your editing project.

VIDEO AS EVIDENCE TIP

If you have an edited video and the unedited original source files used to create it, do not delete the original source files when you are finished with your edit! Unedited original files are more valuable as evidence than edited videos.

ACQUIRE: TAKEAWAYS

- Decide what you will—and will not—collect and save; create a **selection** policy based on your goals and needs.
- **Acquire unaltered original files whenever possible.**
- **Acquire all available metadata and related documentation about your videos.**
- Check your acquired files to make sure you have copied or **downloaded** them completely and correctly.
- Do not rename video files if they have their original camera-given filenames.
- Maintain the **chain of custody** by documenting the source, time, date, and location of your acquisition.
- For edited videos, acquire a high-quality **master** whenever possible.
- For edited videos, acquire production elements like project files and graphics.

KEY CONCEPTS IN THIS SECTION

Selection Policy:

A selection policy provides clarity on what you will acquire and what you will not.

[Read More...](#)

Integrity:

Ensure that no loss, tampering, or file corruption occurs during the process of acquisition.

[Read More...](#)

Authenticity:

Maintain the authenticity of a video when you acquire it by collecting the intact original file(s) and the metadata that comes with it.

[Read More...](#)

Chain of Custody:

Your acquisition forms a part of a video's chain of custody. Document your acquisition, so that an unbroken chain can be traced all the way back to the source.

[Read More...](#)

Completeness:

Be sure that you acquire all of the files needed to create a complete record, as defined by the purpose or requirements of your collection.

[Read More...](#)

Original Order:

Always acquire an exact copy of the file created by the camera with no alterations to content or technical specifications, unless doing so is impossible.

[Read More...](#)

Original File:

The ideal result of a transfer is to receive the original file.

[Read More...](#)

Metadata:

Metadata may be embedded within a video file, or it may be a separate document. It is as important to acquire a video's metadata as it is to acquire the video itself.

[Read More...](#)

THE WORKFLOW: ORGANIZE

ORGANIZE: INTRODUCTION

Organizing your collection involves arranging your files into a coherent directory structure, and clearly naming those directories. Good organization is needed to retain the **original order** of your video files, and ensures that videos do not get lost or accidentally overwritten. It is also easier to find videos in a well-organized collection.

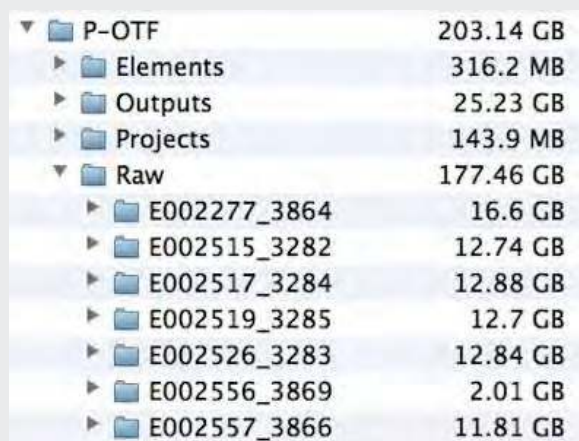
A SCENARIO

WHEN EVERYTHING IS IN SOMEONE'S HEAD

The Children's Rights Center regularly produces short edited videos about children's rights issues. For every video that the Center produces, it ends up with a large amount of raw footage and production elements like graphics and music that can be re-used in other productions. The material is not organized, but Mohammad, the video editor who works with the footage, remembers where everything is stored and can find clips when he needs them.

One day, Mohammad is offered a job at another organization and leaves the Children's Rights Center. The Center's new video editor, Raja, cannot make sense of Mohammad's files and cannot locate the footage she needs.

To prevent this from happening again, Raja starts to organize new videos by production in clearly marked directories. In each production, she separates the raw footage, final outputs, and production elements. Within these subdirectories, she places files into clearly named folders with **unique identifiers**.



▼ P-OTF	203.14 GB
▶ Elements	316.2 MB
▶ Outputs	25.23 GB
▶ Projects	143.9 MB
▼ Raw	177.46 GB
▶ E002277_3864	16.6 GB
▶ E002515_3282	12.74 GB
▶ E002517_3284	12.88 GB
▶ E002519_3285	12.7 GB
▶ E002526_3283	12.84 GB
▶ E002556_3869	2.01 GB
▶ E002557_3866	11.81 GB

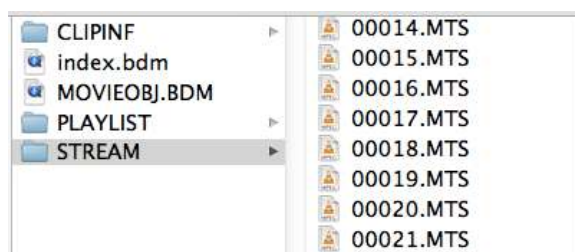
Video files and metadata are stored in folders labeled with unique identifiers. Folders are organized into directories by production project, and content type.

ORGANIZE: FILENAMES

DO NOT RENAME CAMERA FILENAMES

A filename generated by a camera provides valuable information about a video. For example, in a group of video files, you can easily tell that DSC_991.AVI was recorded after DSC_990.AVI, but before DSC_992.AVI, and that it was not recorded on the same camera as VID0005.AVI.

Retaining the filename is part of maintaining the **original order**, which is important for evidence and contextualization. In addition, some complex video **formats** rely on the original filename to function properly.



Raw camera footage in its original order.

WHAT IF I HAVE DUPLICATE FILENAMES?

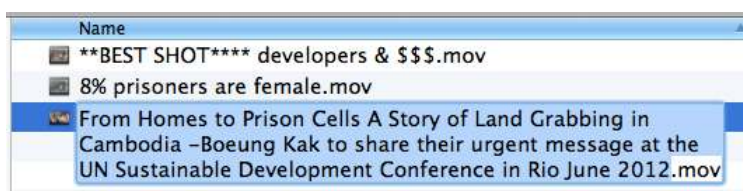
Duplicate filenames can sometimes occur when you acquire raw footage files from different people who use the same camera brand. Rather than renaming the files, organize footage from each source person into a separate folder (see **"Folders and Directories"** for more on this).

If you must rename your camera files, retain the original filename as part of the new filename.

WHEN TO RENAME FILES

Bad filenames will impede activities like transferring files between systems and **backup**. You should always rename the file if:

- The file contains special characters like @#% &* "<>?/\~| that are reserved for filesystem operations.
- The filename is very long (maximum number of characters depends on the rest of the file path).
- The filename contains spaces (bad for certain programs and for web).



Examples of bad filenames.

HOW TO NAME RAW FOOTAGE FILES

If you need to rename raw footage files:

REFER TO THE SOURCE OF THE VIDEO IN THE NEW FILENAME

Include the camera-assigned filename if possible. You can also include the date recorded, location, or videographer name. You can also include any **unique identifier** provided by the source, such as a YouTube ID if your source is YouTube.

USE A TEMPLATE

Name your files consistently by using a filenames convention or template. For example, a template like “YouTubeID_DateRecorded_Location” means that you will always name raw footage files with those elements in that order, separated by underscores.

Name
iYUXsHaDzY8_20131110_PhnomPenh.mp4
UALphxHdFaM_20131031_BoaVista.mp4
XcfmcntdYYE_20141030_CapeTown.mp4
zpFm7a_Cz6o_20131024_Zaragosa.mp4

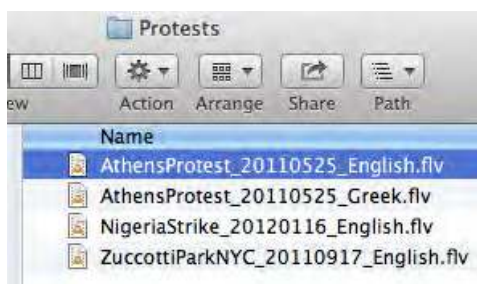
If re-naming, rename files consistently according to a template.

AVOID USING “ILLEGAL” CHARACTERS

Characters like @#\$% &*”<>?/\-| are reserved for filesystem operations. Also avoid overly long file names, and spaces in your filenames.

HOW TO NAME OUTPUTTED EDITED VIDEO FILES

Videos that you edit and output from a video editing system need to be given filenames. Give each file a unique name that follows a consistent filenames template. The components of the filename should help you easily distinguish one output from another, e.g. “ShortTitle_DateOutput_Language” or “ID_ShortTitle_VersionNumber.”



Name edited video files according to a template.

If you are acquiring an edited video from somewhere else, it is generally not necessary to rename the file. While the filename given to an edited file is less significant in terms of original order than a filename assigned to a raw video by a camera, it can still provide evidence of where the edited video came from (e.g. if the filename includes a unique identifier from the source). The only instances when you should rename an acquired edited video file is if the filename contains special characters that can confuse software or operating systems (e.g. ? [] \ = + < > ; , ' *), the filename is overly long, or if it contains spaces.

ORGANIZE: USING UNIQUE IDENTIFIERS

WHAT IS A UNIQUE IDENTIFIER?

A **unique identifier** is a number or code that can unambiguously distinguish one object from another in a given system, and group things associated with an object together. We frequently encounter unique identifiers in our everyday lives, such as credit card numbers, phone numbers, barcodes, and book ISBNs. A credit card number, for instance, distinguishes your purchases from someone else's, and allows all of your purchases to be grouped together on one bill.



A product barcode is an example of a unique identifier.

You can use unique identifiers to organize your videos. Imagine that you have 10 video files acquired from various sources, whose camera-assigned filenames have all been changed. When you review the videos, you find that 9 are unique, and one is a copy. You can create 9 unique identifiers to distinguish the 9 videos from one another. You can also give the one non-unique copy the same unique identifier as its original to associate them together.

Files as Acquired	Files with Unique Identifiers Added																						
<table><tr><th>Name</th></tr><tr><td> ASEANSummit.mov</td></tr><tr><td> BKL.mp4</td></tr><tr><td> ConferenceHousing.mov</td></tr><tr><td> Detainees.mov</td></tr><tr><td> EvicteesMarch.AVI</td></tr><tr><td> Free15.mp4</td></tr><tr><td> HousingConf.mov</td></tr><tr><td> LandGrab.mov</td></tr><tr><td> UNSecretary.mov</td></tr><tr><td> ViolentCrackdown.flv</td></tr></table>	Name	 ASEANSummit.mov	 BKL.mp4	 ConferenceHousing.mov	 Detainees.mov	 EvicteesMarch.AVI	 Free15.mp4	 HousingConf.mov	 LandGrab.mov	 UNSecretary.mov	 ViolentCrackdown.flv	<table><tr><th>Name</th></tr><tr><td> A0001_Free15.mp4</td></tr><tr><td> A0002_BKL.mp4</td></tr><tr><td> A0003_ASEANSummit.mov</td></tr><tr><td> A0004_LandGrab.mov</td></tr><tr><td> A0005_Detainees.mov</td></tr><tr><td> A0006_ViolentCrackdown.flv</td></tr><tr><td> A0007_UNSecretary.mov</td></tr><tr><td> A0008_EvicteesMarch.AVI</td></tr><tr><td> A0009_HousingConf_LowResCopy.mov</td></tr><tr><td> A0009_HousingConf.mov</td></tr></table>	Name	 A0001_Free15.mp4	 A0002_BKL.mp4	 A0003_ASEANSummit.mov	 A0004_LandGrab.mov	 A0005_Detainees.mov	 A0006_ViolentCrackdown.flv	 A0007_UNSecretary.mov	 A0008_EvicteesMarch.AVI	 A0009_HousingConf_LowResCopy.mov	 A0009_HousingConf.mov
Name																							
 ASEANSummit.mov																							
 BKL.mp4																							
 ConferenceHousing.mov																							
 Detainees.mov																							
 EvicteesMarch.AVI																							
 Free15.mp4																							
 HousingConf.mov																							
 LandGrab.mov																							
 UNSecretary.mov																							
 ViolentCrackdown.flv																							
Name																							
 A0001_Free15.mp4																							
 A0002_BKL.mp4																							
 A0003_ASEANSummit.mov																							
 A0004_LandGrab.mov																							
 A0005_Detainees.mov																							
 A0006_ViolentCrackdown.flv																							
 A0007_UNSecretary.mov																							
 A0008_EvicteesMarch.AVI																							
 A0009_HousingConf_LowResCopy.mov																							
 A0009_HousingConf.mov																							

Use unique identifiers to distinguish and associate files.

CREATING UNIQUE IDENTIFIERS

To create your own sets of unique identifiers, decide what kind of objects you want to identify, such as projects, individual files, or folders containing groupings of files.

For each kind of object you want to identify, define a template or strategy for assigning identifiers for that kind of object. For instance, you may choose to identify folders using numbers that count sequentially starting with the number “00001,” or you may want to identify projects using a five-letter code that starts with “P-.” The date recorded can be a good basis for unique identifiers for raw footage, since it changes every 24 hours, e.g. “20130623-001.” You can also use identifiers created by other systems (e.g. camera filenames, YouTube IDs).

Keep track of your unique identifiers in a registry recorded using a spreadsheet or database application. You can also use a spreadsheet or database application to automatically generate unique identifiers for you.

id	titleVariant:title	dates:date	main_credits
6209	Maurice Makoloo - ELAW Interview Series.	2009-03	WITNESS
6210	Rugemeleza Nahala - ELAW Interview Series.	2009-05-14	WITNESS
6211	Children of War. [NBC Dateline episode]	2005-08-21	NBC
6212	Yeral Sánchez - ELAW Interview Series.	2009-03	WITNESS
6213	Thevinai Amarthalingam - ELAW Interview Series.	2009-05-14	WITNESS
6214	[Unedited raw footage for vlogs related to Hear Us, Stand With Us at SADC]	2009-08/2009-09	WITNESS
6215	[Kelly Matheson and Priscila Neri Hub vlogs from Public Interest Environmental]	2009-02-05	WITNESS
6216	[Hub videos from courthouse rally for Wiwa v. Shell, May 27, 2009]	2009-05-27	WITNESS
6217	[Courthouse rally for Wiwa v. Shell trial, May 27, 2009]	2009-05-27	WITNESS
6218	Michael Goldhaber on the Outcome of the Shell Trial Settlement. [Hub vlog]	2009-06-09	Michael Goldhaber /
6219	[Hub interviews with 2008 Silverdocs Documentary Film Festival WITNESS]	2008-07-17	WITNESS
6220	[Unedited interviews with 2008 Silverdocs Documentary Film Festival]	2008-06	WITNESS
6221	[Interview with Joe Berlinger, director of CRUDE]	2009-07-22	WITNESS
6222	[Post-campaign videos from 'What Image Opened Your Eyes to Human Rights']	2008-12-11	WITNESS
6223	[Edited responses by WITNESS staff for 'What Image Opened Your Eyes to	2008-12-05	WITNESS
6224	[External responses to "What Image Opened Your Eyes to Human Rights?"	2008-12	
6225	[Amnesty International Small Places Tour promotional videos with musicians]	2008-08-13	AI
6228	Asian NGOs Network on National Human Rights Institutions (ANNI) Training	2008-11-26/2008-11	WITNESS
6229	Dilemma: Caught Between the Tiger and the Crocodile.	2008	APNSW
6230	Asia Training and Studies Session for Human Rights Defenders in Bangkok.	2008-11-16/2008-12	WITNESS
6231	Human Rights and Video in China: A Conversation with Ai Xiaoming.	2008-09-18	WITNESS
6232	Interview with WITNESS Core Partner Chintan on Wastepickers' Rights.	2008-11-06	WITNESS/Chintan

Keep track of your unique identifiers.

WAYS TO USE UNIQUE IDENTIFIERS

You can organize your collection by using unique identifiers in your directory names and filenames. Say, for example, you output a **master** video file called “00001_MyVideo_Master.mov.” You can name a lower resolution copy made for web upload “00001_MyVideo_LowRes.mov.” Similarly, you can name the shot list “00001_ShotList.xls.” All three of these files can be organized in a folder named “00001_MyVideo.”



Unique identifiers in directory names and filenames.

If you have an inventory or **catalog**, you can include the unique identifier as a spreadsheet column or database field so that you can easily retrieve each video in your collection.

If you are sharing videos and documentation with others, you can refer to unique identifiers so that it is clear what you are talking about. You can also send and receive video and documentation separately and put them together later by putting the same unique identifier in their filenames.

ORGANIZE: FOLDERS AND DIRECTORIES

ORIGINAL ORDER

The key principle when organizing or grouping raw video footage into folders is to preserve its **original order**. In the context of video documentation, the original order is the order in which video files are recorded-- for example VID00001.avi, VID00002.avi, VID00003.avi. The original order of files has evidential significance; you can infer that VID00002.avi was shot after VID00001.avi, and nothing was filmed in between. Original order also provides context to the individual files -- for example, the events depicted in VID00003.avi somehow relate to the events in VID00002.avi and VID00004.avi.



Note that you may not always receive files in their original order, and that you may need to restore the original order when you organize your files.

FOLDERS AS INFORMATION PACKAGES

A simple way to organize your videos and documentation is to make **information packages**. “Information package” is a term borrowed from the archiving world that simply refers to a container, such as a folder, that holds the object being archived-- your video file-- and information about it that enables it to be archived-- your **metadata** and/or documentation.

An information package can be as simple as a folder containing a video file and a text file, although information packages can also include multiple video files and multiple documents.



A basic information package.

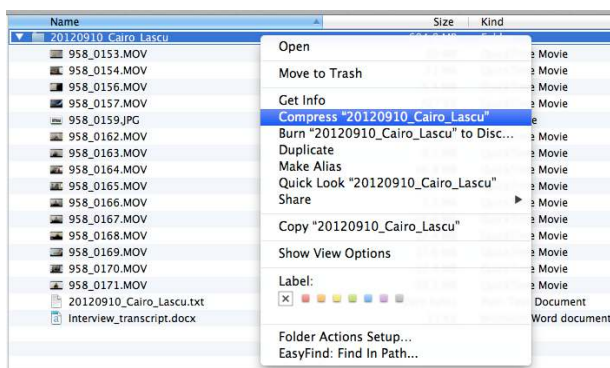
Information packages allow you to:

EASILY GROUP RELATED VIDEO FILES

Information packages allow you to easily group related video files, which helps maintain the original order and context. For example, if you record an event and end up with 15 video files, you can group them together in a single information package. You can then add a text file containing metadata that pertains to all 15 files to the package.

KEEP YOUR VIDEO AND METADATA/DOCUMENTATION TOGETHER

Using information packages prevents videos from becoming disassociated from the information about them over time and as you move the videos from place to place. For example, if you need to send videos to someone, you can compress the entire information package into a .ZIP file and transfer the video along with its metadata and documentation in one piece.



After organizing into information packages, compress into a .ZIP file content for easy transfer.

SEARCH AND BROWSE YOUR COLLECTION MORE EASILY

By using your Spotlight or Windows Search tool, you can find videos by searching within package folder names and text file contents. You can also organize your packages into directories to make them easier to browse (See “Organizing Packages into Directories” below).

HOW TO MAKE AN INFORMATION PACKAGE

- Maintain the original order of the videos by only including videos recorded by one source at one place at one time in a package.
- Do not mix video files from multiple sources or events in a single information package.
- Name your information package folders consistently. The purpose is to make your package easy to identify and find. For example, you can name your package folders according to a “PackageID_DateRecorded_Location_SourceName” template.
- Make sure your package names are unique from one another (creating **unique identifiers** for your packages can help with this).
- If you have multiple video files and multiple documents in a single package, you can create a simple subdirectory structure within the package to make it more organized, such as:

```
Package Base Directory/
    Videos/
    Documentation/
```

ORGANIZING PACKAGES INTO DIRECTORIES

As with all electronic files, organizing your digital videos involves putting them into directories in your file system. There is no one correct way to structure your directories, and the best way will depend on how you access your files.

Some tips:

USE A STRUCTURE THAT WORKS FOR YOU

If you primarily access your stored files using your file browser (e.g. Finder or File Explorer), create a hierarchical directory structure that reflects how you would browse for a video. For example, if you would browse first by date, then by location, then by videographer to find a video, create three levels of directories that align with these categories.



Group video files and related metadata or documentation together in an information package, and organize into directories.

VIDEO AS EVIDENCE TIP

If you are collecting video for evidence, make sure information packages retain the original order of the videos, and organize your videos in a way that is easily browsable by creator, date recorded, and location.

USE YOUR DIRECTORY STRUCTURE CONSISTENTLY AND DO NOT DEVIATE

If the third level in your directory structure files content by videographer, for example, then only put videographer names on this directory level. Always spell your folder names consistently!

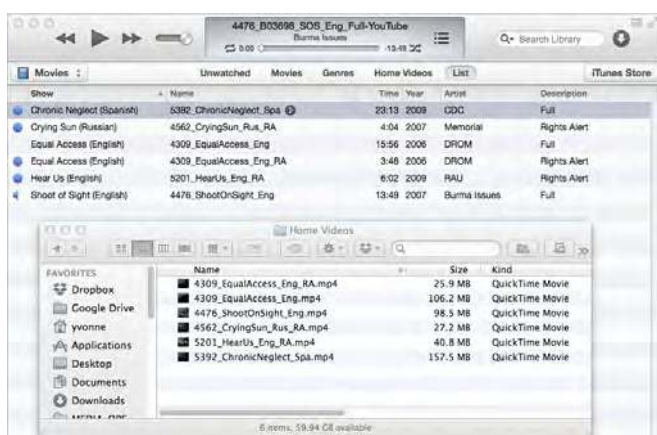
AVOID CREATING TOO MANY LEVELS OF NESTED SUBDIRECTORIES

Too many levels can make browsing cumbersome. It can also cause **interoperability** problems. Many Windows programs, for example, cannot handle file paths that exceed 260 characters.

UNDERSTAND THE DRAWBACKS FOR BROWSING AND SEARCHING

One drawback of relying on Finder or File Explorer to browse your collection is that the file system is hierarchical, i.e. browsing is done by continuously narrowing the scope of your search as you go down the directory tree. This can be problematic if you want to navigate your collection other than the way your directory structure is set up. It can also be problematic if you are trying to organize your videos according to multiple non-hierarchical attributes -- for example, if you want to organize your videos by multiple topics.

To make your collection browsable or sortable by multiple non-hierarchical attributes -- such as topics -- you will need to use a separate database or **media management** application. With it, you can assign multiple attributes, such as topics, names, and descriptions to a record that point to your video. You may be familiar, for example, with how the media management application iTunes allows you to organize your music files in various ways without actually moving the stored mp3s in your file system. See **“Tools for Media Management”** for more on this topic.



Media management tools (like iTunes) can give you different ways to browse and sort your videos, without affecting how the files are stored.

ORGANIZE: TOOLS FOR MEDIA MANAGEMENT

Using your Finder or File Explorer to browse organized directories and folders may be perfectly sufficient for your needs. However, if you need to navigate or sort your files in more complex ways there are many tools ranging from simple to highly sophisticated that you can use alongside your organized directories.

PERSONAL MEDIA MANAGEMENT APPLICATIONS

Personal media management tools often come pre-installed on your computer, or can be purchased for a low cost. These systems are usually very easy to use, but are limited in their functionality, so are best suited to small collections. Some examples include:

- iTunes
- iPhoto
- Windows Media Center

Note that personal **media management** tools are not usually built to allow you to export your information to other systems. If you enter a description of a video in iTunes library, for example, you cannot easily move that information into another system later on.

VIDEO PRODUCTION MEDIA MANAGEMENT SYSTEMS

Media management systems built for video production usually offer extra functionality beyond organizing your videos, which you may or may not need, such as logging, **transcoding**, batch processing tools and integration with video editing systems. These systems also usually provide more access to your video's technical **metadata**. Some examples include:

- CatDV
- Adobe Bridge

CUSTOMIZED DATABASES APPLICATIONS

If you have the in-house resources, you can customize off-the-shelf database applications to function as both a media management and a **cataloging** tool. This will take substantial time and know-how to develop, but will be specific to your needs. See “**Catalog**” in the workflow for more information. Common database applications include:

- [FileMaker Pro](#)
- [Microsoft Access](#)
- [OpenOffice Base](#)

INSTITUTIONAL-OR ENTERPRISE-LEVEL COLLECTION MANAGEMENT SYSTEMS

Museums, libraries, and corporations use specialized systems to manage their collections and **repositories**. These systems usually require professional support to install, customize and maintain. They are suited to large collections. Some examples include:

- [Collective Access](#)
- [DSpace](#)

ORGANIZE: TAKEAWAYS

- **Always preserve the original order when naming and organizing your files.**
- Do not rename filenames assigned by a camera.
- Do not use “illegal” characters such as @#\$\$% &*”<>?/\~| or spaces in folder or file names.
- Do not make your folder or filenames overly long (260-character limit on total filepath)
- Name files consistently by following a template.
- Use **unique identifiers** to identify and help organize your files.
- Use “**information packages**” to keep media and **metadata** together.
- Organize your information packages into directories.
- Use a **media management** tool if you need to navigate your collection in more complex ways.

KEY CONCEPTS IN THIS SECTION

Information Package

Content can be organized into self-describing units of content, called information packages.

[Read More...](#)

Unique Identifier:

Unique identifiers are a helpful organizing tool for identifying items in your collection, and grouping them with or distinguishing them from others.

[Read More...](#)

KEY CONCEPTS IN THIS SECTION

Original Order:

Videos should be organized in a way that preserves the context of their creation.

[Read More...](#)

Metadata:

Metadata is the basis for organizing your content.

[Read More...](#)

Findability:

Good organization supports navigation and retrieval, and contributes to the findability of an item.

[Read More...](#)

THE WORKFLOW: STORE

STORE: INTRODUCTION

Storage is not just the device or service you use to hold your videos; it also requires a set of actions or practices to ensure your media stays intact, secure, and accessible. Making copies, checking files, controlling access, and **refreshing** your devices are simple strategies for keeping your videos safe while in storage.

A SCENARIO

AN ACTIVIST'S PERSONAL COLLECTION

Ryan has been filming various events, protests, and meetings that he has participated in for the past year. He has amassed a collection of over a hundred videos that serve as a document of the social movement that he is part of. He stores his videos on a 4-bay **RAID 5 Firewire** unit at home, which is backed up to an external hard drive using Time Machine. To protect against accidental deletion, Ryan keeps his videos separate from his family's other files, and sets read-only permissions on the videos. Also, every couple of months, he makes a copy of his collection on a hard drive and brings it to his brother's house.

A hurricane sweeps in to the region while Ryan is on vacation, causing major flooding in his home. The Firewire unit is water-damaged beyond repair. To make matters worse, the Time Machine backup was kept on the same shelf as the Firewire unit and is also damaged. Most of Ryan's collection can be recovered, however, thanks to the copy he brought to his brother's house two months ago.

CAUTION!

BEWARE PHYSICAL THREATS

Your storage devices may be vulnerable to physical theft, seizure, or destruction. Protect your stored collections by controlling access (e.g. a locked room), monitoring the area (e.g. security camera, alarm system), and keeping them away from potential physical hazards (e.g. windows and heating/air conditioning units, and off the floor).

BEWARE NETWORK THREATS

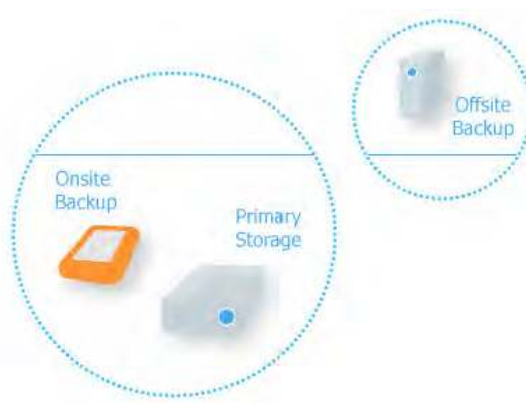
If your storage devices are connected to your network, they may be vulnerable to hacking and **malware** such as viruses or spyware. Some precautions include making sure you have firewall software installed and turned on, only downloading or opening attachments from known and trusted sources, and using strong, uncompromised passwords.

ENCRYPT SMARTLY

Encrypting your storage devices or volumes can be risky. While encryption protects sensitive data from being read by the wrong people, it can also mean that your data is locked up forever if you lose the key. Depending on the encryption, there may be no way to “crack” or decrypt your files without the key.

STORE: STORAGE STRATEGIES

MAKE COPIES



Have 3 copies in 3 different storage locations: primary storage, an onsite backup, and an offsite backup.

Storing multiple copies is the most important strategy to ensure that your videos are not lost. You should make at least two copies of your **originals**, and keep them in different storage locations. Having copies allows you to recover content that has been accidentally deleted, tampered with, or become corrupted. Keep one copy onsite with your originals so you can access it quickly if needed, and one copy offsite in case something happens at your physical space like theft or flood.

USE A BACKUP TOOL

For the parts of your storage that will be updated or changed (e.g. directories in which you add new videos or documentation, or that you plan to reorganize later), use a **backup** tool to make copies. Backup tools allow you to schedule regular backups to keep up with new content and updates. It can be more efficient than simple copying, because backup can be done incrementally. Backup tools also facilitate the restoration process when damaged or lost files need to be recovered.

Your computer likely comes with backup software installed, such as Time Machine (Mac), or Backup and Restore or File History (PC). There is also various backup software that you can purchase (e.g. Backup Exec) or download for free (e.g. Bacula).

WHAT ABOUT SYNCHRONIZATION?

Some services like [Dropbox](#) and [Google Drive](#) offer **synchronization**, also known as replication or mirroring. Synchronization mirrors the files in one location (e.g. a directory on your computer) to another (e.g. your online account). Its purpose is to allow you to access the same content in multiple locations. Synchronization is an easy way to make copies, but it is important to note that, unlike regular copies or backups, synced locations are constantly updated to be identical to one another.

If you accidentally change or delete a file in one location, that deletion is also made in the synced location; you therefore cannot restore from a synced copy like you would from a regular copy or backup. Interestingly, some services like [Dropbox](#) additionally offer backup for synced files, allowing you to restore deleted files or previous versions of changed files.

SEPARATE YOUR COPIES

Having lots of copies will not always protect you from loss if all your copies are in the same place. Imagine for example, if a natural or man-made disaster were to strike, if your property were to be seized, or you were to be barred from entering the locale where your collection is stored. Keeping copies in different places is one of the most important things you can do to safeguard your collection.

REGIONAL SEPARATION

Separate your copies geographically in case something catastrophic happens at one site, such as a flood or bombing. The appropriate location for your secondary copies depends on the threats you face. For example, if you are in a politically unstable region, keep a copy outside of the region; if you are in an environmentally vulnerable area, keep a copy outside of the area.

INSTITUTIONAL SEPARATION

If your organization is under threat, whether politically, financially, or otherwise, consider keeping a separate copy with another organization. Choose an organization that you trust with your collection, and that would not be vulnerable to the same threats as you. See the **“Preserve”** section in the workflow to learn more about finding a long-term archive.

STORAGE MEDIA SEPARATION

If possible, store your copies on 2 different types of storage media (e.g. networked storage, external hard drives, offline data tape, etc.) so that you are protected against the particular vulnerabilities of each one. For example, if your networked storage is compromised by hackers, it is good to have copies on offline external hard drives.

CONTROL ACCESS

An important way to safeguard your collection is to control who has physical and electronic access to your storage devices.

- Keep your storage devices in a physically secure place, accessible only to those who need to handle the hardware.
- Store your video files on a volume separate from your other files to limit the number of people who need to access the storage location.

- Set your file sharing and permissions so that only certain people have write-access to the volumes where your collection is stored.
- When you need to provide access to particular files to someone, copy the file and make it accessible in a separate location.

ENSURE FILE FIXITY

Storage includes making sure your stored files remain intact and unchanged over time, which can be helped by performing **fixity** checks. This means computing and comparing a file's **hash value** (also commonly called a checksum) with a previously computed hash value. See **“Keeping Files Intact (and Proving It)”** for more on hashes.

Compute (and make a record of) a hash when you first receive a file, and again when you want to check it. As long as a file remains exactly the same, its hash value will always be the same. If the file is altered in any way, its hash value will be different. You can compare hashes to confirm that files have not become corrupted, that you have copied a file properly from one location to another, or to see if two files in different storage locations are the same as one another.

If a fixity check shows that a file has been altered or corrupted, restore (i.e. make a new copy of) the original file from one of your backup copies.

REFRESH YOUR STORAGE MEDIA

More than likely, you have experienced the frustration of a failed hard drive, a jammed optical disk, or odd-sized memory card for which you have no card reader. No matter what kind of media or device you use, none are designed to last beyond the short-term. The actual lifespan of a piece of media or hardware depends on many factors such as its environment and use, but you should anticipate needing to replace your storage media and hardware every few years.



Old hard drives at WITNESS that have failed.

STORE: STORAGE MEDIA / HARDWARE

CHOOSING STORAGE MEDIA

There are many different types of storage media, and you can use them in different combinations in a storage system. How to decide? Here are some key considerations:

LEVEL OF IT SUPPORT AVAILABLE

You will have problems if you choose a system and do not have access to the resources and skills needed to operate and maintain it.

SIZE OF YOUR COLLECTION

Consider the total size of your collection and the size of an average file. If your collection is made up of large video files, for example, DVD-Rs are probably not a good choice since each disk can only hold 4.7 GB of data. Even if your files could fit on a disk, you would end up having to manage hundreds of disks (which could easily fit on a single hard drive).

WHO NEEDS ACCESS AND WHERE

Different devices and media offer varying degrees of accessibility. If multiple people need to access the collection at the same time from different places, for example, a set of external USB hard drives will not work as well as a networked storage device, like a **NAS**.

EASE IN REFRESHING

The ease with which your files can be copied to new media and hardware is an important consideration. Copying data off hundreds of DVD-Rs, for example, would be very tedious!

COMPARISON OF TYPICAL STORAGE MEDIA / HARDWARE

PORTABLE HARD DRIVE



A hard disk drive with an external casing that can be easily plugged into or removed from a computer.

- **Ideal for**
 - Collections no larger than 2-3TB.
 - Collections that only need to be accessed by one computer/user at a time.
 - Collections that need to be moved.
- **Advantages**
 - Relatively low cost (usually \$100-\$500).
 - Portable.
- **Disadvantages**
 - Drives (especially FireWire) fail often.
 - Platform-dependent.

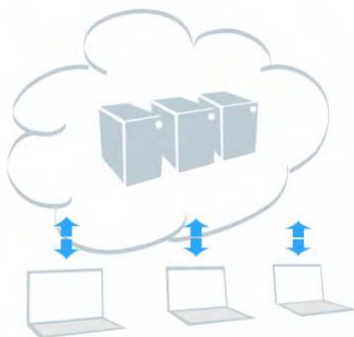
NETWORK-ATTACHED STORAGE (NAS) UNIT



A computer specially built to serve files from its storage devices to other computers in the network.

- **Ideal for**
 - Collections larger than 1TB.
 - Collections that need to be accessed by multiple networked users.
 - Networks with at least 1 Gb Ethernet, if files are large.
 - Organizations with IT support.
- **Advantages**
 - Multiple users can access NAS at the same time, collection can be consolidated.
 - Can be used in Windows/Mac mixed environments.
 - Relatively affordable (Consumer-grade NAS starts at \$200. Higher-end NAS ranges from \$1000-\$2000).
- **Disadvantages**
 - Potentially less secure because it is always on.
 - Less portable than external hard drives.
 - Requires skilled IT to resolve network problems.

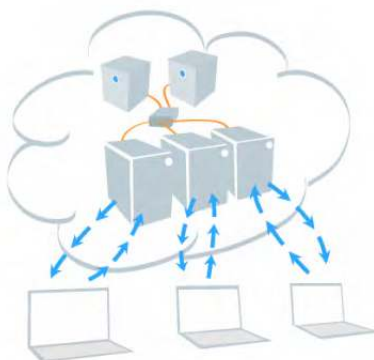
CLOUD STORAGE



Remote storage that is managed by a third party, like a data center. Content is stored on multiple servers, and is accessed by users through an online interface.

- **Ideal for**
 - Small collections.
 - Collections that need to be accessed by people in different locations.
 - Users with stable Internet access.
- **Advantages**
 - Collections can be shared around the world.
 - Storage is maintained by third party, often with significant infrastructure.
- **Disadvantages**
 - Need substantial bandwidth to **upload** and **download** files
 - Ongoing subscription fees for commercial services, sometimes also fees for access.
 - Service can terminate at any time, sometimes without notice or cause.

STORAGE AREA NETWORK (SAN)



A high-speed network of storage devices separate from a regular local area network. **SANs** make storage accessible to servers as if they were locally attached.

- **Ideal for**
 - Collections that require high-speed access, such as for video editing, over a network.
 - Collections that need to be accessed by multiple networked users.
 - Organizations with strong IT infrastructure and support.
- **Advantages**
 - High-speed network.
 - Multiple users can access collection at the same time, can consolidate collection.
- **Disadvantages**
 - High cost (starting at \$10,000).
 - Many hardware and software components, requires professional IT support.

WHAT IS RAID?

You may have seen the term “**RAID**” in the names or descriptions of disk-based storage devices. RAID stands for “redundant array of independent disks.” It is a storage technology in which multiple hard drives are used together to provide fault tolerance and improved performance. Data from your files is distributed across drives with some additional calculated data, so that they can be recovered if part of the RAID gets damaged.

A RAID provides protection for your files in case a piece of hardware fails. Fault tolerant storage is not the same as having multiple copies or backup, however, and does not provide as much protection as having multiple copies or **backup**. Fault tolerant storage allows you to rebuild data when a drive fails, but does not allow you to recover corrupted, deleted, or altered files.

There are a number of ways that data can be distributed in a RAID. The standard configurations are referred to as RAID “levels” (e.g. RAID 5, RAID 6). Different RAID levels provide different degrees of fault tolerance. Generally, the more fault-tolerant your storage is, the more disk space is required to store your collection.

STORE: TAKEAWAYS

- **Make (at least) 2 **backup** copies of your originals. Keep one backup copy onsite for quick recovery, and one offsite in case of major disaster.**
- For the parts of your storage that are frequently updated or changed, use backup software that can perform incremental backups.
- **Synchronization** – also known as replication or mirroring -- is not the same as backup. Synchronization does not allow you to go “back in time” to recover lost or changed files.
- Separate your copies in different geographic locations, on different media, and even with other organizations.
- Control physical and electronic access to your collection to prevent accidental or deliberate tampering and deletion.
- Use **hashes** – also known as checksums -- to periodically check your files for errors to ensure data integrity.
- Consider your available IT support, nature and size of your collection, and access requirements when choosing storage media and devices.
- Different storage media and devices are ideal for different situations. Choose the ones that suit you.
- Fault tolerant storage (i.e. **RAID**) can protect your files when hardware fails, but it is not the same as copying or backup.
- Anticipate the need to **refresh** (i.e. replace) your storage media and devices every few (approximately 3-5) years.

KEY CONCEPTS IN THIS SECTION

Refreshing:

Storage devices are not long lasting, and need to be replaced every few years before they fail.

[Read More...](#)

Fixity:

The aim of good storage strategies is to ensure the integrity of stored objects over time.

[Read More...](#)

THE WORKFLOW: CATALOG

CATALOG: INTRODUCTION

Cataloging means creating and organizing descriptive information in a structured way so that video can be found, used, and understood. Cataloging allows you to expand on the basic **metadata** you have acquired, and should help you better access your content. A catalog may include descriptive information, contextual information, technical information, rights information, keywords and so on. To ensure future access, especially for larger collections, some kind of cataloging is critical.

Be forewarned that building a catalog is a labor-intensive process and that cataloging requires skills and knowledge of the video content. Rather than doing it yourself, you may want to work with an institution with trained staff, such as an archive or library. You can start, however, by making a simpler inventory -- a list of your media that contains only the most essential information -- which can eventually grow into a full catalog.

The screenshot displays the 'Witness Video Archive - 2 (Antarctica)' interface. At the top, there's a search bar and a list of items. Below this, a detailed view of a specific item is shown. The item is titled '7835 | Why TRUST for Earth Day? - #WITNESSlive'. The interface includes various tabs for navigation: Search, Summary, Preview, Titles & Credits, Content & Description, Logs & Scripts, Items, Rights & Security, Usage History, Admin, and Preservation. The 'Summary/Description' tab is active, showing a detailed description of the video content. To the right of the description, there are several form fields for metadata, including Date Type, Date, Geographic Locations of Footage, Topic Keywords, Corporate Names, Personal Names, Languages, and Notes. The interface is designed to be user-friendly, with clear labels and a structured layout for entering and viewing catalog data.

A screenshot from a video catalog.

A SCENARIO

STEPS TOWARD BUILDING A CATALOG

The Institute for Democracy has a video collection that documents democracy movements worldwide. As part of its mandate, it provides access to the collection to researchers. The Institute maintains a simple inventory of its videos in an Excel spreadsheet.

Miyoko, a graduate student, comes to the Institute to research Chinese democracy movement activists. She uses the inventory to narrow down her search, but since the metadata is limited, she has to view a few dozen videos to identify the ones that are about the activists she is researching. Still, she eventually finds what she is looking for.

The Institute starts to host more and more researchers like Miyoko who are interested in the video collection, and realizes that it needs a more robust way for them to find what they are looking for. First the Institute assesses their existing capacity and hires Grace, an archivist. Grace consults with researchers to learn how they want to find content, evaluates the collection, and assesses existing **metadata standards**. She then chooses Dublin Core as a metadata standard, and selects Filemaker Pro as a database platform. Grace works with a programmer to build the database. Once the database is set up, she begins cataloging newly acquired videos in it. She also recruits and supervises interns to catalog the existing collection. Eventually, records are created for all of the videos in the Institute's collection, and researchers are given access to the database.

CAUTION!

PROTECT SENSITIVE INFORMATION

Before you create a catalog, identify videos or information that need to be kept private. Identify videos that cannot be published or shared at all, and videos that can be shared, but that contain information that needs to be restricted, such as the identities of people depicted or the videographer.

CATALOG: GETTING STARTED

START WITH AN INVENTORY

Building a catalog can be a labor-intensive process, and **cataloging** requires at least some training. Start small by creating a simple inventory of your collection. An inventory is a list of your videos with only essential information such as ID, file or folder name, title, storage location(s), and security restrictions. An inventory can provide basic access to your collection until you are able to build a more elaborate catalog, and the data you enter in the inventory can be incorporated into it.

Package ID	Package Title	Filename	Storage Location	Project	Content Type
E007746	[Interview with Florence Mwenge in Bukavu]	VID00006.MP4	SAN11_Archive	P-GBV01	Raw
E007746	[Interview with Florence Mwenge in Bukavu]	VID00009.MP4	SAN11_Archive	P-GBV01	Raw
E007745	[Interviews with Aline Keke Mwenzeavake in Bukavu]	VID00033.MP4	SAN11_Archive	P-GBV01	Raw
E007745	[Interviews with Aline Keke Mwenzeavake in Bukavu]	VID00034.MP4	SAN11_Archive	P-GBV01	Raw
E007745	[Interviews with Aline Keke Mwenzeavake in Bukavu]	VID00035.MP4	SAN11_Archive	P-GBV01	Raw
E007696	[Demonstration by mothers of disappeared in Chechnya]	B04015-1.mov	SAN6_Archive	P-MEM02	Raw
E007696	[Demonstration by mothers of disappeared in Chechnya]	B04015-2.mov	SAN6_Archive	P-MEM02	Raw
E007696	[Demonstration by mothers of disappeared in Chechnya]	B04015-3.mov	SAN6_Archive	P-MEM02	Raw
E007696	[Demonstration by mothers of disappeared in Chechnya]	B04015-4.mov	SAN6_Archive	P-MEM02	Raw
E009129	[Visit to Río Santiago and riverside communities El Salto / Juanacatlán]	DSC_5548.MOV	SAN9_Archive	P-FEMEX01	Raw
E009129	[Visit to Río Santiago and riverside communities El Salto / Juanacatlán]	DSC_5549.MOV	SAN9_Archive	P-FEMEX01	Raw
E009129	[Visit to Río Santiago and riverside communities El Salto / Juanacatlán]	DSC_5550.MOV	SAN9_Archive	P-FEMEX01	Raw
E009129	[Visit to Río Santiago and riverside communities El Salto / Juanacatlán]	DSC_5551.MOV	SAN9_Archive	P-FEMEX01	Raw

Example of a typical inventory.

EVALUATE YOUR COLLECTION

Before deciding to build a catalog, evaluate whether you really need something more complex than an inventory (and acquired **metadata** and documentation) to make your videos findable and understandable. An inventory may be sufficient.

If you do want to make a catalog, consider aspects of your collection that will affect the complexity of the catalog and time required to build it:

COLLECTION SIZE

How many items do you have? What is your rate of acquisition? The catalog you need for 100,000 titles will be different from one for 10,000.

INFORMATION NEEDS

How complex is the information you need to capture?

ACCESS NEEDS

How do you or your current or future users need to access information? What are the gaps in your current ability to search, and what functionality does your catalog need to have to address them? What are the critical **access points**?

RESTRICTIONS

Is there restricted data that only some users should be able to see?

DO YOU HAVE THE RESOURCES?

A catalog is only useful if it is properly maintained. The amount of work required depends on the size of your collection and what you wish to do with it. Evaluate your capacity for building and maintaining a cataloging system.

- Do you have at least one trained person who can oversee the cataloging?
- Do you have enough people who can dedicate significant amounts of time to being trained and doing the cataloging?
- Do you have the technical support to build or customize your cataloging system?

- Do you have the IT support to maintain a cataloging system?
- Do you have an ongoing budget to sustain sufficient staff and the cataloging system?

DEFINE STRUCTURE, RULES AND ACCESS POINTS

Choose the metadata standard(s) that your catalog will be based on, or create your own (see “**Structure and Rules**” for more on this). A **metadata standard** is a set of rules that defines the kinds of information and how it is structured in a catalog. Many metadata standards have been developed by various communities to suit different kinds of materials. Using an existing standard (or combination of standards) saves you the effort of creating rules from scratch, and makes your data more **interoperable**. To meet the search needs of your users, you can also customize and add additional access points to your catalog.

DEVELOP A CATALOGING SYSTEM

Your catalog must be built on a system that allows you to create, structure, and search records. Typically, catalogs rely on some kind of computer database (see “**Tools for Inventories and Catalogs**” for more on this). Choose a system that you have the resources to develop and support.

TRAINING AND QUALITY CONTROL

Cataloging is more complex than it may seem at first glance. Describing content – especially human rights content – requires familiarity with the subject matter. Decisions need to be made on what to prioritize or spend time on.

A usable catalog must always adhere to its established structure and rules, otherwise data will not be effectively searchable, and relevant materials cannot be found. Consistency can be difficult to achieve, however, as language is inherently full of ambiguities.

Using volunteers to catalog is a great way to get large volumes of work done, but there should be at least one person with the skill and oversight to train them and ensure quality control. Rules and terminology should be clearly documented. Catalogers can also check each other’s work.

START WITH NEW VIDEOS FIRST

Do not imagine you will have all your videos cataloged once your system is in place. Cataloging takes a lot of time; the world’s biggest archives can take years to catalog a collection. Start with newly acquired videos, and set up a process for cataloging older or existing video as time allows.

CATALOG: TYPES OF METADATA

You can include as many data fields or elements as you want in your catalog, but there are a few types of information that are most important to make your videos identifiable and findable.

SOURCE METADATA

The date recorded, the geographic location of recording, the identity of the creator(s).

Date Recorded	2013-03-23
Location	38.897096,-77.036545
Creator	Cortez, Ricky

Example of some source metadata.

CHAIN OF CUSTODY

Who you acquired the video from and when, who had custody of the video prior and when, any changes made to the video file and when it happened, **fixity** checks (i.e. **hashes**).

Date Acquired	2013-03-29
Acquired From	Cortez, Ricky
Date of Fixity Check	2013-03-29
MD5 Hash Value	050c4e80050fe93033edcdf58f57e3aa

Example of some chain of custody metadata.

DESCRIPTIVE INFORMATION

What is happening in the video, who is depicted in the video, background information about the event, and why the video was recorded.

Summary	Bukeni Waruzi interviews an Akhdam woman from Sana'a who has suffered violence due to her ethnicity. Video was recorded in Washington DC as part of project to document ethnic discrimination in Yemen.
---------	---

Example of some descriptive metadata.

SECURITY RESTRICTIONS

What information in the video needs to be restricted and from whom.

Restriction Status	Restricted
Restriction Detail	Interviewee does not want her full name used. Face and voice do not need to be obscured.

Example of some security restriction metadata.

RIGHTS

Who owns the video, who is allowed to use the video and how.

Rights Owner	WITNESS
Rights Declaration	Available for public use under Creative Commons-Attribution-NonCommercial-NoDerivatives license.

Example of some rights metadata.

CONTENT TYPE

Whether the video is raw or edited, and the specific types of content in the video (e.g. interview, news report, livestream, etc.)

Content Type	Raw video
	Interview

Example of some content type metadata.

VIDEO AS EVIDENCE TIP

Accurate and truthful cataloging will support the use of your video as evidence. Always be clear about disputed or unverified information, and do not editorialize.

KEYWORDS, TAGS, AND SUBJECT TERMS

Access points with any terms that help make the video findable.

Topics	Discrimination
	Violence
	Ethnicity
Group Names	Akhdam
Geographic Locations	Sana'a
	Yemen
	Washington DC
	United States of America

Example of some subject term metadata.

TECHNICAL METADATA

Technical data about the video file from the file itself.

Generation	Camera Original
Format	MPEG-4
Video Encoding	AVC
File Size	71 MB
Duration	00:08:13

Example of some technical metadata.

CATALOG: STRUCTURE AND RULES

Cataloging is all about structure and rules.

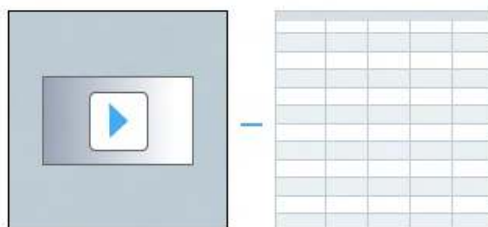
METADATA STRUCTURE

To begin, every catalog must have a structure, or **data model**, that defines **entities** and the relationship between different entities. An entity is a “thing” about which data is collected, such as a video, a person, or an event. In a relational database, an entity is the equivalent of a table.

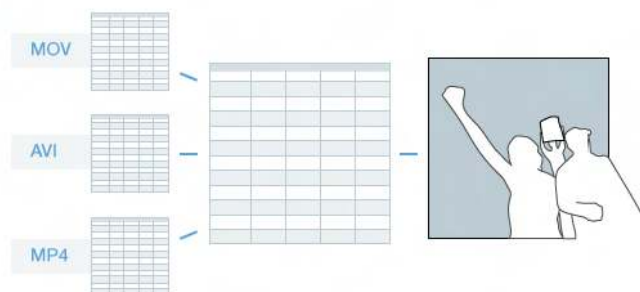


An entity is any “thing” that is being described.

In its simplest form, a catalog may only have one entity. In an inventory, for example, the entity or “thing being described” might be the video file. Each record in the inventory spreadsheet represents one video file, and all of the data in the spreadsheet describe those files.



A more complicated catalog can describe more than one “thing” and involve multiple entities. This can be done with related tables in a database. For example, imagine you have copies of every video in your collection in 3 different file formats. If you made an inventory record for each of the three copies, the same descriptive information would be repeated in each one; only the technical information about the file formats would change. By creating a separate entity for “video content” to hold the descriptive information, you would only need to describe the video content once, then relate it each of the three records with the technical file information.



A catalog can have multiple entities that relate to each other.

METADATA RULES

In a catalog, all of the records within a particular entity must contain the same set of fields, and data must be entered in those fields consistently. For example, if you search a “Subject” field for “Protests” but a cataloger sometimes uses the term “Demonstrations” instead, you will not find all the videos you are looking for.

SUBJECT		
protest		
protest		
demonstration		
protest		
protest		

For each field in your catalog, define rules for what information gets entered and how. For example, if you have a field for “Date Recorded” you must define what you mean by “Date Recorded” and what format you want the date entered in (e.g. yyyy-mm-dd). You can make data entry in particular fields mandatory or optional.

³² <https://www.huridocs.org/resource/micro-thesauri/>

³³ <http://www.vocabularyserver.com>

³⁴ <http://pbcore.org>

³⁵ <http://dublincore.org/documents/dces/>

DATE RECORDED		
2013-05-01		
1 May 13		
05/01/2013		
May 1, 2013		

Try This BASIC

HURIDOCs³² provides 48 different micro-thesauri, or lists of terminology, relevant to human rights documentation that can be used to create controlled vocabularies.

DOCUMENT YOUR RULES

Document your structure and rules and a cataloging manual or “data dictionary” so that all catalogers understand the structure and follow the same rules when entering data. To ensure text is entered into fields consistently, create **controlled vocabularies**, or lists of allowable terms with preferred spelling. If possible, use built-in tools in your cataloging software— such as drop-down lists or dialog box warnings-- to enforce rules.

Try This ADVANCED

Tema Tres³³ is a content management system for controlled vocabularies.

METADATA STANDARDS

A **metadata standard** is a set of structure and rules for describing all kinds of materials. You do not have to adhere to a standard, but there are two obvious benefits to doing so. One is to save yourself from having to develop your own structure and rules from scratch; the other is to make your data more interoperable –easier to share with others or export to other systems. You can use different metadata standards in combination and add custom structural components and fields to meet your needs.

Try This BASIC

PBCore³⁴ is a metadata standard for audiovisual materials developed by the public broadcasting community in the US.

Try This BASIC

DublinCore Metadata Element Set³⁵ is a widely used, simple set of fifteen elements for describing any kind of digital resource.

³⁶ <http://www.ica.org/10207/standards/isadg-general-international-standard-archival-description-second-edition.html>

Try This
BASIC

General International Standard Archival Description³⁶ (ISAD(G)) is a standard for describing digital and non-digital archival collections.

CATALOG: TOOLS FOR INVENTORIES AND CATALOGS

Catalogs and inventories can be created in many formats, using many different technologies. You may recall that library catalogs were once cabinets full of carefully organized printed index cards. Today, catalogs can take forms ranging from simple but organized text documents, to spreadsheets, to more complex databases.

Some easily accessible tools to make inventories or flat/single-entity catalogs:

- [Microsoft Excel](#)
- [Google Spreadsheets / Google Forms](#)
- [Omeka](#)

Some easily accessible tools to make catalog databases:

- [Microsoft Access](#)
- [FileMaker Pro](#)
- [MySQL](#)

These tools can provide the technological basis for your catalog, but you will still need to build it according to your own structures and rules, and enter the data to create the catalog records.

CATALOG: TAKEAWAYS

- **Cataloging is labor-intensive, and requires training and quality control.**
- **Before cataloging, start by making an inventory of your collection.**
- Assess whether you need a catalog, and whether you have the resources to build one.
- Start cataloging new videos first. Set up a process for cataloging the backlog later.
- Source **metadata**, **chain of custody**, descriptive information, and security restrictions are among the most important metadata to catalog for human rights evidentiary video.
- Define your metadata structure and rules, and document them in a cataloging manual or data dictionary.
- Using **metadata standards** can make your work easier and your catalog more **interoperable**.
- You can use a spreadsheet to make a simple catalog, or a database for a more complex catalog.

KEY CONCEPTS IN THIS SECTION

Interoperability:

Using metadata standards ensures that your metadata can be more easily used and understood by others.

[Read More...](#)

Data Model:

A data model defines how metadata is structured and organized in a catalog.

[Read More...](#)

Controlled Vocabulary:

Catalogs use controlled vocabularies to ensure consistency and findability.

[Read More...](#)

Metadata Standard:

Cataloging relies on standardized structures and rules for creating metadata.

[Read More...](#)

Findability:

The primary purpose of cataloging is to enable and improve findability.

[Read More...](#)

Metadata:

Metadata is the basis of cataloging.

[Read More...](#)

THE WORKFLOW: PRESERVE

PRESERVE: INTRODUCTION

Preservation means ensuring the long-term accessibility of your collection. All of the actions outlined in this guide up to this point are part of the digital preservation process. However, the long-term aspect of preservation requires additional commitment and actions. In most instances, you cannot do this alone. Even the biggest institutions need to collaborate when it comes to preservation.

A SCENARIO PARTNERING WITH AN ARCHIVE

The Center for Human Rights produces videos for its campaigns. Over the years, the videos have grown into a large collection, which the organization regularly draws upon in its work. The organization has built its **archive** up over time, and it now employs an Archivist and has a stable system for managing its collection.

The Center recognizes that its videos have important historical and educational value, but does not have the mandate or resources to provide external access, so no researchers have ever been able to make use of the collection.

Eventually, the Center decides to reach out to Major University Library, which has a collecting focus on human rights. After some negotiation, the Center agrees to deposit a copy of all of its videos in the library's digital **repository** for research, scholarly, and public access. The Center transfers copies of its collection and catalog to the MU Library, while maintaining its in-house archive to support its ongoing campaign work.

CAUTION!

PROTECT SENSITIVE INFORMATION

If you work with an archive, make sure that you inform the archive of all security restrictions on your videos.

PRESERVE: ASPECTS OF LONG-TERM PRESERVATION

While all of the steps outlined in this guide contribute to the preservation of your videos, there are additional elements to consider when thinking in a long-term context:

TECHNOLOGICAL CHANGE

As you have likely experienced, technology changes rapidly and dramatically, and hardware does not last long. Even if your videos remain intact and uncorrupted in storage, at some point in the future they may become **obsolete**-- unplayable because new machines and software will not be able to read them.

Long-term preservation involves not only maintaining the original, but also regularly **refreshing** it on new storage media and, for access, **migrating** to up-to-date formats or building software that can play the obsolete format.

SUSTAINED COMMITMENT AND INVESTMENT

By definition, preservation requires ongoing resources. Whoever is going to preserve your videos has to be able to commit to investing what is necessary to retain, manage, and provide access over a long period of time. This includes technological and organizational infrastructure, skilled staff, financial resources, planning, and policies.

PRESERVE: PRIORITIZING FOR PRESERVATION

Because of the significant resources that **preservation** requires, it is prudent to prioritize some videos over others for long-term retention and access. Note that your priorities for long-term preservation might differ from your priorities for immediate or medium-term use.

For example, sharing an Al Jazeera newscast on your website might be a good idea now, but you may not want to preserve it in the long run because it belongs to Al Jazeera and it is being preserved elsewhere, probably in a higher quality and with more documentation. Your resources would be better spent preserving an original evidentiary video in your collection that no one else has.

Here are some general prioritization criteria to maximize your preservation resources:

ARCHIVAL VALUE?

Is the video significant and useful as evidence or information?

UNIQUE?

Is this video a copy? Is the original or a higher quality copy being preserved elsewhere? Note that sometimes a lower quality copy is the only one that exists, and is worth keeping.

HAS CONTEXT?

Does the video have enough context to be understandable as evidence or information?

RIGHTS?

Does the video belong to someone else, and are your **rights** to reuse it limited?

	Video from known activist's camera, with complete metadata.	Youtube video by anonymous activist with limited descriptive information.	Al-Jazeera news video retrieved from the web.
Archival Value	Yes	Yes	Yes
Uniqueness	Yes	Maybe	No
Sufficient Context	Yes	No, needs research.	Yes
Rights	Yes, if obtained.	No, unless CC licensed.	No, unless licensed.
Preservation Priority	HIGH	MEDIUM	LOW

An example of how criteria could be used to prioritize different videos for preservation.

PRESERVE: WORKING WITH AN ARCHIVE

Most individuals and organizations cannot do long-term **preservation** on their own. Rather, they partner with an institution that has a specific mandate for preservation, such as an **archive**, historical society, museum, or library. You may also look to institutions engaged in gathering evidence, like human rights organizations, documentation centers, and courts and tribunals that have archives.

An archive that is potentially interested in acquiring your collection will likely want to first assess whether



Institutions like the US Library of Congress have significant infrastructure to support archiving and preservation.

it has value and fits with their interests, and what the usage restrictions will be. The archive will also want to do an initial survey of your collection to understand its size, scope, and **formats**. Having an inventory or catalog of your collection can facilitate this process.

Working with an archive does not mean that you must give up your collection. With digital collections, you can easily deposit an exact copy of all your videos and documentation to an archive, while holding on to your own copy. Because of their investment, most archives will want rights to provide access to your collection to their users, and many will want you to eventually donate your collection. Some archives, however, are open to deposit relationships where you do not have to give up ownership of your collection.

VIDEO AS EVIDENCE TIP

Depositing a video with a trustworthy archive that performs regular repository audits can simplify your work of maintaining an unbroken chain of custody.

CHOOSING AN ARCHIVE

There may be one or many institutions or organizations interested in acquiring your collection. When choosing a potential archive, there are several factors you should consider:

TRUSTWORTHINESS

Do you trust the archive (and the institution it may belong to) to take care of your collection and abide by its agreements with you (e.g. regarding security restrictions, access, preservation)?

RESOURCES

Does the archive have the staffing and infrastructure to meet the processing, storage, preservation, and access needs of your collection?

COLLECTING FOCUS

Does the archive have a real interest in your collection, and experience and expertise in dealing with collections similar to yours?

RESTRICTIONS/ACCESS

Can the archive accommodate your expectations for security and privacy restrictions?

OWNERSHIP

Do you want to retain ownership of your collection, or are you willing to transfer ownership to the archive? Some archives will accept collections they do not own, but some will not.

RIGHTS

Do you own the copyright or have rights to the content in your collection? If not, can you provide the archive with information about third-party rightsholders? Archives need to understand the rights restrictions in order to provide access.

DEPOSIT LOGISTICS

Are you able to get your collection to the archive?

DONOR/DEPOSIT AGREEMENTS

If you work with an archive, draft a written agreement that outlines their acquisition of your collection and the terms of your relationship. This ensures that both sides clearly understand their rights and obligations, which ultimately protects the collection.

The main areas that the written agreement should address are:

SCOPE

What exactly is being acquired by the archive? What is not being acquired?

OWNERSHIP AND RIGHTS

Who owns the collection, and what rights are being transferred to the archive?

RESTRICTIONS

How will materials with restrictions be handled? When, if ever, will the restrictions expire?

RESPONSIBILITIES

What is the archive responsible for? What are you responsible for?

PRESERVE: OTHER PRESERVATION OPTIONS

You may have reasons for not wanting to deposit your collection at an established archival institution. Besides working with an archive, two other available options are to establish your own archive, and/or deposit your collection with a unique non-profit called the Internet Archive.

ESTABLISHING YOUR OWN ARCHIVE

It is challenging, but not impossible, to establish and sustain an archive on your own or with a network of like-minded organizations. This option requires significant ongoing infrastructure, human resources, and financial support.

Establishing an archive involves building a repository, developing archive policies and procedures, and performing the day-to-day work of acquiring, cataloging, preserving, and providing access to users.

Try This ADVANCED

OAIS Reference Model³⁷ is an International Organization for Standardization (ISO) standard that defines archive concepts and establishes the minimum requirements for an archive.

Try This ADVANCED

Audit and Certification of Trustworthy Digital Repositories³⁸ provides metrics for measuring the trustworthiness of your digital repository.

INTERNET ARCHIVE-BACKED ARCHIVE

The Internet Archive is a unique non-profit digital library that allows the public to upload and download digital material at no charge. Its mission is to provide permanent access to historical content in digital format. The Internet Archive holds approximately 10 **petabytes** of digital material in datacenters in California, USA and at Bibliotheca Alexandrina in Egypt.



³⁷ <http://public.ccsds.org/publications/archive/650x0m2.pdf>

³⁸ <http://public.ccsds.org/publications/archive/652x0m1.pdf>

You can use the Internet Archive as a way to store, preserve, and provide access to your videos. You can upload videos simply by setting up an account on the website. It is also possible to create sub-collections through special arrangement with Internet Archive. Videos hosted by Internet Archive can be easily embedded in other websites. With some technical expertise, it is also possible to build a GUI client for Internet Archive's S3-like **API** to upload your videos and descriptions.

Some important notes about the Internet Archive:

- Anything uploaded to the Internet Archive is accessible (i.e. streamable and downloadable) by anyone. You can choose to apply a Creative Commons license to your videos to designate how people can use your video, but this will not prevent anyone from simply viewing or downloading a copy.
- Internet Archive provides storage, preservation, and access, but it does not provide any cataloging or description to make your videos findable. You must upload your own descriptions along with the video. You can include as much metadata or as many related documents as you wish.
- Unlike YouTube and other video sharing platforms, Internet Archive does not transcode your video (except to make additional access copies), and allows anyone to download your original file.
- You retain the ownership over the content you upload; the Internet Archive does not assert any rights. If you upload content you do not have the rights to, however, be forewarned that the Internet Archive may remove it if it receives a valid complaint.

PRESERVE: TAKEAWAYS

- **Digital preservation is never-ending and requires an ongoing commitment of resources.**
- **Preserving videos requires regular refreshing on new storage media and migration to new usable formats.**
- Prioritize videos for preservation based on their archival value, uniqueness, contextualizing information, and whether you have rights to use them.
- Most small organizations cannot do preservation on their own. Consider partnering with an archival institution.

KEY CONCEPTS IN THIS SECTION

Refreshing:

Over time, video files need to be regularly moved to new storage media.

[Read More...](#)

Repository:

A repository is the locus of long-term digital preservation.

[Read More...](#)

KEY CONCEPTS IN THIS SECTION

Obsolescence:

Over time, file formats and storage media become unusable because the technology they rely on is unavailable.

[Read More...](#)

Migration:

Over time, video files need to be transcoded to new formats to remain usable.

[Read More...](#)

Fixity:

The long-term integrity of your original files is a fundamental goal of preservation.

[Read More...](#)

THE WORKFLOW: SHARE

SHARE: INTRODUCTION

Sharing involves enabling users to find, view, obtain, and/or use videos in your collection. To share effectively, you need to help your users find the videos they want, and then provide it to them in a **format** and medium they can use. Note that you may also need to set access limits to parts of your collection for safety and security or **copyright** reasons.

A SCENARIO

SHARING WITH AVAILABLE TOOLS

The Global Activist Media Group documents protests around the world, and wants documentary filmmakers to be able to find and use its video footage. The group is volunteer-run and relies on members' personal resources. Sameer, a member of the group, offers to make a **finding aid** for the group.

Sameer knows that filmmakers like to research footage online, and that they want to look for content by geographic location and date. He decides to set up a YouTube Channel to function as a finding aid to the group's videos. He names the Channel after the group, and in the description, he writes about the group, the collection, and how filmmakers can contact them. Sameer **uploads** low-resolution copies of the videos that the group wants to share, and adds them to playlists on the Channel, which are organized by geographic location. He makes sure that each video has a descriptive title, including the date, a **unique identifier**, and detailed description and tags. He also includes copyright and contact information in each of the descriptions.

Hannah, a filmmaker, hears about the Global Activist Media Group's collection and visits their YouTube Channel to look for footage for her documentary. After watching videos from the "Bahrain" playlist, she contacts the group with a list of the videos she wants to use. The group then locates and **FTP**'s full-quality copies of the clips to her.

CAUTION!

PROTECT SENSITIVE INFORMATION

Control access by obscuring or redacting parts of video or metadata that contain sensitive information, and do not share video or information that is private or has security restrictions. Assume that anything you share or put online can be made public, used without your permission, or used in a way you might not agree with.

SHARE: IDENTIFYING YOUR USERS

Who are your users? You probably know who they are, or who you would like them to be. For example, if the reason you are collecting videos is to gather stories in order break down negative stereotypes in your community, your users might be community organizations, law enforcement agencies, or schools. Make a list of your most important potential user types.

Users have different needs in terms of how they want to find videos, and how they want to access them. You may also want to limit access to videos or information according to user type. For each of your user types, consider:

FINDING AND IDENTIFYING VIDEOS

- What level of detail do they need in the descriptions you provide?
- What kind of terms or categories would they use to browse and search?
- What language(s) do they understand?

ACCESSING VIDEOS

- Does the user have technological or other barriers that require content to be made accessible in a certain way?
- Do they need copies of the videos, or just need to view them (e.g. from a website)?

LIMITS ON ACCESS

- Do you want them to contact you or obtain special permission for access?
- Do you want to collect any information from them before granting access?
- Does your content need to be edited or redacted before you can share it?

SHARE: HELPING USERS FIND VIDEOS

You can help people find videos in your collection by providing a document or platform that serves as a **finding aid**. A finding aid is any tool that helps your users navigate a collection and understand what is in it.

WHAT ABOUT MY INVENTORY OR CATALOG?

An inventory or catalog is an internal tool to manage your collection, whereas a finding aid is public-facing and meant for your users. You can re-purpose an internal inventory or catalog as a finding aid; just be sure to remove or hide data that is private or not relevant to your users, put it in a sharable format, and perhaps add some user **access points** (see “Making Videos Findable” below for more on this).

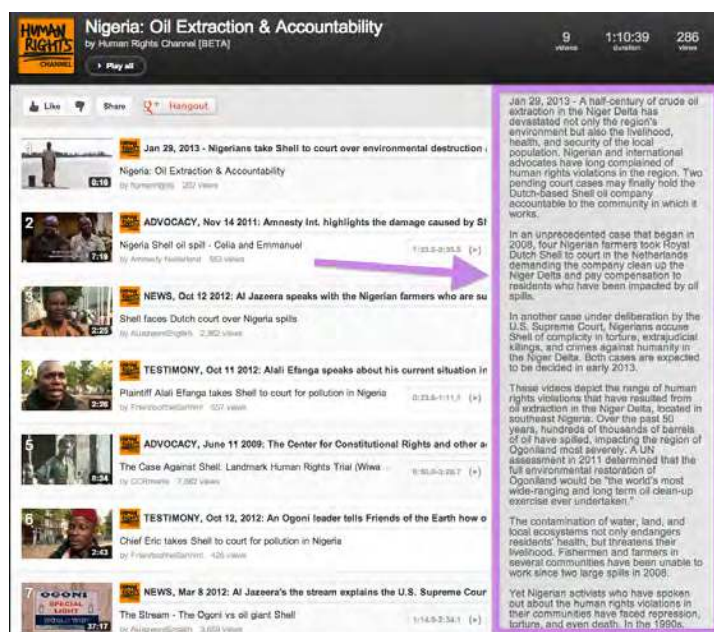
You do not need to have an internal inventory or catalog in order to make a finding aid. Alternately, if you do not have external users, you do not need to make a finding aid separate from your internal inventory or catalog.

TYPES OF FINDING AIDS

A single finding aid can incorporate more than one of these forms below:

GUIDE

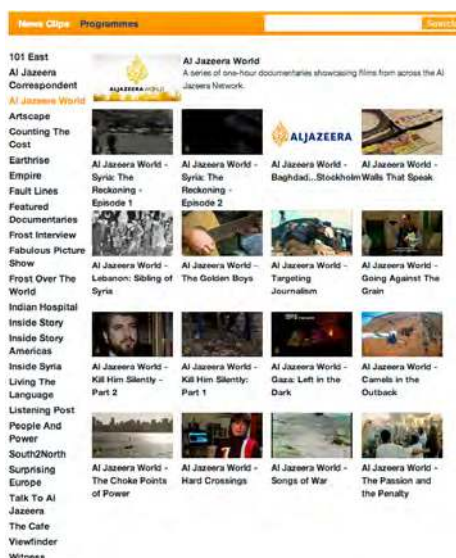
A written description that provides a broad overview of a collection. This can be useful if you do not have time to describe each video in your collection individually. You can also make guides for smaller groupings within your collection. Guides can be used in conjunction with lists.



The descriptive sidebar in this Human Rights Channel playlist is an example of a guide (which is used in conjunction with a list).

LIST

A list of the individual items in a collection informs people that the item exists, and provides minimal information (e.g. a title). You can use a list in conjunction with a guide.



Al Jazeera World's Programmes is an example of a list.

INDEX

[illegible]

CATALOG

[illegible]

78 ACTIVISTS' GUIDE TO ARCHIVING VIDEO: WORKFLOW - SHARE

TOOLS TO CREATE FINDING AIDS

There are many offline and online tools that you can use to create a finding aid or discovery tool:

- A spreadsheet application like [Microsoft Excel](#) or [Google Spreadsheet](#) can provide a way to present

Title	YouTube ID	Storage Location	Project	Keywords	Language
How to Set Up a Pocket Camera Kit.	PliGv_uvn9Y	dml2	P-WITLIVE	activists, cameras, mobile devices, documentation, human rights, technology	Eng
A Conversation About Gender Based Violence.	oxg08Ohyz50	dml2	P-WITLIVE	accountability, activists, art, gender based violence, men, social media, women	Eng
WITNESS and The Guardian Project Share the Latest News.	HsY64fOCA40	dml2	P-WITLIVE	activists, technology, mobile devices, privacy	Eng
The Intern Experience.	4ystQfpYEno	dml2	P-WITLIVE	education, WITNESS	Eng
WITNESS 20th Anniversary Interview Series: Emmanuel Jal.	hPCqQ2xOcUg	dml2	P-WITLIVE	ceremonies, music, WITNESS	Eng

- A database application like [Microsoft Access](#) or [FileMaker Pro](#) offers more functionality than a spreadsheet, such as repeatable fields. Database applications can be useful for making indexes and catalogs.
- Some video sharing websites like [YouTube](#) have features like channels and playlists that allow you to create guides and indexes to point to videos hosted on the site. The [YouTube Human Rights Channel](#) is a good example of a finding aid that helps journalists find human rights videos.
- A web curation platform like [Crowdvoice](#) or [Storify](#) can be useful for making guides and lists about content (including videos) that are already up on the web.
- A web content management system (CMS) like [Drupal](#) or [Wordpress](#) can be customized to make websites that function as indexes or catalogs. [Omeka](#) is a CMS that is especially designed for digital cultural heritage collections.

MAKING VIDEOS FINDABLE

No matter what form your finding aid takes, or what technology you use, make your videos findable by creating access points in the finding aid that match the way your users want to browse or search for content.

An **access point** is basically an entryway to the content in your finding aid. For example, if you have a list, the access points might be subheadings in the list that divide records up by topic. On the Syrian Revolution Martyr Database, for example, the list of videos is divided with headings for “Children Martyrs,” “Funerals,” “Poetry,” and so on. This provides its users with a way to find videos.

Identify the access points that would maximize your users’ ability to find and access what they want in your collection. For example, if your users are prosecutors in the International Criminal Court, they may want to find content according to the elements of a crime or by the name of a perpetrator. Or if your users are human rights organizations, they might be interested in finding content by geographic region or human rights issue.

MAKE VIDEOS FINDABLE ON YOUTUBE

While YouTube is not suitable for storing your collection, it is an excellent platform for sharing and providing access to your videos.

You can integrate videos uploaded to YouTube (or other video sharing websites) into finding aids as links or video embeds. As mentioned above, you can also create a finding aid within YouTube using its channel and playlist features.

If you are simply uploading your videos to YouTube with no finding aid, you can rely on YouTube's search and filters to help people find your videos. As you may have experienced, however, browsing and finding specific videos within the large volume of videos on YouTube and with its limited access points can be difficult. To maximize the findability of your videos on YouTube without a finding aid:

- For raw footage, upload the original file if possible (YouTube will not keep your original file, but will keep some of the original metadata from the file).
- Make your title informative, and include the date recorded and location of your video.
- Make your description informative, answering questions of who, what, when, where, and why.
- Tag your video using access points relevant to your users (see above).
- Make your titles, descriptions, and tags multi-lingual if your users understand different languages.

VIDEO AS EVIDENCE TIP

Many journalists and legal observers look for videos on YouTube.

Including the date recorded, location, and the name of the source (if safe) and other informative description is important to enable them to authenticate and verify your video.



The YouTube video on the left is poorly described, making it difficult for potential users to find. The YouTube video on the right is well described, making it easier for potential users to find, understand, and verify.

Appropriately titling and describing your videos also lets YouTube editors know that your video contains important news and information, not just graphic or violent content. If your video is flagged, YouTube editors will rely on your title and description to determine whether your video is newsworthy or should be taken down.

SHARE: PROVIDING VIDEOS TO USERS

After users find videos in your collection, you need to provide the content to them in some form. The best delivery **format** will depend on what the user needs and their circumstances. Some users, for example, will only want to view the video online. Others will want a broadcast-quality copy. Some users may have unreliable Internet and electricity, while others have high-speed broadband.

VIDEO SHARING FORMATS

The archival concept of “**generation**” refers to the relationship between a copy of a video to its original. A single video can have multiple generations of copies, such as an original, a preservation **master**, a duplication master, a use copy, and a preview. Usually, a change in generation implies that the video has been **transcoded** into a different format (as opposed to being an exact copy of the original). Having multiple generations of a video therefore does not replace having **backup** copies of your original. Rather, its purpose is to allow you to use the video in different ways.



Generally, you will provide users with a use or preview copy, which is generated from a duplication master or directly from the original (if the original is in an easily usable format). The format of the use copy depends on how the video is going to be used, and the user should provide you with specifications. A news outlet might require a broadcast-quality MPEG-2 file, for example, while an academic researcher might request a DVD. YouTube prefers an H.264/mp4 file. In some cases, you may be asked to provide something other than a use copy, such as copy of the original for a court case, or a copy of the duplication master for a distributor.

See the section on “**Transfer**” for more on how to upload or send your videos.

Try This BASIC

[xmedia](#)⁴⁰ recode is a free GUI for ffmpeg.

Try This ADVANCED

[MPEG Streamclip](#)⁴¹ is a free video player, editor, and converter.

Try This ADVANCED

[ffmpeg](#)⁴² is a free collection of software that can transcode many video and audio formats.

⁴⁰ <http://www.videohelp.com/tools/XMedia-Recode> ⁴² <http://www.ffmpeg.org>

⁴¹ <http://www.squared5.com>

SHARE: CONTROLLING ACCESS

There are many reasons why you may want to control access, such as:

- For the safety of the activists, victims, or others in high-risk situations whose identities or locations cannot be revealed.
- To respect the wishes for privacy expressed by the people depicted in your videos.
- To protect particularly vulnerable people or people who did not give **informed consent** to be filmed.
- You do not trust the user who is requesting your video.
- You want to derive revenue from providing access to your video.
- You do not have the rights to allow others to use the video.



Control access to protect the privacy or security of people in your videos.

WAYS TO CONTROL ACCESS

There are ways to control access without making your collection completely inaccessible:

VET YOUR USERS

It is reasonable for you to ask users for details about who they are and why they want your video. This can be done through a one-on-one interaction, or through something like a web submission form.

CREATE ACCESS TIERS

Depending on what tools you use to share information and videos, you can provide different levels of access to different types of users, for example, by requiring a login and password.

CREATE ALTERNATE VERSIONS

You can create redacted, sharable versions of your videos. Depending on the restrictions required, you can edit out sections, blur faces, or alter voices. You can also create versions that are lower resolution or watermarked.

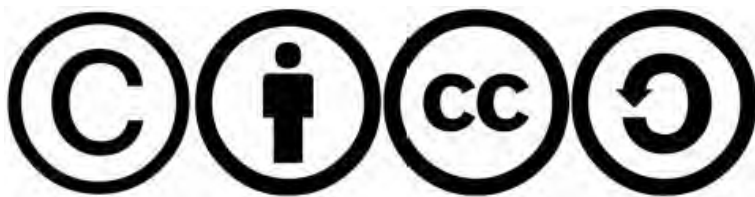
COPYRIGHT LICENSING

Copyright is a legal mechanism that protects a creator's exclusive right to copy, distribute, and use their work. If you own the copyright to a video, you can license, or share, some or all of those rights with others. You can license a video to someone one-on-one, or you can use an "open license" such as [Creative Commons](#) to share your video with everyone. See the next section on "[Understanding Copyright](#)" for more information.

Methods of controlling access are not foolproof. To be on the safe side, you should assume that anything you share or put online can be made public and possibly used without your permission or in a way that you do not agree with. If a video presents a serious risk, do not share unless you are sure it is going to a trusted destination.

SHARE: UNDERSTANDING COPYRIGHT

You may be unconcerned with **copyright** and **intellectual property** laws when trying to get important videos out to the world. This is especially true if you are working a situation where there is no rule of law. There are some instances however, especially in the longer term, when an understanding of intellectual property rights may come in handy.



- If a site like YouTube takes down your video because of a third-party copyright claim.
- If someone uses your video without your permission in a way you do not agree with.
- If a television producer wants to use your video but needs to clear the broadcast rights.
- If a film festival wants to show your video but needs the public performance rights.
- If you want to derive revenue from your video collection.
- If you deposit your collection in an archive that requires rights information.

Intellectual property laws vary from country to country, but there are general principles that most countries (the 165 signatories to the [Berne Convention](#)) adhere to. The following information is not intended to be legal advice or substitute for legal advice.

COPYRIGHT

Copyright laws protect rights of creators to their work, including videos, for a set amount of time (around 50 years, varies by country). These rights include the right to copy, distribute, display or broadcast, and to re-use or adapt the work.

The person who records raw video footage, or who creates an edited video, automatically owns the copyright from the moment the video is created. This person can, however, transfer these rights to someone else (see "Granting Permissions" below).

In sum, copyright protection means that:

- People cannot copy, distribute, display, broadcast, re-use, or adapt your videos without your permission.
- You cannot copy, distribute, display, broadcast, re-use, or adapt someone else's videos without their permission.

EXCEPTIONS TO COPYRIGHT

Laws vary, but one of the general exceptions to copyright protection is “free” or “fair” uses. In some countries, free or fair uses include use for teaching purposes, use for news reporting, and copying for private, personal, non-commercial use.

This means that:

- People can make limited use of your videos without your authorization, within the bounds of free or fair use exemptions in their country's law.
- You can make limited use of others' videos without their authorization, within the bounds of free or fair use exemptions in your country's law.

Try This BASIC

The Fair Use/Fair Dealing Handbook⁴³ summarizes fair use laws in 40 countries.

Try This BASIC

Columbia University Libraries Copyright Advisory Office has a Fair Use Checklist⁴⁴ to help determine whether usage falls within the limits of fair use in US Copyright law.

GRANTING PERMISSIONS

As a copyright holder, you can give other people permission to copy, distribute, display, broadcast, re-use, or adapt your video. There are a few ways you can do this:

ASSIGNING COPYRIGHT

Completely hand over the copyright ownership of your video to someone else, i.e. you do not have rights to it anymore. It is common for staff at organizations, for example, to have agreements that state that the work they create during work hours belongs to the organization.

LICENSING

Allow someone to use your video in a particular way (often for a fee), without giving up the ownership of the video. You negotiate terms that specify how, where, and for how long your video will be used. For example, you could allow a filmmaker to use 10 seconds of your video in a documentary, for DVD and European broadcast, for the next 2 years.

⁴³ <http://infojustice.org/wp-content/uploads/2013/04/Band-and-Gerafi-04032013.pdf>

⁴⁴ <http://copyright.columbia.edu/copyright/fair-use/fair-use-checklist/>

“OPEN” LICENSING

Allow anyone to use your video, for free and without consulting you, without giving up the ownership of your video. You can set some limitations on use. Using a [Creative Commons](#) license is one easy way to do this. With a Creative Commons license, you can specify whether uses require attribution, have to be non-commercial, and other qualifications.

SHARE: TAKEAWAYS

- Identify your key users, how they want to be able to find and access your videos, and if any controls need to be put on usage.
- **Create a [finding aid](#) -- in the form of a guide, list, index, and/or catalog -- with appropriate [access points](#) to enable your users to access your videos.**
- Make use copies from your duplication [masters](#) or originals as needed, in the format your user requires.
- Control access to your collection, if necessary, to protect the identities of those in high-risk situations or to respect privacy.
- **Assume that anything you share or put online can be made public or used without your permission or in a way you do not agree with.**
- Be sure you have the legal rights to provide access.

KEY CONCEPTS IN THIS SECTION

Informed Consent:

There are potential consequences to providing access. This is why you obtain informed consent when you film.

[Read More...](#)

Generation:

Provide your users with use copies generated from your duplication master or original.

[Read More...](#)

Finding Aid:

A finding aid is the tool that you provide to your users to help them find what they are looking for.

[Read More...](#)

Findability:

A key aspect of providing access is making it easy for users navigate and locate what they are looking for.

[Read More...](#)

RESOURCES: VIDEO AS EVIDENCE



From the Thomas Lubanga Dyilo case at the International Criminal Court (ICC).

Video is increasingly serving as evidence in a broad range of legal settings, but there are currently no universal concrete standards for admissibility. If you want to use a video as evidence, ensure that you investigate and consult legal professionals on the requirements relevant to your court's jurisdiction.

As a rule, however, any evidence must first and foremost be deemed relevant to the case or investigation in question, and to hold probative value. Probative value is the ability of evidence to prove an issue, and increases when the evidence can be shown to be **authentic** and reliable. The actions you take to ensure the authenticity of your video therefore strengthen its probative value.

Video evidence needs to be properly documented and handled to maintain its authenticity. According to Elliott Goldstein, author of *Visual Evidence: A Practitioner's Manual*, "any defensible procedure for documenting and preserving digital video evidence must answer these questions:

1. Who captured the image and when?
2. Who had access to the image between the time it was captured and the time it was introduced into court?
3. Has the original image been altered in any way since it was captured?
4. Who enhanced the image, when and why?
5. What was done to enhance the image and is it repeatable?
6. Has the enhanced image been altered in any way since it was first enhanced?"

Source: Careless, James. "Video Evidence." CBA PracticeLink. Canadian Bar Association.

Steps taken throughout the **archiving** process, as outlined in this Guide, can help to ensure that you can answer these questions. In summary:

CAPTURE IMPORTANT METADATA AT THE POINT OF CREATION

The most important information to capture is that which can lead to corroboration: date and time, geographic location, and the video's creator or source. This metadata can support a video's authentication. See **"Create"** for more.

KEEP CONTEXTUAL METADATA ABOUT YOUR VIDEO

Cataloging and detailed description can support the credibility of video evidence by ensuring that corroborating contextual information has been documented and linked to the video in a structured way. However, the description must be accurate; always be clear and truthful about disputed or unverified information; and do not editorialize. See **"Acquire"** and **"Catalog"** for more.

DOCUMENT CHAIN OF CUSTODY

Keep a complete summary of when you acquired a video file, who else has had custody of the video file and when; who had access to your video file and when; what actions (e.g. alterations) were performed on the file and by whom. See **"Acquire"** and **"Catalog"** for more.

MAINTAIN AUTHENTICITY

Always retain the **original files** from the camera, unaltered and un-**transcoded**, and do not rename them. Always retain the **original order** of files from the camera. See **"Transfer," "Acquire," "Organize,"** and **"Store"** for more.

DOCUMENT FILE FIXITY

Hash values can show whether your files have been tampered with, so it is valuable to compute and capture hashes early in the video lifecycle. Compute and keep a record of hashes at the point of creation, or as soon as you **offload** files from your camera. See **"Transfer"** for more.

ADDITIONAL RESOURCES

Try This BASIC

"Video as Evidence" chapter in Video for Change: A Guide for Advocacy and Activism.

Try This BASIC

WITNESS Filming for Human Rights Documentation, Evidence and Media tipsheet.

RESOURCES: KEY CONCEPTS

Here are some key concepts important for understanding archiving. For additional terminology used in the Guide, see the [Glossary](#).

ACCESS POINT

A name, term, code, or type of information such as the date, by which a set of records can be sorted or searched. For example, in a library book catalog, access points are author, book title, and subject. In a database, access points are any fields you can search, such as name, date, and title.

ARCHIVE

An organization made up of people and systems responsible for [preserving](#) records and documents of enduring value and making them available to a designated community. Archives are sometimes parts of larger organizations, such as universities, public libraries, media centers, or museums.

ARCHIVING

The practices and decisions that support the [preservation](#), [authentication](#), use, and accessibility of content with enduring value.

AUTHENTICITY

The quality of being genuine, not fake or counterfeit, and free from tampering. Authenticity means that an object was actually created by the person represented as its creator, and that it was actually created at the time and place that is represented as its time and place of creation. Video footage that has been manipulated or altered but is represented as if it had not been, for example, is not authentic.

To authenticate a video means to verify the relationship between it and its creator and point of creation. Documentation about who created something, when and where it was created, and the [chain of custody](#) can provide a starting point for this authentication process.

CATALOGING

Creating and organizing descriptive information in a structured way so that resources can be found, used, and understood. Cataloging expands on basic [metadata](#), and enables users to access content in multiple ways.

CHAIN OF CUSTODY

Chronological documentation that shows who has held or controlled a video file from the moment it was created. The ability to show an unbroken chain of custody is one important indicator of the authenticity of a video, and therefore a factor in using video as evidence.

COMPLETENESS

The quality of having all of the information a record contained when it was created, and that its original context is maintained. Incomplete records are not as reliable as complete ones, since one might not know what information is missing and why. **Transcoding** a video to another format can reduce the image quality and discard metadata, making the video less complete and therefore less reliable. Keeping original video files, documenting context, and organizing videos in a way that maintains the original order of video files contributes to the completeness of the video records.

CONTROLLED VOCABULARY

A predefined list of terms used to ensure consistency in **cataloging**. Since there is usually more than one way to describe or refer to a concept, choosing one term eliminates guesswork and circumvents the normal ambiguities of language (and spelling). Imagine searching for “Doctors” only to later learn that some records use the term “Physicians”. Consistent vocabularies increase the **findability** of records.

FINDABILITY

The ability of a user to easily find what they are looking for.

FIXITY

Related to **integrity**, the quality of being unchanged over a given period of time. Fixity maintains the authenticity of an object over time, and is key to the concept of **preservation**. Long-term fixity requires good policies and handling practices, sustainable infrastructure, and strong security. Regular fixity checks (e.g. computing and comparing checksums) are used to detect changes.

GENERATION

The relationship between a copy and its **original**. This term originates from the time of analog copying. In the digital realm, where it is possible to create exact copies of originals, generation usually implies a change in format or specifications, such as an H.264 access copy generated from an Apple ProRes **master**. Having a video available in multiple generations is therefore not a replacement for having exact **backup** copies of your originals.

INFORMATION PACKAGE

A self-describing container - usually a clearly named folder or directory - used to keep media and its related documentation or **metadata** together.

INFORMED CONSENT

The process of ensuring that a person identified in a video fully understands the purpose and intended use of the recording, as well as any potential unintended consequences of his or her participation. With this awareness, the person must voluntarily give his or her permission to be identified and for the recording to be used.

INTEGRITY

The quality of being whole, unaltered, and uncorrupted. A file that is not intact may not be usable or may have decreased informational and evidential value. Videos files can lose their integrity if they are accidentally mishandled, deliberately tampered with, or if data corruption occurs in transfer or storage due to hardware or software malfunction. The best way to ensure integrity is to establish a system to check file **fixity** regularly (e.g. by computing **hashes** and checking them against a registry of previously computed hashes) and to restore any corrupted files from an intact copy.

INTEROPERABILITY

In an information technology (IT) system, the quality of being able to exchange information with another system and being able to use that information. Using widely adopted **formats**, **metadata** standards, and **controlled vocabularies** enhances interoperability.

MEDIA MANAGEMENT

The process of keeping track of media, such as the video files in your collection, and overseeing any actions performed on your media, such as **backup**, **refreshment** or **migration**. Media management can be performed manually, or with the aid of a software system (e.g. a media asset management (MAM) system).

METADATA

Any information about a video: from technical information **embedded** in the file that allows the video to function, such as **format** and duration, to descriptive information about the content to help you understand or find it--such as keywords, security restrictions, geographic locations, and so on. Metadata is critical to any future use, and is important throughout the archiving process.

Despite what is sometimes said, images almost never speak for themselves. They require context and description to make sense, to corroborate their factuality, and to be accessible beyond one person's memory or desktop.

Metadata can be automatically generated and embedded in the file, such as with technical metadata, or it can be manually recorded on an external medium, such as with descriptions, security flags, and keywords in a database. Metadata capture sometimes needs to be manually enabled on your device, such as with GPS or location services.

MIGRATION

The process of re-encoding or transferring data from one digital or physical **format** to another to ensure long-term accessibility of the information as the format becomes **obsolete** and unusable over time.

OBSOLESCENCE

The process of becoming out-of-date and unsupported by available technology. Video cameras, video **formats**, storage media and storage devices, can all become obsolete over time. The obsolete technology is functional but is unusable because the other technologies they depend on no longer support them. An old video camera, for example, may not be able to plug into new computers, or an old video format might not be playable on new desktop video players.

ORIGINAL FILE

In the digital realm, the "original file" is any copy of a file that is exactly the same (i.e. bit-for-bit) as the file in question when it was created. This means that there are no accidental or deliberate alterations to any aspect of the file, including its **format** and technical specifications.

ORIGINAL ORDER

The archival principle of maintaining files in the same order they were created. Original order is important to preserve context and the relationship between individual files, so that you can make sense of each file and of the whole. Keeping files in their original context makes them more **complete** and reliable.

PRESERVATION

The process of ensuring the long-term accessibility of **authenticated** content. Digital preservation involves preventing loss or damage to digital objects, and extending their existence beyond the lifespan of their storage media or technology. Preservation requires ongoing resources, commitment and actions.

REFRESHING

The process of copying data from one storage medium to another to ensure continued access to the information as the storage medium becomes **obsolete** or degrades over time. It is one strategy for avoiding loss of digital information.

SELECTION

The process of identifying materials to be acquired, or to be preserved, because of their enduring value. Having selection criteria, or a selection policy, helps ensure you acquire and save only what is most important.

UNIQUE IDENTIFIER

A number, word, or symbol for unambiguously identifying and distinguishing an object from other objects in a set. Common everyday unique identifiers include computer logins, credit card numbers, tax ID numbers, and so on. Applying unique identifiers to video files makes it easier to identify, distinguish, and organize videos and related documents.

WORKFLOW

A map of processes and roles for activities that require multiple stages and usually more than one person.

Control, accountability, and consistency are key to effective **archiving**, yet archiving involves many steps and potentially many people. It is therefore important to clearly define roles and document procedures so that people working in distributed locales understand their responsibilities, produce usable results, and ensure safety and security. Workflows need not be complex, but are often a helpful tool to plan your work.

RESOURCES: GLOSSARY

API (APPLICATION PROGRAMMING INTERFACE)

A protocol that specifies a way for a software application to communicate and integrate with a program that provides a service. Google provides APIs, for example, so that people can use its data, such as location data from Google Maps or video data from YouTube, in their applications.

BACKUP

A copy of data, stored in a secondary location, which is used to restore data in the primary storage location that is corrupted or lost. Restoring involves copying data from the backup to the primary storage to replace the corrupted or lost files. Backing up is a storage strategy that allows you to recover from data loss.

CHECKSUM

See “**Hash Value**”

CLI (COMMAND-LINE INTERFACE)

A way of interacting with a computer program which involves typing lines of text in a command-line shell. Some programs are only available with command-line interfaces, which facilitate their automation and use in programming scripts. However, command-line interfaces can be harder for casual computer users to interact with than **graphical user interfaces** (GUI), which use windows, icons, menus, and pointers.

CODEC

A codec is software that can encode/compress and decode/decompress digital files, including video files. Common video codecs include H.264/MPEG-4 AVC, MPEG-2, and DV. A video stream can be encoded with one of these codecs and contained in a **file format** like AVI or Quicktime.

COPYRIGHT

A legal protection intended to give the creator of original work exclusive rights to their work for a designated length of time. It gives the creator the exclusive right to copy, use, adapt, show, and distribute their own work, and the right to determine who else can copy, use, adapt, show, and distribute the work.

DATA DICTIONARY

A document that explicitly describes **metadata** structure and rules so that all catalogers input metadata in a catalog consistently. A data dictionary may also specify your **controlled vocabularies**. Data dictionaries do not contain actual metadata, only the instructions needed to create your metadata.

DATA MODEL

A description of the way that data is structured in a database. It can define what types of things the data describe, what types of data are included in the descriptions, and how different types of things relate to each other.

DERIVATIVE

A copy of a video generated from a master that is usually in a different format and of lower quality than the **master**. Derivatives can be made for various uses, such as web upload or DVD.

DIGITAL VIDEO

An audiovisual signal that is represented in discrete bits, as opposed to a continuous analog signal. Analog video, such as Hi8 or VHS, is **obsolete**; all video cameras available today record digital video. Digital video can be tape-based (e.g. miniDV, HDV) or file-based (e.g. .mov, .avi). In this guide, we focus on file-based digital video, as tape-based digital video is mostly obsolete.

DOWNLOAD

To receive data from a remote computer system and save it in a local computer system. The inverse of download is “**upload**.”

EDL (EDIT DECISION LIST)

A document used in video post-production that contains a list of clips used in an edited video. EDLs originate from older film and video workflows when editing was a two stage process. Today, they can be used to move editing projects from one software or system to another. EDLs also provide useful documentation, showing what source files were used to create an edited video.

EMBEDDED METADATA

Metadata that is stored within the digital object it describes. Some embedded metadata, such as file size, are essential to the functioning of the file, and are always written to the file by the device or software system. Other embedded metadata are non-essential and can be optionally added (e.g. rights information). Embedded metadata is not guaranteed to be accurate—for example, if your camera is set to the wrong date. Embedded metadata stay with the digital object as long as the object is intact, but can be intentionally stripped or altered. Embedded metadata can be lost if a file is transcoded to another format.

ENCRYPTION

The process of encoding your files using a cryptographic algorithm so that only authorized parties with a “key”(e.g. a password) can decrypt them. The two main types of encryption are symmetric-key and public-key. Symmetric-key encryption uses the same key, or password, to encrypt and decrypt information. Public-key encryption uses one key to encrypt, and a different one to decrypt, and is more secure.

ENTITY

In data models, an entity is any “thing”that is identified and described with data. For example, if a database keeps track of the model, year, and license plates of all the cars in a sales lot, each car is an entity.

FAT32

A computer file system developed by Microsoft that can be read and written to by Mac and Windows devices. Many USB flash drives come formatted as FAT32. The maximum file size on a FAT32-formatted volume is 4GB, which may not meet the needs of large video files.

FILE FORMAT

The specification by which a digital file is encoded. Some file formats are designed to store particular kinds of data while others are more like containers that can hold many kinds of data. Common video file formats like Quicktime (.mov), AVI, and mp4 are container formats that contain video and audio streams, metadata, subtitle tracks, etc.

FINDING AID

A document that contains information about a specific collection within an **archive**. It is a simple way for users to determine if the content in a collection is relevant to their research. The structure of finding aids differ depending on the material being described; they can contain detailed content lists, a description of the scope of the collection, biographical and historical information, and even restrictions on use or access to the content.

FIREWIRE

An interface standard for transferring data between digital devices, especially audio and video equipment. Developed by Apple in the 1990s, FireWire is becoming **obsolete**.

FTP (FILE TRANSFER PROTOCOL)

A network protocol for transferring files between two points over the Internet. Users use FTP client applications (e.g. [FileZilla](#)) to communicate with an FTP server.

GUI (GRAPHICAL USER INTERFACE)

A way of interacting with a computer program that involves using windows, icons, menus, and pointers. Most computer users are familiar with graphical user interfaces. GUIs can be easier for casual users to interact with than **command-line interfaces** (CLI), which require commands to be typed as lines of text.

HASH FUNCTION

An algorithm that computes a **hash value** or checksum from any set of data, like a file. Common hash functions include MD5 and SHA1. Hash functions are used to check file **integrity** and for security purposes.

HASH VALUE

The string of alphanumeric characters that results from running a **hash function** algorithm on data or a file. The hash value of a file will always remain the same as long as the file is unchanged, so it can be used to identify altered, corrupted, and duplicated files.

HFS

A computer file system developed by Apple that can only be read by Windows devices using special software. Windows devices cannot write to HFS-formatted volumes.

INTELLECTUAL PROPERTY

A legal concept that refers to creative works for which exclusive rights are recognized. Common types of IP rights include **copyright**, trademarks and patents.

MALWARE

A term derived from “malicious software,” and that refers to all computer viruses, worms, Trojans, and spyware.

MASTER

The earliest generation or highest-quality output of a video from which duplicates are made.

METADATA STANDARD

A published document that describes how to create, use, and interpret **metadata** in a specific domain or for a specific purpose, which is intended to establish a common understanding among its users. A metadata standard defines the structure and meaning of its acceptable data elements, rules, and values. Many communities, including broadcasters, social scientists, and art museums, publish metadata standards to meet their descriptive needs.

NAS (NETWORK ATTACHED STORAGE)

Computer data storage that is accessed through a network. A NAS appliance is a computer that is specially designed to store and serve files over a network.

NTFS

A computer file system developed by Microsoft that is read-only on Macs. Macs can write to NTFS-formatted volumes only with special software.

OFFLOAD

To copy media from a camera or memory card to a storage device connected to a computer.

OUTPUT

To export a completed video at the end of the post-production process. It is important to always output a **master**.

PETABYTE

A unit of measure for data. One petabyte (PB) is equivalent to 1,000 terabytes (TB), or 1,000,000 gigabytes (GB).

RAID (REDUNDANT ARRAY OF INDEPENDENT (OR INEXPENSIVE) DISKS)

A storage technology that combines multiple hard drives together to provide fault tolerance and better performance. Data is spread out across the drives, along with additional calculated data, so that data can be re-generated if part of the array fails. RAID protects you against data loss in the case of hardware failure. Unlike **backup**, RAID does not offer protection against file corruption or deletion, or data loss to **malware**, theft, or natural disaster.

REPOSITORY

A system that acquires, stores, monitors, **preserves**, and provides access to its resources, run by an organization committed to providing long- term access to **authenticated** content to its users. A repository requires significant infrastructure to build and maintain.

SAN (STORAGE AREA NETWORK)

A dedicated network of storage devices shared among multiple servers, designed for fast access and large data transfers.

SYNCHRONIZATION

The process of ensuring that computer files in one location are copied to one or more other locations on a regular basis. Synchronization is also referred to as mirroring or replication. Unlike **backup**, synchronization does not allow you to go “back in time” to recover lost or altered files.

TRANSCODE

To re-encode a digital file to a different encoding scheme, such as converting an H.264/MPEG-4 AVC video to Apple ProRes. Transcoding is usually done when a video’s encoding is not supported by the system that needs to use it. Transcoding fundamentally alters the file, although lossless methods can allow the original data to be reconstructed from the transcoded data.

UPLOAD

To send data from a local computer system to a remote one. The inverse of upload is “**download**.”